A Multi-Channel Steganographic Communication Protocol: Design, Game-Theoretic Evaluation and Application to a Case Study in SMS Mobile Banking

A DISSERTATION PRESENTED
BY
Anthony Michael Obinna Omego
TO
The Faculty of Science, Engineering and Computing

IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
Doctor of Philosophy
IN THE SUBJECT OF
Computer Science

Kingston University
Kingston Upon Thames, England
October 2021

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgement, the work presented is entirely my own.

I hereby certify that this thesis constitutes my own work, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the thesis describes original work that has not previously been presented for the award of any other degree of any institution.

Obinna Omego Date: 20/10/2021

Abstract

In the twenty-first-century society, which focuses on digital technologies and services, systems such as mobile banking are progressively adopted by the worldwide population. Currently, the number of mobile banking subscribers worldwide exceeds 1.75 billion, representing 32 percent of the global adult population. Banks and payment institutions continue to provide accessible and reliable channels for payment transfer and seamless coordination of banking activities. Mobile banking has become one of the principal domains targeted by tech-savvy criminals due to the lack of user awareness and insufficient software security measures. In some parts of the world, SMS banking offers a convenient mobile banking service that is easy to implement. However, it is only feasible under the assumption that SMS service providers provide secure SMS services to users.

In this thesis, a novel secure SMS banking protocol based on steganography is proposed. The steganographic system proposed is based on a multi-channel security protocol that combines steganography by cover synthesis and steganography by cover modification. The new security protocol has been inspired and developed by protocols proposed for the security of Online Social Networks and Social Media Platforms. The resulting protocol considers the mobile characteristics and constraints, delivering confidentiality based on steganography with multiple channels but avoiding the need for hardware devices creating symmetric session keys as in traditional cryptographic protocol solutions. The secure system is designed in such a manner that it makes the protocol robust against various types of adversarial attacks.

Furthermore, this novel protocol is evaluated with a theoretical framework by applying the concept of game theory to a range of steganographic protocol settings. The game theory models developed are based on two-player non-zero-sum complete information games in strategic standard form. A range of use cases is designed, simulating these game-theoretical models using Matlab.

Dedication

This thesis is dedicated to Ezechitoke, Ndishi/ Nna, Ata Oyere, Ata Ona, Ata Omego, Arushi Isi Iyi-Ogwugwu, Arushi Ideyi ma-ma Eze, Eze-Nwanyi Iyi Opobo, Omaba, Arushi Ngwu and Igbo.

Acknowledgement

I am very grateful to all individuals who has supported me during my doctoral study journey. I will take this opportunity to acknowledge those whose advice greatly influence the success of this research.

At first, I would like to sincerely express my appreciation to my supervisor Dr Eckhard Pfluegel for his utmost support, encouragement, motivation, patience and knowledge. The guidance of my supervisor aided me greatly during my research.

Secondly, I would like to thank my second supervisor, Dr Martin Tunnicliffe, for all the insightful feedback, questions, and comments throughout my study.

Thirdly, I am deeply grateful to my co-authors for the various valuable and helpful comments that considerably contributed to this thesis: Dr Charles Clarke and Dr Gordon Hunter.

Finally, I would like to express my sincere gratitude to my family, the love of my life and my friends, who have continuously supported me throughout my doctoral studies.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

THE establishment of telephone communication networks at the inception of the 20th century is often comparable to the impact of Internet technology in society worldwide. Internet technology through e-commerce enables the relationship between customer and merchant flexibility. Contemporary advances in this technology enable mobile computers and devices to be equipped with wireless interfaces. Technology offers a new paradigm of computing that enables people with mobile devices to share infrastructure irrespective of their geographical location. In Japan, the success of the Mobile phone operator company, namely NTT DoCoMo's i-mode, with about 34 million data subscribers, exemplifies the necessity for mobile data services. In Europe and Africa, the widespread uptake of Short Messaging Services (SMS) has demonstrated the high demand for additional services in the market. In 2001, over 30 billion SMS messages were transmitted according to the GSM Association and a billion wireless users by the end of 2005. Several mobile devices were explicitly manufactured to aid users in processing stock trading, collecting product information, and product purchasing [194].

The advancement of payment from the physical exchange of notes and writing cheques to payment through cards over the internet has made purchasing goods and services flexible. For example, in card payment, the interchange occurs between the merchant's bank and customer's bank over a communication channel managed by card payment services or organisations. The development of e-commerce payment services has put extra pressure on payment service providers, card companies, mobile operators and banks to provide adequate security and interoperability. The emergence of mobile payments has introduced an extra layer of complexity through constrained devices with numerous capabilities. Mobile banking executed through a mobile network should be placed to the same level of standardisation that governs physical payment cards used to be perceived as familiar and secure by the public.

Mobile banking services are diverse and determined by regional differences and the individual market dynamics. For instance: in Europe, a mobile top-up for prepaid phone services is ubiquitous. In Japan, mobile Internet services are successful. They can be attributed to the high concentration of populations in urban areas, consumer satisfaction with portable electronic devices, extensive commute times, and widespread wireless network infrastructure [194]. The launch of M-Pesa mobile money accounts in Kenya has over 13 million Kenyans using their mobile phones to purchase goods and services. There are over 90 million active mobile subscribers in Nigeria. This adoption perhaps has motivated the Central Bank of Nigeria (CBN) to establish mobile financial services all over the country [155] [68].

Mobile banking is a subset of online banking; there are differences. According to the study in [123], mobile banking over online banking is due to the mobility, portability and instant connectivity of mobile phones. The classification of mobile banking payments is

Macro-payments and Micro-payments. Macro-payments refer to substantial payments such as online shopping, while micro-payments refer to $5 or fewer payments. The difference between these two types of payments is essential since the required security will be dissimilar. For instance, authentication for every macro-payment via a trusted financial entity is crucial, although network authentication could be sufficient for micro-payments that only use the operator's infrastructure.

The SMS (Short Message Service) is an alternative payment scheme to achieve payments with simplicity, convenience and low cost. The SMS is a texting service available on an extensive range of networks, including 3G and 4G networks. However, it was initially designed as part of the GSM (Global System for Mobile communication) and can transmit non-sensitive messages across the mobile network. Many organisations, businesses and individuals use SMS for official purposes. SMS is used to enquire about transaction information and account status in mobile banking. In order words, with mobile, SMS banking enables an environment where users can request banking information, transfer money, check account balance, manage an account, pay bills, request a cheque, and so on through the mobile network. Though securing SMS is challenging due to the nature of the wireless medium. The wireless network uses an air interface that is a shared medium; an adversary tuned into the frequency correctly can access the SMS. Secondly, encryption techniques used for security is considered insecure and, therefore, vulnerable to various attacks. Hence, this motivates the need to design a secure SMS based mobile banking protocol that intends to provide confidentiality and integrity to users while performing transactions on the network environment.

1.1 Research Aims and Objectives

This research aims to improve the security of existing SMS based mobile banking frameworks by designing new security controls in the area of cryptographic and steganographic protocols, to alleviate fraud and surveillance in mobile banking. These goals will be attained by addressing the following objectives:

- To devise a novel multi-channel SMS-based mobile banking protocol, based on extending protocols employed for secure communication in Online Social Networks, for application to a suitable use case in developing rural areas.
- To design a more robust version of the protocol, mitigating typical network security attacks such as multi-channel replay and man-in-the-middle attacks.
- To develop a novel game theoretical framework for information hiding models in a range of network scenarios, enabling the evaluation of a hybrid-entropy steganographic protocol based on simulations using Matlab.

1.2 Research Contributions

The research contributions made in this thesis focus on the design and evaluation of a novel security protocol for SMS-based mobile banking. As presented in the previous section, these contributions align with the individual research objectives.

- Contribution 1, the new security protocol, has been designed and inspired by the security protocols in the context of Online Social Networks and Social Media Platforms [26, 47, 63, 170]. The resulting contribution to knowledge is the adaptation of these types of protocols to the SMS mobile banking setting, and the arising confidentiality protection against eavesdropping by the actual service providers. To the author's knowledge this has not been investigated in previous works.

- Contribution 2 is a strengthening of the new security protocol, designed in such a way that it makes the protocol robust against typical network security attacks such as single-and multi-channel man-in-the-middle attack, single-and multi-channel replay attack, and steganalysis under certain circumstances. As a result, the protocol achieves data integrity and message freshness for SMS banking transactions. This robust security design could be essential for adapting the protocol in future real-world scenarios. Together with the previous contribution, this establishes a thorough security analysis of the multi-channel protocol.

- Contribution 3 of this thesis describes a novel theoretical framework for models applying the concept of game theory to a range of steganographic protocol settings. The game theory models are based on two-player non-zero-sum complete information games in strategic standard form. This framework is then used to evaluate the steganographic protocol of Contribution 2. Using the Matlab scientific tool, a range of use cases is designed, simulating these game-theoretical models.

1.3 Thesis Organisation

This thesis is organised as follows:

Chapter 2 — Background and Network Security Concepts. This chapter presents a brief introduction to various security concepts. The areas presented include the security services such as Data Confidentiality, Data Integrity and Data Availability. Secondly, various steganographic concepts are discussed. These steganographic concepts include Digital steganography, steganography by Cover Selection, steganography by Cover Synthesis and steganography by Cover Modification. Finally, this chapter also discusses the reference model for mobile banking, mobile banking applications and entities in mobile banking.

Chapter 3 — Security Definitions and Terminologies. In this chapter, the cryptographic security definitions and terminologies used throughout this thesis are presented. This chapter presents cryptographic terminologies such as encryption, hash functions, semantic security, Secret Sharing and anonymity concepts. Also, this chapter presents concepts in game theory such as the non-cooperative game theory, strategies in normal-form games, and solution concepts in game theory.

Chapter 4 — Literature Review. In this chapter, various literature relevant to this thesis are discussed. The literature presented is divided into four sections. At first, the security issues and attacks in the short message service (SMS) are discussed. Secondly, the techniques used to secure SMS transmission are presented as well. This technique includes secure SMS protocols based on encryption and steganography, respectively. The following section presents SMS banking approaches based on encryption and steganography, which researchers have proposed. It also presents the specialised multi-channel Online Social Network (OSN) protocols. Finally, we present security games based on steganography which are specific non-cooperative two-player games relevant to the games developed in this thesis.

Chapter 5 — A Multi-Channel Steganographic Protocol for Secure SMS Mobile Banking. This chapter introduces the concepts of dual entropy steganography in an SMS based mobile banking environment. In this paper, a novel secure SMS banking protocol is proposed. The approach is based on a multi-channel security protocol combining low and high entropy steganography. One of the distinct advantages of this protocol is its confidentiality property against the mobile network operator, which, to the author's knowledge, is a novel feature. Furthermore, the required architecture is simple and only involves GSM services and one additional internet connection, which can be insecure. As such, it offers security, low deployment costs and would be suitable, for example, in rural areas or countries without individual secure home internet connections.

Chapter 6 — Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol. In this chapter, an improved SMS banking protocol that was already presented in Chapter 4 is described. After analysing the security of this prototype protocol, the threat of a multi-channel replay attack is addressed by introducing server-side nonces. As a result, the strengthened protocol is secure and robust for real-world scenarios. In addition, a thorough strategy of the practical requirements necessary for implementing the system is described. Finally, a Cost-Effectiveness analysis is calculated against an existing solution to justify the practicability and benefits of the protocol.

Chapter 7 — A Game-Theoretic Decision Model for a Hybrid-Entropy Steganographic Protocol. In this chapter, we devise a novel game theoretical control framework for steganographic models in an insecure and constrained public network based on considering two-player non-cooperative games. These models aim to evaluate steganographic systems developed in Chapters 5 and 6 by designing use cases with reasonable strategies that can be applied in a realistic environment. Also, the models can assist in studying the principles of game theory for the development of steganography. The evaluation of these models is implemented with the aid of the MATLAB computing tool.

Chapter 8 — Conclusion. Finally, in this chapter, the summary of the research results from this thesis is presented. The conclusion chapter is divided into two major sections: discussion and future research. The discussion section discusses a significant security challenge known as a confidential messaging exploit and traffic analysis. The future research section outlines four major challenges that need to be addressed.

1.4 Associated Publications

As part of the research carried out for this thesis, the following peer-reviewed articles have been published:

1. Obinna O, Pfluegel E, Clarke CA, Tunnicliffe MJ. A Multi-Channel Steganographic Protocol for Secure SMS Mobile Banking. In: The 12th International Conference for Internet Technology and Secured Transactions (ICITST-2017). Cambridge, United Kingdom: IEEE; 2017. p. 248–53.

2. Obinna O, Pfluegel E, Tunnicliffe MJ, Clarke CA. Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol. In: International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018),. Glasgow, Scotland, UK: IEEE; 2018.

3. Tunnicliffe MJ, Obinna O, Pfluegel E. Hidden Protocol Strengthening with Random Sentences as Cryptographic Nonces. In: Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019. London, England: IEEE; 2019.

As part of the materials published in these papers, an additional collaborative contribution was made in the paper **Hidden Protocol Strengthening with Random Sentences as Cryptographic Nonces**. This research is included in Section 6.6 for reasons of completeness, and we refer to the published paper to study the novelty aspects of this contribution in detail.

Chapter 2

Background and Network Security Concepts

This chapter presents various background and network security concepts relevant to this thesis. In the contributions Chapters 5 and 6 of this thesis, the central focus regarding security services is Data Confidentiality and Data Integrity. The Data Confidentiality goal directs towards preventing surveillance, the discourse of SMS banking transactions and using financial information for malicious intent by unauthorised persons and adversarial entities. The Data Integrity interest is towards preventing modification attacks such as replay attacks and man-in-the-attacks. Therefore, this chapter presents security services, such as Data Confidentiality, Data Integrity and Data Availability. Secondly, the steganographic protocol developed in this thesis is a scheme that synthesises steganography by Cover Synthesis and steganography by Cover Modification; consequently, these steganographic concepts are discussed in section 2.3, which also includes steganography by Cover Selection. Finally, this chapter discusses the reference model for mobile banking, mobile banking applications and the entities in mobile banking considered in this thesis.

2.1 Security Services

The use of security services in mobile banking enables secure transactions. The security services employed use mathematical algorithms to safely transmit transactions in an unreadable manner to unauthorised entities. After the transaction has reached its destination, the authenticated recipient should reconstruct the original message. In [18], the security services consist of six services. However, in this thesis, the security services are classified into three primary services:

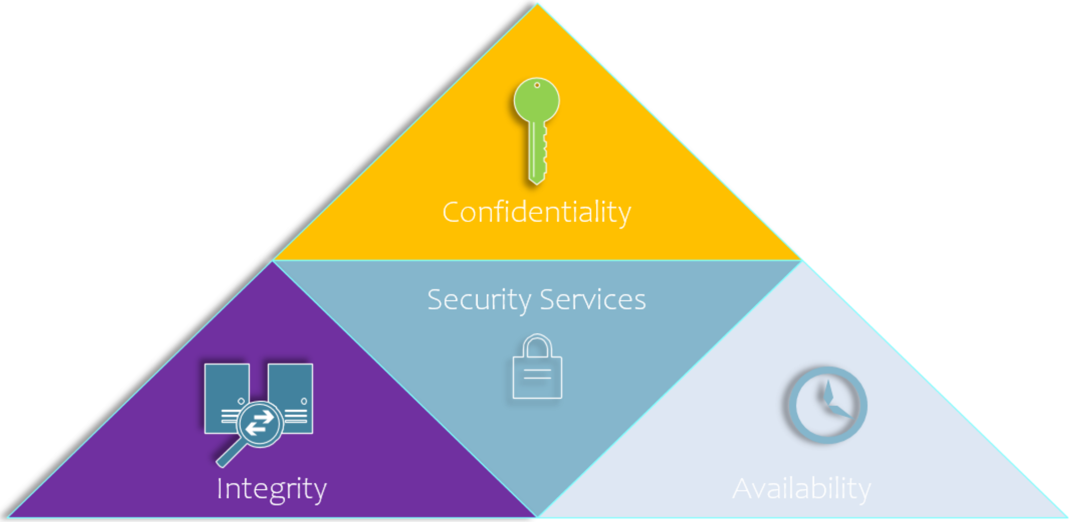


Figure 2.1: Network and Computer Security Services

2.1.1 Data Confidentiality

Data confidentiality protects private information from specific unauthorised individuals or systems. There are several levels of protection that can be used to protect data while in transmission. The TCP connection can protect the connection between two communicating entities that wish to exchange sensitive data. The small details of the service can also be defined, and the details may include the specific fields within the private message or protection from a single message. Protecting data in this method might be less cost-effective, complicated to implement and less valuable than a comprehensive approach.

Another necessary aspect of confidentiality is data traffic flow protection from traffic analysis. This concept requires that an adversary cannot know the source, destination and other characteristics of traffic flow.

2.1.2 Data Integrity

Integrity is another important factor that can be applied to a single message and a stream of messages. Data integrity ensures that sensitive data is not modified, deleted and interrupted without authorisation. A connection-oriented integrity service like the TCP ensures that data is not replayed, modified, inserted, reordering, duplicated or destroyed. Thus, the connection-oriented integrity service ensures security against denial of service attack and modification. However, connectionless integrity services can only ensure that messages are not modified.

There is a difference between integrity without recovery and integrity with recovery.

Integrity services relate to the detection rather than prevention of active attacks. If attacks are detected, the service will only report this violation and not recover from the attack. Other alternative mechanisms can be used to recover from the loss of integrity. For example, automated recovery systems are a more alternative approach in general.

Origin Integrity The concept of origin integrity as a subcategory of data integrity pertains to a mechanism that ensures that an intended recipient can prove or verify the originator's identity when information is transmitted across a channel. A typical example of such a system is an electronic-mail system. When a sender transmits an email to a particular recipient, the recipient can verify that the email is legitimate by confirming the expected claimant email address. For simplicity, this service provides proof of the integrity and origin of a message; neither the sender nor the receiver can deny a transmitted message. This service may also be referred to as non-repudiation of data.

Authentication This service assures that communication is authentic. In a case of a single message, such as an intrusion detection system (IDS) alarm signal, the purpose of the authentication service is to assure the recipient that the message is from a legitimate source. This service can also be seen as the authentication of network participants, which is the collaboration of the identity that a person can claim a formal assurance of a trusted third party. Authentication is essential to make certain non-repudiation of network users and network components.

2.1.3 Data Availability

The availability of a system can be defined with the RFC 4949 and X.800 services. This service enables system resources to be accessible and usable to authorised entities by performance specifications for the system. There are various kinds of attacks that can render system resources unavailable. Some of these attacks can be mitigated with countermeasures such as encryption and authentication, though other attacks require physical activity to prevent the unavailability of resources. This service resolves the security concerns of denial-of-service attacks.

Access Control Access control in the context of network security is the ability to control the privileges to host applications and systems through communications channels and links. In order to achieve access control, each individual that needs access to a system must be identified through authentication.

2.2 Steganography

The word “Steganography” originated from two Greek words, steganos, meaning “covered, invisible or concealed”, and graphein meaning “writing”. Steganography is a technique that covers or camouflages the message’s existence by using a cover message to embed a secret message that is to be transmitted. Steganography can also be referred to as the science of invisible communication [58] [73] [166]. In contrast, encryption is a technique that converts plaintext to ciphertext. This technique hides or encrypts the message from attackers but not the message’s existence.

Modern steganography is on the increase, driven by the digital age and used for legitimate and illegitimate purposes, which include: DRM, copyright, watermarking and espionage, crime, activism, malware, respectively. Indicators show that the proliferation of data hiding tools, such as "Android Data Hiding Tools", is in use but difficult to prove. If deployed effectively, steganography can overcome the limitations of encryption [106] [183] [80]. In the following section, 2.3, the steganographic schemes used in developing the protocol in Chapters 5 and 6 of this thesis are discussed. The proposed steganographic protocol is a synthesis that combines steganography by cover synthesis and steganography by cover selection. At first, section 2.3 briefly discusses the concept of digital steganography in-network computing environment.

2.3 Digital Steganography

Information and computing technology have made concealing private information more feasible and challenging to access by unauthorised personnel. Digital steganography can be defined in various ways. It can be defined as the science and art of using digital media to hide or cover private or secret digital information. It can also be defined as the science of hiding sensitive data in digital format or media such as text, image, audio, and video-based [73] [206]. Steganalysis is the science of uncovering embedded or private messages, just like steganalysis systems are used to detect stego data in an image [73].

Modern techniques in steganography use powerful steganographic software tools to conceal information. However, the application of steganography has attracted great interest in government and commercial organisations. Commercial institutions that wish to protect their data-related assets from piracy have shown interest in utilising steganography. Today, steganography is often used to secure and transmit data safely in images and music to ensure copyright.

For steganography to be deployed effectively, a performance triangle needs to be considered. The performance triangle includes secrecy, capacity and robustness. This performance triangle separates steganography from encryption. To attain secrecy, the effectiveness of concealment must be attained. For adequate capacity, storage space limitations for confidential data within a cover medium must be considered. This notion is important because one needs to consider what happens to the cover medium if a capacity threshold is exceeded. Robustness considers the limitations, vulnerabilities and thresholds of a carrier medium.

In this thesis, essential components that define steganographic communication is discussed. Consider the following example: Alice and Bob want to communicate secretly, although both of them must agree on an essential proceeding to communicate (Protocol) their secret messages. Specifically, both communicating entities need to hide their secret message with some type of cover medium. They also need to respectively design algorithms necessary to hide and extract their secret messages. In order to increase security, both algorithms need to be dependent on a secret key (stego-key) known only by Alice and Bob. Besides the type of cover the internal workings of the algorithm, an authorised entity's capacity (For example, Eve) to detect the secret communication depends on the size of the message. Finally, Alice and Bob will transmit their messages through a channel controlled by the warden (Eve). Eve may or may not interfere with the communication. In digital steganography, the following are basic terminology is used:

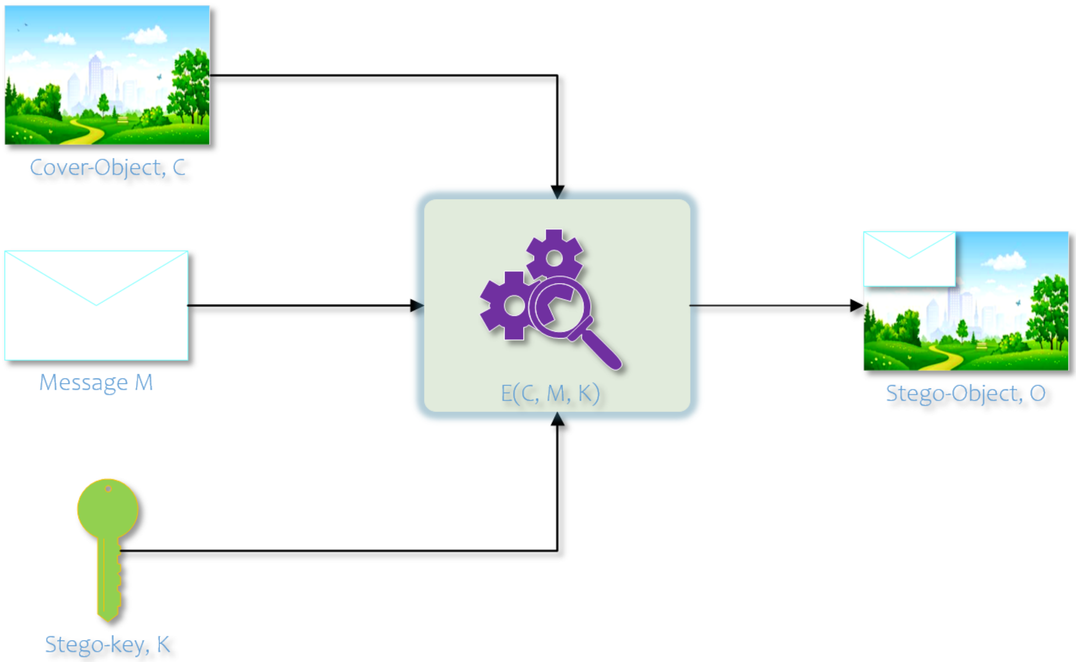


Figure 2.2: Component of a standard-stego system.

- **Cover Media:** The cover media is the carrier in which the secret data is hidden such as an image file.
- **Payload:** The secret data to be hidden in cover media.
- **Stego-Media:** The media with embedded payload.
- **Steganography:** The process using which the payload is embedded in the cover media.
- **Steganalysis:** An attack on stego-media using which the hidden payload is to be extracted from it.

Some forms of steganography are analogous to camouflage [180]. At times, they often rely on exploiting a weakness to be successful. Steganography has different techniques:

text, image, audio, and video-based. These techniques have different approaches, including steganography by cover selection, cover synthesis, and cover modification.

2.3.1 Steganography by Cover Selection

In this method, a sender has a database of images available, which can communicate a secret message. A bit of data could be transmitted by using a picture. For example, a picture with the presence of a cat in a portrait could have covert meanings such as "attack at dawn". The steganographic encoding algorithm can work by simply drawing images randomly from the database until a suitable image can communicate the desired message. Here, the stego-key is the set of principles that tell both the sender and receiver how to interpret the images.

Another case of steganography by cover selection involves hash functions. A sender can select an image from a database and apply a hash function. If the hash matches the desired message bitstream, the image is transmitted to the receiver; the sender selects a different image until a suitable match is obtained.

2.3.2 Steganography by Cover Synthesis

The sender can create a cover that conveys the desired message in steganography by cover synthesis. An interesting example is a text that involves the cover rather than a digital image so that the text can look like legitimate spam. The sender uses the fact that spam often has unusual wording, which can be used to embed a message. SpamMimic (www.spammimic.com) utilises mimic function to encode messages in an artificially created spam-looking stego text.

In exceptional cases, steganography by cover synthesis could be combined with steganography cover selection to alleviate the exponential complexity of embedding by hashing [168]. This thesis combines steganography by cover synthesis with steganography by a cover modification to form a new system, and the approach is presented in chapter 5 of this thesis.

2.3.3 Steganography by Cover Modification

Steganography by cover modification is the most studied and widely used approach. A specific example of this approach is the List Significant bit (LSB) technique. The most popular steganographic algorithms used to implement the LSB technique are the jsteg, F5 and the ± 1 embedding. Eminent research [95] [92] in this area use information theory, Complexity-theory and cryptographic concepts to formulate the theory of steganography by cover modification. Here, the sender uses a cover medium (image) and modifies that image so that confidential data such as text can be hidden. Both the sender and the receiver can work a set of all possible messages and keys that could, in most cases, depend on specific covers:

$$\mathcal{C} \text{ is the set of cover objects } c \in \mathcal{C},$$

$$\mathcal{K}(c) \text{ is the set of all stego keys for c},$$

$$\mathcal{M}(c) \text{ is the set of all message inc}$$

$$\mathsf{Enc} : \mathcal{C} \times \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C},$$

$$\mathsf{Dec} : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M},$$

such that for all $c \in C$, and all $k \in K(c), m \in M(c)$,

$$\mathsf{Dec}(\mathsf{Enc}(c, k, m), k) = m.$$

The sender can use any suitable cover-medium $c \in C$ and encode m in it. The number of messages that can be communicated in a specific cover x depends on the steganographic scheme and it may also depend on the cover itself.

2.4 Mobile Payments

2.4.1 Reference Model for Mobile Banking

With the advancement of information and communication technology (ICT), access to services and competition have pushed banks to introduce mobile banking services. These services have led to the development of various mobile banking models, which can be classified into the following models [205]: Mobile Service Provider-led, Third-Party Service Provider Model, and Bank-led Model. In this thesis, the Bank-Centric Model will be mainly considered, focusing on SMS banking. In this thesis, the Bank-Centric Model is used to develop the protocol considering the bank is trusted; all payment routes and operations are centralised at the bank; this is further explained in Chapters 5 and 6 of this thesis. Although the Mobile Service-led Model and the Third-Party Service provider Model are not used in this thesis, it is essential to discuss them briefly.

Bank-Centric Model In this Model, the bank controls the whole payments process leaving the transport and network functionalities to the mobile operators. This Model uses the technical and financial capabilities of a fully developed financial system. This system's functionality can translate into the usage of dual-slot mobile phones, where one SIM slot is used for mobile banking while the other is used for telecommunications. Though, banks need to ensure the protection of all mobile network operators and customers in a given market. In the event the customer mobile phone is lost or stolen, banks may depend on or collaborate with the mobile operator to deactivate the application.

Mobile Service Provider-led Model In this Model, all operations are centralised at the mobile network operators. The chip installed on the mobile phone handles both financial and security aspects. The mobile operator pays the merchant, and when customers make purchases, credit is extended to them at the end of the billing process with a small transaction fee. A solution such as this is specifically suitable micropayments, as seen in the instance of a popular mobile internet service in japan known as i-mode®. Underdeveloped financial institutions can also use this system in terms of quality, considering it takes advantage of the mobile network reaches in rural areas.

The merchant and purchaser are restricted to the same network. In the case of the banks, there are a few dangers in giving the mobile network operator exclusive privilege to customers. In this thesis, the Mobile Service-led Model is not considered in developing the protocol developed in Chapters 5 and 6 considering they are not to be trusted. This Model is not considered for the reason that the mobile network service operators are participating in mass phone surveillance, which includes logging text messages and phone calls. In Chapter 5, the System Model in section 5.5 presents the rationale for the lack of trust in the Mobile

Service-led Model.

Third-Party Service Provider Model The Third-Party Service Provider Model is an independent service provider that acts as a trusted entity to manage the security credentials. In some instances, it may provide private currency to settle the accounts. The significant responsibility of this Model is to bridge the mobile network operators and providers (for example, banks.). During a purchase, credits the merchant's account by debiting the purchaser's account. This Model gives some independence to the customer from the mobile network operators or the bank. The protocol presented in Chapters 5 and 6 is a cost-effective solution designed to operate in rural areas or poor infrastructural environments; therefore, using a trusted third party is not considered as this would introduce additional and unnecessary costs to deploy.

There are some risks associated with the Third Party Service Model. Some risks could be considered in a case where a service provider pays a merchant before the customer payment is settled. On the other hand, the service provider will bear no risk if the customer payment must be cleared before merchants are paid.

2.5 Mobile Banking Applications

Messaging-based Applications. There are various SMS mobile banking services that banks offer in order to enable flexibility of financial and non-financial transactions to customers. The services offered include the PUSH and PULL SMS mobile banking services. Although SMS messages are, by default, designed to transmit non-sensitive messages over

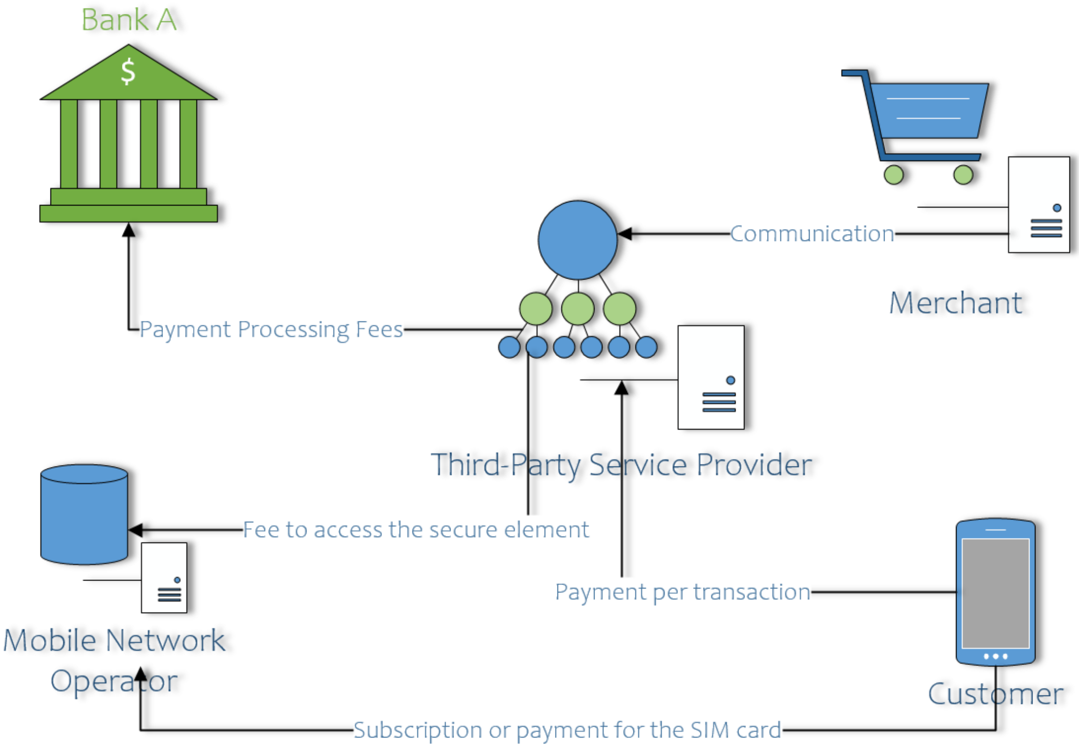


Figure 2.3: The Third Party Service Provider Model

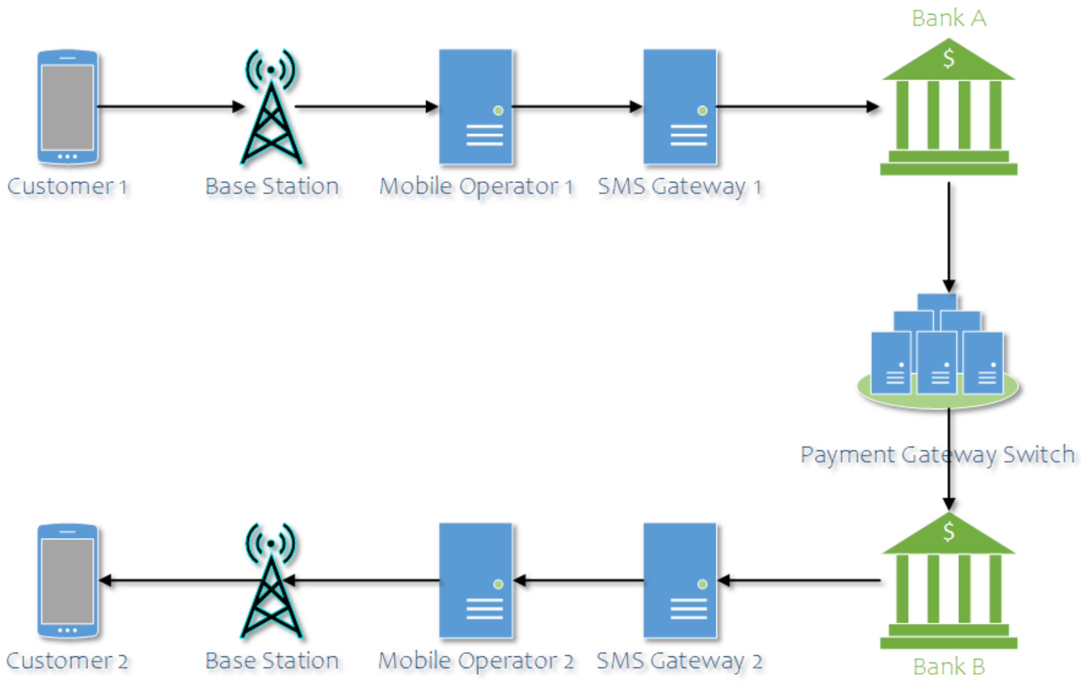


Figure 2.4: SMS banking Architecture

the communication network and the SMS encryption used for transmission is not secure, this, however, potentiality leads to various threats that have been identified and discussed by various scholars.

In SMS banking, customers can perform financial transactions such as bill payment, balance payment and account transactions. With the use of secure text messages through a mobile or cell phone. In this banking system, the details about a customer's credit card in the SIM card and an installed payment application is given by the mobile operator. There are two methods of SMS widely used in today's applications: the PUSH SMS and PULL SMS messages.

The PUSH SMS messages are inquiry-based services that enable text messages to be sent from the bank to the customer's mobile phone without the customer initiating a request for information. For example, a customer can receive a withdrawal alert from the bank whenever a transaction is performed. The PULL SMS messages are transaction-based services that enable a customer to use a mobile device or phone and send a request to the bank to obtain financial information or perform a transaction. This messaging application is a full-duplex communication system where a customer sends a request to the bank, and the bank replies to the information sought by the user. For example; when a customer makes an account balance enquiry, such is considered a PULL SMS message [23], [213], [214]. This thesis is focused on the use of the messaging based application.

Web-based Applications. The mobile device uses a browser interface to display HTML generated by server-based applications. Data processing is done solely on and by the server in the browser-based application, and this means that there is no need for third-party software and significant processing power on the mobile device. Web-based applications are reasonably suitable for mobile devices with low processing power and memory. Additionally, the interaction between the user and the application is simplified by the predefined browser graphical interface [225].

Client-based Applications. This approach requires a mobile banking customer to download software (mobile app) on a mobile device. The entry of transaction details can be prepared offline. Once all crucial information is imputed in the software, a server connection is established, and then data is transmitted. Security measures take place employing PINs and TANs before data transmission. Client-based applications are attractive because a significant part of the banking process is conducted offline, reducing online connection time and cost [225].

2.6 Entities in Mobile Banking

2.6.1 Banks

Banks have continued to upgrade their infrastructure to accommodate new banking techniques and security methods in response to the growth and development of online and mobile commerce. Various banks have managed several generations of software and hardware. In general, many information technology infrastructures of the bank had continued to include subsystems that are outdated. Studies estimated that the information technology infrastructure of banks globally spends about 70%-87% on maintaining outdated systems. Banking interconnecting elements might mask this heterogeneous system at the cost of inefficiency and complexity. Though, at the time being, to put pressure on traditional organizations, startups unburdened by outdated systems are free to explore new ways and experiment with novel ideas.

Online access to the bank has highly increased. For example, banking customers regularly check their account balances from smartphones and tablets, which could be overburdened on systems designed for less frequent requests. Banking disruption such as a shutdown of the Royal Bank of Scotland in 2012 could frustrate millions of customers from accessing their bank accounts. Furtherly, if the increase of cryptocurrencies such as Bitcoin becomes highly adopted, the role of banks may change radically.

In retort, more than a few established banks have started offering cloud storage to corporate clients, while others have partnered with technology companies to improve their services.

2.7 Summary

This chapter introduces essential security concepts such as confidentiality, integrity, and availability. This chapter also introduced an overview of steganographic schemes and core concepts used in developing the protocol in Chapters 5 and 6 of this thesis. In digital steganography, this chapter introduced the three approaches to implementing steganography: steganography by the cover selection, steganography by cover synthesis and steganography by cover modification—furthermore, mobile payments, mobile payments, mobile banking applications and entities in mobile banking were presented. Chapter 3 of this thesis presents the vital cryptographic security definitions and terminologies considered in developing the contribution.

Chapter 3

Security Definitions and Terminologies

In this chapter, the cryptographic security definitions and terminologies are presented used throughout this thesis. Since the contributions described in Chapter 5 and 6 of this thesis are concerned with confidentiality, privacy and integrity controls of SMS banking transactions, the definitions described in section 3.1 -3.4 are confidentiality and privacy concepts that needed to understand the remaining chapters of this thesis. This chapter presents cryptographic terminologies such as encryption, hash functions, semantic security, Secret Sharing and anonymity concepts. Also, this chapter presents concepts in game theory such as the non-cooperative game theory, strategies in normal-form games as well as solution concepts in game theory. For the basic cryptographic notions presented in this chapter, more details can be found in [142].

3.1 Cryptographic Definitions

Negligible Function: A function $f(\cdot)$ is considered to be negligible if a polynomial $p(\cdot)$, and a function $f(\cdot)$ is bounded by $p(\lambda)^{-1}$ in the security parameter λ..

Symmetric-key Encryption: A symmetric-key encryption system Π constitutes of three algorithms:$\{\mathsf{keyGen}, \mathsf{Enc}, \mathsf{Dec}\}$

- On the input of a security parameter λ, the $\mathsf{keyGen}(\lambda)$ returns a key (k).
- The $\mathsf{Enc}_\mathsf{k}(\cdot)$ takes a key k and a secret message $m \in \mathcal{M}$, and returns a ciphertext $c \in \mathcal{C}$.
- On the input of a key k and correct c, the $\mathsf{Dec}_\mathsf{k}(\mathsf{c})$ will return m, otherwise $\perp$ is returned.

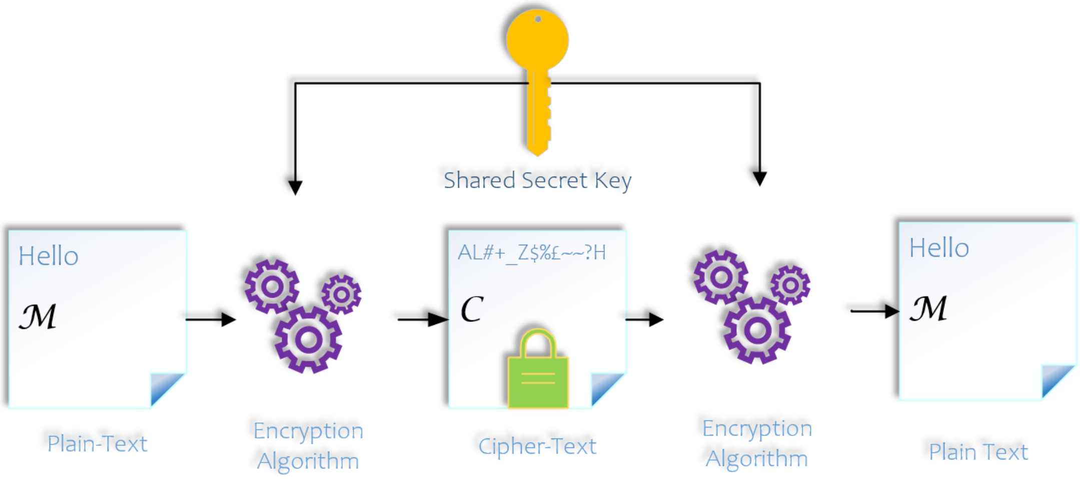


Figure 3.1: Symmetric Key Encryption

Public-Key Encryption: A public-key encryption system PKE constitutes of the following algorithms:{keyGen, Enc, Dec}

- On the input of a security parameter λ, the $\mathsf{keyGen}(\lambda)$ returns a set of public keys (pk, sk).
- The $\mathsf{Enc}_{\mathsf{pk}}(\cdot)$ takes a public key pk and a secret message $m \in \mathcal{M}$, and returns a ciphertext $c \in C$.
- With the correct secret key sk and correct c, the $\mathsf{Dec}_{\mathsf{sk}}(\mathsf{c})$ will return m, else $\perp$ is returned.

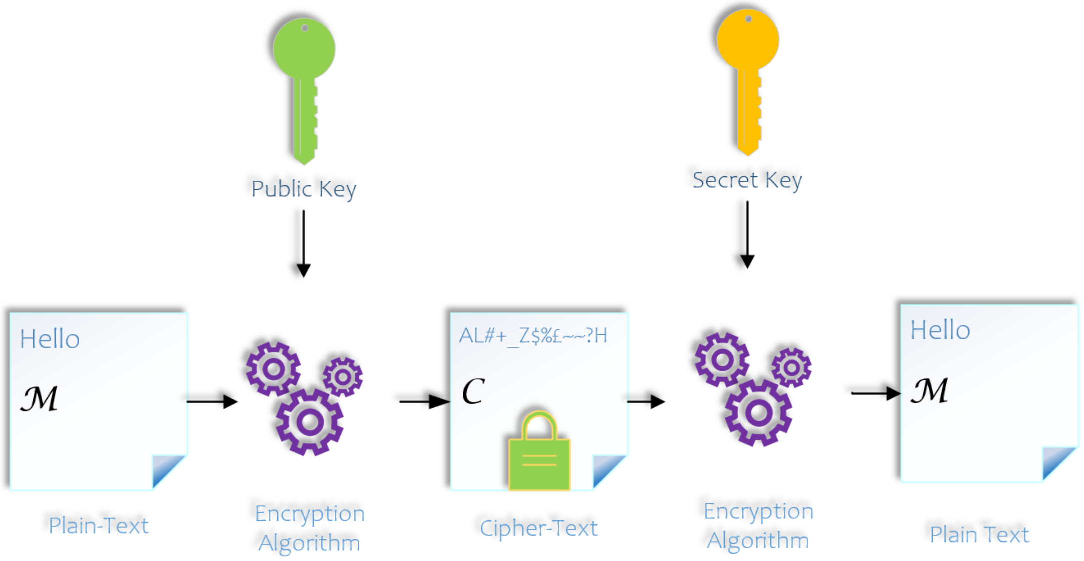


Figure 3.2: Asymmetric Key Encryption

Pseudo-Random Functions: A pseudo-random function (PRF) is a deterministic efficient algorithm that uses a key k and a string of n-bit length $x \leftarrow \{0,1\}^n$ and returns an n-bit string $y \leftarrow \mathsf{PRF}_k(x)$, this makes impossible to distinguish y from a truly random output. To simplify, $\mathsf{PRF} : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$.

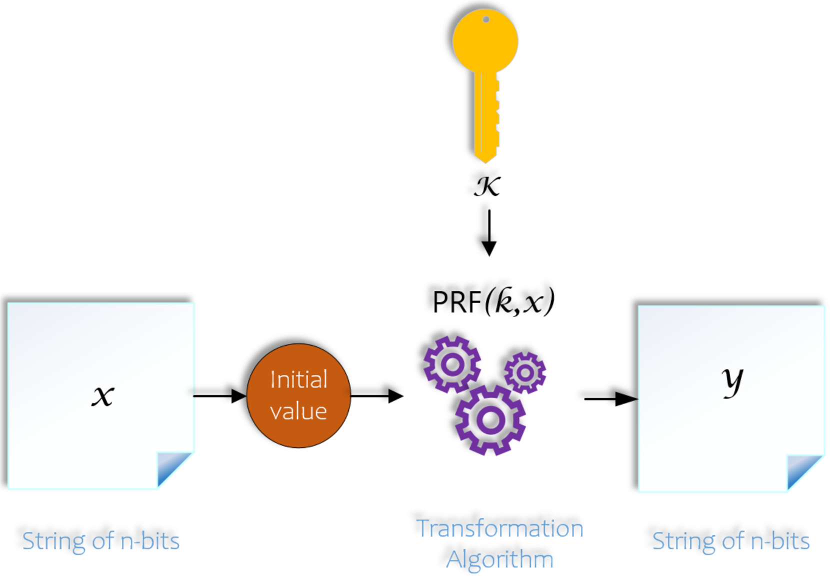


Figure 3.3: Pseudo-Random Function

Hash Functions: A cryptographic hash function $H(\cdot)$ is a suitable algorithm that takes as an input, a variable length of message or bit string $m \in \mathcal{M}$ maps it into a fixed length l $s.t : \{0,1\}^* \longrightarrow \{0,1\}$, simply $m \leftarrow H(m)$.

Universal Hash Functions: A random algorithm $\mathcal{H}$ is universal if it can be used for constructing hash functions $h : U \longrightarrow \{1, \ldots\ldots, M\}$ if for all $x \neq y$ in $\mathcal{U}$. Also, a set of hash functions $\mathcal{H}$ is considered universal if the methodology used in choosing $h \in \mathcal{H}$ at random is universal.

(HMAC) Hash-Based Message Authentication Code: Unlike the MAC function, the HMAC is a particular kind of message authentication code that involves the combination of a private key and cryptographic hash function as input. The output is a fixed length which provides data integrity, as a MAC would, $HMAC_K(m \in \mathcal{M})$.

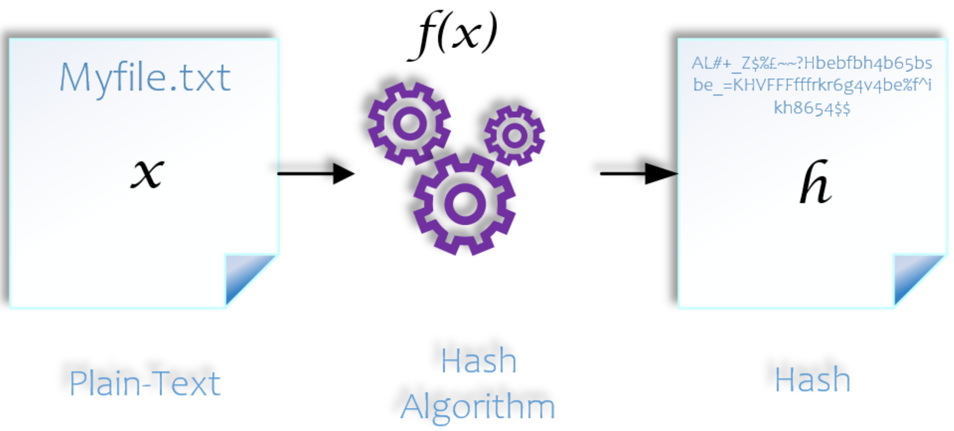


Figure 3.4: Hash Function

3.2 Security Definitions and Polynomial Security

It is challenging to use arguments in information theory to prove the security of most cryptographic background terminologies. Though, security in cryptographic systems or settings can be bound to the complexity of mathematical tasks. This reason is due to the presumption that no algorithm could solve this task in polynomial time with a probability of negligibility. The secure scheme of Chapters 5 and 6 is described by showing that a probabilistic adversary has a negligent advantage in breaking the steganographic protocol under certain conditions. Consequently, it is essential to introduce some general security concepts relevant to this thesis. The security definition such as indistinguishability is applied to the contributions of Chapters 5 and 6 of this thesis.

Semantic Security: Throughout this thesis, a cryptographic system is considered secure semantically if the property of indistinguishability for a ciphertext and message holds.

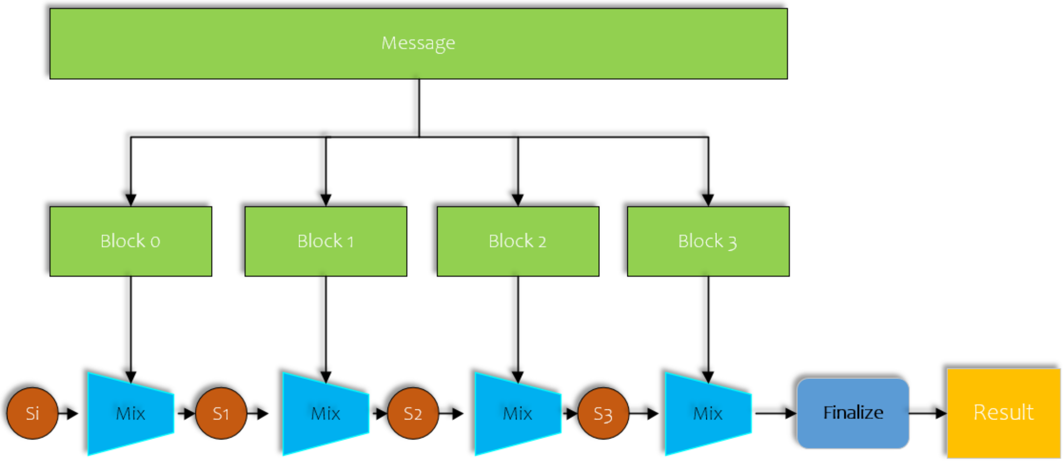


Figure 3.5: General Purpose Hash Function Algorithms

Definition 1: (*Message Indistinguishability*). A cryptographic system $S(\cdot) : C \longleftarrow S(\lambda, m)$ is said to be indistinguishable if a *probabilistic polynomial time (PPT)* $\mathcal{A}$ is unable to distinguish between the outputs of $S(m_1)$ and $S(m_2)$ plus a non-negligible function ϵ. It should the following:

$$|P[\mathcal{A}(C_1 \leftarrow S(\lambda, m_1)) = 1] - P[\mathcal{A}(C_2 \leftarrow S(\lambda, m_2)) = 1]| \leq \epsilon$$

Definition 2: (*Ciphertext Indistinguishability*). A cryptographic scheme $S(\cdot) : C \longleftarrow S(\lambda)$, is said to be ciphertext indistinguishable if no *probabilistic polynomial time (PPT)* adversary $\mathcal{A}$ is able to distinguish the output of $S(\lambda)$ from any random value $r \longleftarrow \{0, 1\}^{\lambda}$, with non-negligible probability.

$$|P[\mathcal{A}(C_1 \leftarrow S(\lambda)) = 1] - P[\mathcal{A}(r \overset{r}{\leftarrow} S\{0, 1\}^{\lambda}) = 1]| \leq \epsilon$$

Key-Privacy: Public key privacy was initially defined in [27] as the indistinguishability property of public keys used for encryption. It is used most in particular to identify the public key encryption defined as follows.

Definition 3: (*key-Privacy*). A public key encryption system $Enc_{pk}(m) \longrightarrow c$, is key private if any adversary bounded in polynomial time (PPT) $\mathcal{A}$, with ingress to the keys $\{pk_1, pk_2\}$ is unable to distinguish the output c_i of $Enc_{pki}(m)$ when using pk_1 and pk_2 such that $i = \{1, 2\}$, with non-negligible probability.

Cryptographic Random Oracle: A cryptographic random oracle O is a mathematical function chosen at random that maps any input $O(x)$ to a fixed random output h with a uniform distribution. They are used for an ideal replacement of a hash function where randomness is needed. $h \leftarrow O(x)$ [17]. A cryptographic random oracle can also be seen as a theoretical black box that responds to every unique query with a truly random output in its output domain. If queried the same input repeatably, it gives the same output [28].

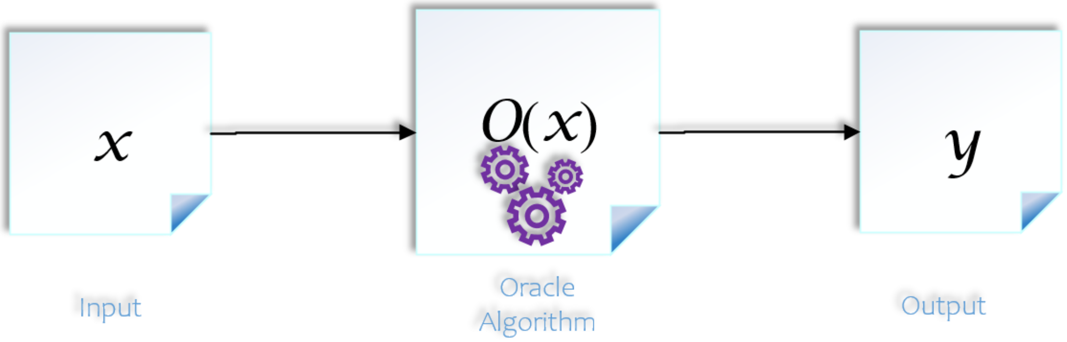


Figure 3.6: Cryptographic Random Oracle

Secret Sharing: The idea of secret sharing was initially proposed by Adi Shamir [203]. The idea of the secret sharing scheme is to divide a secret S into n shares amongst n individuals, in a way that each individual does not gain information about S. By combining their shares the secret S can be constructed. However, knowledge of any piece or more than pieces can reconstruct S. This can be achieved through the $t \leq n$, where t is the threshold. Any individual with t or more piece of the secret S can reconstruct $f(n)$ using Lagrange Interpolation.

$$S = \sum_{ai,si}$$

for

$$ai = \prod_{j \neq i} \frac{j}{j-i}.$$

3.3 Anonymity

Encryption techniques provides confidentiality of private content, though it does not directly provide anonymity. Techniques such as traffic analysis can be used to track and identify users communicating without their knowledge. Although, it is a challenging task to provide definition of anonymity. Pfitzmann and Köhntopp [169] defined anonymity as follows.

Definition 3.3.1. *"Anonymity is the state of being not identifiable within a set of subject, the anonymity set".*

The entity e_i is considered anonymous if and only if it is difficult to e_i in the set

$\mathcal{E} = \{e_i, ..., e_N\}$, such that, $N = |\mathcal{E}|$. Hence, an effort to quantify anonymity in communications, the study in [200] and [60] propose the use of entropy within the anonymity context. Although the initial technique in [200] allows for the measurement of an anonymity set, while the latter technique in [60] enables a classification of the anonymity degree within an interval from 0 to 1. Let $H(x)$ be the entropy of a random variable x such that, $p_i = \mathsf{P}[x = i]$ for the anonymity set $\mathcal{E}$, then the effective size of the anonymity set $H(x)$, and the degree d of the anonymity are calculated, individually, as:

Definition 3.3.2. *(Anonymity Size [200]). Given an anonymity set* $\mathcal{E} = \{e_i, ..., u_N\}$*, s.t.,* $N = |\mathcal{E}|, e_i \in \mathcal{E}$*, and considering* $p_i = \mathsf{Pr}[x = i]$ *as the size probability distribution of* u_i *among all users in* $\mathcal{S}$*. Then, the effective anonymity is computed as follows:*

$$H(x) = -\sum_{i=o}^{i=N} pi \cdot log_2\, pi.$$

Definition 3.3.3. *(Degree of Anonymity [200]). Given the anonymity set for the set* $\mathcal{S}$*. The degree d of anonymity of* $\mathcal{S}$ *is calculated as follows:*

$$d = \frac{H(x)}{H_{max}}$$

for

$$H_{max} = log_2 N.$$

Unlinkability: In a secure system, a secret is considered unlinkable if an adversary is inadequate in mapping two or more pieces of that secret to a single user. For example, if Alice publishes m_1 and m_2, and publishes m_3 later, though, an adversary with a preceding knowledge of m_1 and m_2 is incapable of linking m_3 to Alice.

Pseudonymity: This concept is considered as a state where a user can substitute their identities with a distinct identity known as a pseudonym. However, this is used for anonymizing real identities, the utilization of single pseudonyms can lead to distinctive identifiers. As a consequence, systems with anonymity capabilities normally apply a limited random pseudonym for a single connection to achieve unlinkability by pseudonymity.

Unobservability: This cryptographic concept is closely related to indistinguishability as it designates the state where an action executed by a user is indistinguishable from any other action of the same type from the same or another user. Consequently, it is difficult to distinguish the action from any other random action. At most times, unobservability implies anonymity [169].

3.4 Game Theory

This section presents terminologies in game theory that are relevant to this thesis. The concepts presented in this section are the definition of game theory, its mechanisms, representations and the solution concept used for game theory analysis.

3.4.1 Overview

Game theory can be seen as an analytical tool used to aid in comprehending the phenomena observed in decision making. The general presumptions, in theory, are that decision-makers use objectives that are considered rational. They also consider that their knowledge and expectations of the other decision counterparts are strategic. Game theoretical models are abstract depictions of classes of real-life situations which enables a wide range of phenomena to be studied. Game theory uses mathematics to express its ideas formally. This thesis focuses on the more studied game theory, called non-cooperative game theory in standard forms.

3.4.2 Non-cooperative Game Theory

Utility Theory. The best approach to model an agent interest is utility theory. This theory focuses on quantifying an agent's degree of a greater liking for one alternative over another set of available alternatives. Also, the theory aims to comprehend how these preferences change when an agent faces uncertainty about which alternative he will receive.

Utility Function. When referring to a utility function, it is a mapping from states to real numbers. These numbers can be interpreted as measures of an agent level of happiness in a given state. When an agent is faced with uncertainty about the state he faces, his utility can be defined as the expected value of his utility function for the suitable probability distribution over states.

Normal form games The standard form is the most familiar representation of interactions that are considered strategic in game theory. Games represented in this form are summed up to represent every agent's utility for each state.

Definition 3.4.1. *(Normal-form game:) A standard form game is a finite ordered list of elements* (N, A, u)*, where:*

- N is finite set of n players, indexed by i;
- $A = A_1 \times \cdots \times A_n$, where A_i is a finite set of actions available to player i. Each vector $a = (a_1, \cdots, a_n) \in A$ is called an action profile;
- $u = (u_1, ..., u_n)$ where $u_i : A \mapsto \mathrm{R}$ is a real-valued utility (or payoff) function for player i.

A natural way to represent games is via a n-dimensional matrix. For the first player, each row has a close similarity to a possible action. Each column correlates to a viable action for the second player. Each cell corresponds to a single viable outcome with the first player listed from the inceptive.

3.4.3 Strategies in normal-form games

A pure strategy is defined as selecting a single action and using that action in the game. The choice of pure strategy for each agent is called a pure strategy profile. However, players can use another type of strategy called a mixed strategy. This approach can be made by randomizing over a set of actions available using some probability distribution. It might not be obvious why an agent would want to introduce a random phenomenon, though the multiagent environment plays a critical role in mixed strategies. The mixed strategy is defined as follows.

Definition 3.4.2. *(Mixed strategy) Let* (N, A, u) *be a normal-form game, and for any set* X *let* $\prod(X)$ *be the set of all probability distributions over* X*. Then the set of mixed strategies for player i is* $S_i = \prod(A_i)$.

Definition 3.4.3. *(Mixed-strategy profile) The set of mixed-strategy profiles is simply the Cartesian product of the individual mixed-strategy sets,* $S_1 \times \cdots \times S_n$.

It is essential to note that a pure strategy is considered a special case of a mixed strategy, in which the support is one action only. Though, when it comes to a mixed strategy, it is considered entirely mixed if it has complete support (i.e. if a nonzero probability is assigned to all actions). The mixed strategy is a straightforward concept, and it depends on the rudimentary notion of decision theory-*expected utility*. Initially, the probability of reaching each outcome of a strategy profile needs to be calculated, and secondly, the average of the payoffs of the outcomes needs to be calculated. The expected utility is defined as follows (here, the notation u_i is used for both expected utility and utility).

Definition 3.4.4. *(Expected utility of a mixed strategy) Given a normal-form game* (N, A, u), *the expected utility* u_i *for player i of the mixed-strategy profile* $s = (s_1, ..., s_n)$ *is defined as*

$$u_i(s) = \sum_{a \in A} u_i(a) \prod_{j=1}^{n} s_j(a_j).$$

3.4.4 Solution Concepts in Game Theory

This subsection presents how games can be seen from an individual player's point of view, preferably from the perspective of an outsider observer. By doing so, it is a guide to the Nash equilibrium solution concept in game theory.

The only observation is that if a player knew the strategy that other opponents would play, his strategy would be simple. More specifically, he would be left with the only one-agent problem of choosing a utility that will maximize his action. In a formal setting, define $s_{-i} = (s_1, ..., s_{-i}, s_{i+1}, ..., s_n)$, a strategy profile s that has no player i's strategy. Thus, it can be written as $s = (s_i, s_{-i})$. Suppose the players besides i were to commit to a strategy s_i, an agent i of utility-maximization could be faced with the problem of determining his best response.

Definition 3.4.5. *(Best Response) The best response of Player i's to the strategy profile s_i is a mixed strategy $s_i^* \in \mathcal{S}_i$ such that $u_i(s_i^*, s_{-i}) \geq u_i(s_i, s_{-i}) \forall$ strategies $s_i \in \mathcal{S}_i$.*

Indeed, the best response is not essentially unique, except in cases in which a unique best response is a pure strategy, the number available best response is infinite.

Conventionally, a player is unable to know what strategies other players would adopt. The idea of best response is not a solution concept though it identifies an important and interesting set of outcomes. The notion of best response can define the most central idea in a non-cooperative game theory known as the Nash equilibrium.

Definition 3.4.6. *(Nash Equilibrium) A strategy profile $s = (s_1, ..., s_n)$ is a Nash equilibrium if, for all players i, s_i is a best response to s_{-i}.*

The Nash equilibrium is a stable strategy profile where no player would want to change their strategy if he knew his opponents' strategies. The Nash equilibrium can be divided into two categories, strict and weak. The pure strategy Nash equilibrium can either be weak or strict depending on the game, while the mixed strategy Nash equilibrium is essentially weak.

Chapter 4

Literature Review

The academic research environment has been motivated by the mobile banking system, with a security interest. This interest has led to a significant amount of studies aiming at protecting the privacy and security of mobile banking subscribers and infrastructure. Some of these architectures and protocols suggested providing end-to-end security in the application and transport layer. Though, a few scholars proposed changing the network infrastructure, while others designed protocols that retained the original network infrastructure. In this chapter, various literature relevant to the proposals of Chapters 5-7 is discussed. The literature presented is divided into six sections. At first, the security issues and attacks in the short message service (SMS) are discussed in section 4.1. Secondly, section 4.2 discusses the security vulnerabilities of Mobile Network Algorithms and Protocols. The following section, 4.3, presents techniques used to secure the transmission of SMS. These techniques include secure SMS protocols based on encryption and steganography, respectively. Section 4.4 presents SMS banking approaches based on encryption and steganography, which researchers have proposed. Also, the specialised multi-channel Online Social Network (OSN) protocols, from which the contribution of this thesis is inspired mainly, are discussed. Finally, we present security games based on steganography in section 4.5.

4.1 Security Issues and Attacks in SMS

SMS stands for short message service, and it is a GSM service used to transmit text messages up to 160 characters of 7-bit encoding. SMS messages are transmitted to a receiver through the short message service centre (SMSC). The plain-text is the default format of SMS messages, and end to end encryption is not currently applicable, enabling SMS vulnerable to attacks [196], [44]. The security of SMS is very critical because attacks can be carried out remotely without any user interaction. On low powered mobile phones, SMS filtration options are not available. During the development of the GSM system, the SMS service was designed for users to transmit non-sensitive messages over the GSM network. Security services and considerations such as data confidentiality, authentication, non-repudiation and end to end security were not inclusive to the SMS services. This subsection discusses the security problems with SMS service.

Mobile Station (MS) Vulnerability The mobile station is vulnerable to misplacement and theft. If an adversary could break into a mobile station (cell or mobile phone), sensitive content stored on the phone can be compromised or stolen. This attack also applies to

SMS messages. Theft is very dangerous even if the entire SMS communication channel or network is encrypted; the decrypted SMS messages are stored in the SIM card.

A5 Encryption Vulnerability SMS messages are transmitted in plain-text format. The GSM network does not offer end-to-end security. The only security mechanism available offers encryption between the base transmission station and the SMS bank server during transmission. The only encryption algorithm used is the A5 which is considered insecure, reverse engineering and verified to be insecure. The A5 algorithm has two main types, namely A5/1 and A5/2. Three possible attacks could be achieved in a few seconds with a personal computer on the A5/1 version commonly used in Europe. The A5/2 variant was also cracked in less than a day. This shows how the GSM system is vulnerable to cryptanalysis attacks. For authentication, the GSM systems commonly use the A3/A8 algorithm. However, there are different flaws in this algorithm that can be broken. They were able to obtain the secret key hence making SIM cloning possible [107, 44, 167, 31].

SMS Spoofing Attack An attacker can inject SMS messages into the SMS network with spoofed originator IDs. The SMS spoofing attack can be performed in two ways. One way is to impersonate the authentication server (AS) for an authorised mobile station (MS). The other way is to impersonate the mobile station (MS) for an authorised (AS).

SMS Replay Attack There is a possibility that an attacker could replay SMS messages by sending an authentication request and authentication response messages. However, replaying an authentication response could be a more severe vulnerability. At times it is not obvious to detect an attack of an authentication request message to be replayed. If a replay attack is possible, it could be used to impersonate an authorised user and authenticate a false transaction. However, this attack cannot work if an authentication request number can be used for an anti-replay mechanism that must be included in the response.

Man In The Middle Attack SMS messages are sent across the network channel between the mobile station (MS) and the base station (BS). In most GSM networks, all data traffic transmitted across the network channel is encrypted. Although the choice of encrypting or transmitting messages in plain text is specific, and it is in control of the Base Station Subsystem (BSS). In some countries, SMS encryption is not allowed. However, the choice of using an encryption algorithm must be precise, and it must be of two GSM specific known as the A5/1 and A5/2, which is vulnerable to attacks like eavesdropping. If the network is unencrypted, the attacker can read messages and decrypt the traffic. Intercepting messages is straightforward and assuming there is no suitable encryption implemented, the attacker would have trouble intercepting transmitting messages and linking messages to the transaction of interest.

SMS Service Centre Attack The storage of copies of SMS messages at the SMS centre server hosted by the mobile network service provider also provides a vulnerability vector to the SMS banking service. Since the message is in plain-text, then any personnel who have access to the SMS centre server can easily view sensitive details.

Silent SMS Denial of Service (DoS) Attack A denial of service (DoS) attack is an attack that enables an adversary to attempt making a legitimate user computer resource unavailable. A well-known technique is to prevent legitimate packets by flooding the computer network with a large data packet. A typical target for such an attack is high-profile web servers. This attack also can be deployed to make a hosted internet website unavailable. An attack such as this can be extended to the mobile network domain. If a mobile device is attacked with a Dos attack, the mobile device will be ineffective. Besides, if DoS attack a mobile phone, the victim will not know. The only apparent way to know is the inability to receive phone calls and a rapid decline of battery charge capacity. The ineffectiveness of the mobile phone due to the SMS messages making use of the signalling layer is also used for other network events.

Rapid battery consumption and signal clog may not only be the motivation for the attack. For example, it can be used to gain an economic advantage by making an entity avoid communication and prevent notification of certain events. A second example is an intrusion Detection System (IDS) that informs a network Administration through a mobile phone in the event of an attack. In the event of a DoS attack, the network can be intruded on for much longer without the network administration knowing [48]. To mitigate this threat, the study in [113] proposed a novel detection algorithm that uses a reply rate detection technique to identify an SMS flooding attack. The research further proposes a method to reduce the blocking rate caused by the attack.

SMS-Based Mobile Botnet The study in [97] described a proof-of-concept botnet that uses SMS as its medium. The simulations in this study show that SMS based can covertly transmit over 90% of two thousand bots within 20 mins using a flooding algorithm. Furthermore, each bot can only transmit four SMS messages during the attack process, and the botnet is robust to node failure that is both selective and random. The study thereby demonstrates that the proposed SMS botnet is a significant threat to the security of the mobile network environment. For this reason, several defence strategies against such attacks were suggested.

Brute-force Attack The vulnerability of firmware is an essential target for the internet of things (IoT) attacks; however, it is difficult due to firmware may not be available to the public, or it might be encrypted with an unknown key. The study in [233] discussed an attack on the SMS authentication code. This attack enables adversaries to gain control of IoT devices without firmware analysis. Based on observation, the IoT device has a native application that controls itself. A customer needs to register an account to use this application, and most times, phone numbers are suggested to be used as an account name. The majority of these applications have a ”Reset Your password” feature that uses an SMS authentication code for a password reset when a customer's password is forgotten. An adversary can steal customers account and gain control of IoT devices by automatically initiating a brute-force attack on this SMS authentication code. The prototype called SACIntruder can perform such an attack.

4.2 Security Vulnerabilities of Mobile Network Algorithms and Protocols

Several threats affect the evolved packet core (EPC) architecture. The surfaced threats have characteristics of the radio interface, which pose a significant risk for the integrity of the mobile network environment. In this subsection, we discuss the threats that degrade EPS security, and these threats can be classified into the main threat and risk categories.

Threats against user privacy can be seen as an authorised use of mobile equipment and user identities to ingress network services. More specifically, a malicious entity or persons might gain access to network services. An example is when an authorised user maliciously modifies the user equipment (UE) to lockout a legitimate user from idle usage of services. When it comes to UE/universal subscriber identity module tracking (UE/UIMT), tracking a user based on an Internet Protocol (IP) address could be linked to either an International Mobile Subscriber Identity (IMSI) or a different identity.

Concerning handovers and base stations, an adversary can force a legitimate user to hand over to a compromised base station through a powerful signal. A method for threats that concerns broadcasting or multi-casting is broadening false information across the network, which can cause network disorder in the signalling plane. When it comes to denial of service attacks (DOS), this attack can be deployed on specific UEs.

There is also a high risk of data manipulation. This data manipulation can be done by changing the signalling data EPS protocol to become vulnerable to adversaries such as eavesdroppers. The data can also be modified while in transit. In a situation where there was authorised access to the EPS core network, malicious users or adversaries can establish communication via the system for extra security damage. A falsification of cloned or faked credentials, false configuration, and data associated with remote attacks could undermine security. Reporting a false location of an enhanced NodeBs (eNB) might lead to network configuration with wrong parameters. Besides, the protocol of the eNB can be exploited in such a manner that faked messages can be inserted illegitimately.

4.3 Secure Transmission for Short Message Service

4.3.1 Secure SMS Protocols Based on Encryption

The existing SMS protocols discussed in this section have been proposed to improve the security of mobile SMS transmission. Due to the insecurities in SMS, various studies have utilised different techniques to secure the transmission of SMS messages. The majority of these techniques proposed by scholars uses the encryption techniques. The study in [90] proposed the use of a public-key encryption system. The system was designed and implemented with Java programming language. The Rivest–Shamir–Adleman (RSA) encryption algorithm was used for ciphering SMS messages, while the SHA-1 is used hashing although, according to reference [235] and [219], there are collisions associated with the SHA-1 hashing algorithm. Lisonek David and Martin Drahanský designed and implemented an application for SMS encryption that uses the RSA for signage and encryption. Their research work also describes attacks on the system and future extensions of the application [129]. Research in [3] by Mary Agoyi and Devrim Seral evaluates the ElGamal, Elliptic-curve cryptography (ECC) and RSA encryption techniques for the use of secure SMS transmission. Their research discovered that algorithms with large key sizes are not suitable for the secure transmission of SMS messages due to mobile phones' low computation and small memory. The ECC encryption technique is preferable to RSA and ElGamal encryption techniques, making it suitable for SMS encryption on mobile phones due to the limited computing resources and smaller key size. In the research [53] by De Santis, Alfredo et al. described a SEESMS (Secure Extensible and Efficient SMS) software framework that allows secure transmission of SMS with the use of public-key encryption cryptography. The study also discovered that RSA and DSA (Digital Signature Algorithm) encryption techniques outperform ECDSA (Elliptic Curve Digital Signature Algorithm) when large key size is used. In the paper in [111], the security of mobile network protocol along with data security for governmental transactions was discussed.

The authors in the study [198] implemented the use of the public key encryption method and used the ECDSA method for SMS digital signing. The study also described a possible attack on the proposed technique. Subsequent research in [195] uses digital signatures and encryption to achieve confidentiality, integrity and availability of SMS transmission across the GSM network. The implementation of the approach includes using AES, DES, triple DES and Blowfish algorithms and uses RSA and DSA algorithms, respectively for signage. During the implementation process, the AES encryption algorithm and the DSA signature algorithm were most suitable. An SMSCrypto framework was proposed in [164]. This framework uses lightweight cryptographic protocols and algorithms to provide encryption and authentication services for secure SMS transmission. The framework was implemented with C (for constrained SIM Card processors) and Java (target at JVM-enabled platforms) programming languages. Also, the signature model used in this framework does not require the inherent overhead found in the Public Key Infrastructure (PKI) model and online infrastructure; thus, the development of secure SMS-based applications can be facilitated. The paper [196] described an easy SMS protocol that uses MAES (Modified Advanced Encryption Standard) symmetric encryption for the secure transmission of SMS messages. The symmetric keys used are stored at an authentication server (AS), while all information of mobile subscribers is stored at a Certified Authority/Registration Authority (CA/RA). The efficiency and security of a symmetric block cipher depend on the length of the key. Larger key size compared to a smaller key size results in a slower encryption [110]. The MAES has a key length of 256-bit key length compared to the 128-bit key length of AES. Some researchers have found a vulnerability in AES, as explained in the papers [30] and [112]. A security protocol in research [224] utilises the Blowfish encryption algorithm for securing SMS messages. The Blowfish encryption algorithm is more power efficient when compared to other encryption algorithms.

In the study, [45] the authors Ei Mon Cho and Takeshi Koshiba proposed a VHCGS (Verifiable Hash Convergent Group Signcryption) technique by including the properties of verification facilities and group signcryption for a trusted third party known as a service provider. Saxena, Neetesh, et al. described a BVPSMS (A Batch Verification Protocol for End-to-End Secure SMS for Mobile Users) protocol that provides end-to-end security over an unprotected communication channel with the AES symmetric key cryptography and MAC (Message Authentication Code). Notably, the proposed technique enables subscribers to simultaneously transmit SMS messages securely from one mobile user to multiple users. This protocol can reliably use an algorithm to distinguish a malicious user in a batch [197].

SMS security can also be enhanced through the application layer of the OSI model. The research in the paper [77], a hybrid application-layer security system with compression for secure M2M communication over SMS was proposed. This system was implemented on an Android platform. The evaluation of the system shows that this security mechanism does not influence SMS delivery time.

The SMS security protocols reviewed in this section do not propose a change in the existing cellular network architecture. These protocols propose the use of asymmetric encryption systems, except in the paper [196] which uses symmetric key cryptography. In some cases, some authors propose the use of an additional trusted thirty party.

4.3.2 Secure SMS Techniques based on Steganography

When establishing secure communications, techniques such as encryption have been used to secure short message service (SMS). Covert techniques such as steganography have also been designed as an alternative approach to securing SMS. The study in [201] proposes an educational system based on steganography that enables students to take multiple choice quiz through SMS on their mobile phone. The study in [202] is the first work that suggests the use of steganography to hide SMS pictures messages. In this method, after converting the image into a black and white image that is suitable for a low powered phone, the image is then divided into a three by three block. Each bit of data is embedded in the image with a password by changing one block cell. In the paper, [208] a stego method for hiding private information in SMS was designed and implemented with J2ME (Java 2 Micro Edition) programming language and tested on a Nokia N71 mobile phone. In this method, the stego-program searches the SMS program for existing words within a pre-made list. If the number of words found were less than the length of the array of zero and one bit made from the data that needs to be embedded, the program would be unable to hide the message. Otherwise, the information can be hidden in the SMS.

The study in [89] uses word abbreviation as a method of hiding messages in SMS. The view of these abbreviated words is identified in concerned sentences of chat. For example, the algorithm used in this work in a manner that enables words such as "you" and "university" can be abbreviated to " u" and "univ" respectively. Data will be hidden in the text by placing the complete phrase and words in the same process. Subsequent studies with similar methods by Khan Farhan Rafat [178] proposed a system for SMS steganography, removing the static nature of word-abbreviation list and introducing computationally light-weighted XoR encryption. If used alone, the sequence of the word-abbreviation list provides an average level of security and makes it difficult for an adversary to decode the system. Although, any word abbreviation can lead to suspicion by adversaries.

The Sudoku puzzle game is suitable for implementing steganography. M. Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza proposed a steganographic approach that employs the use of the Sudoku puzzle game. In this method, the private information is hidden in a sudoku puzzle, and the puzzle is transmitted in a manner that prevents suspicion. The steganographic algorithm used is based on the order of placement of numbers 1 through 9 in one of the specified columns or rows of the puzzle. The hidden message is extracted by solving the sudoku puzzle game [209].

Emoticons are a useful tool for communication in SMS; they are a pictorial representation of nonverbal communication and could serve as a few direct face-to-face communication. It includes nonverbal such as regulating social interaction and expressing intimacy [57]. Emoticons can also be used in steganographic approaches; for instance, in the paper [148], it is possible for an alphabet or number can be hidden within an emoticon when used effectively. That is, 8 bits of data can be covertly hidden within a single emoticon. The advantage of this system includes the simplicity of understanding, and messages can be used as a cover to the abbreviation. However, alphabets and numbers assigned to each emoticon should be changed frequently to ensure the security of the proposed approach. Subsequently, further studies on the use of emoticons and lingoes for hiding SMS has been explored in the study [100], implemented and tested on an android based mobile device. This work has two limitations; the first is that some lingoes with more than one character occupy several characters of the cover medium, resulting in smaller data embedding due to the limitation of characters per SMS (160 characters). Lastly, frequent use of a fixed preshared list (key) could be guessed or even disclosed by an adversary in order to extract the secret. A suggested method for improving this system is the use of dual steganography, which considers encryption.

Abdullah M. Hamdan and Ala Hamarsheh described a technique for concealing text in text messages. In the research [81], a Discrete Wavelet Transform (DWT) compression technique is applied to an image for text hiding. The DWT applied to the image enables it to be divided into four sub-band. The approach proposed uses the structure of the omega network to conceal secret text messages. To conceal a secret message, letters from the original message is taken, then two related letters from the selected letter are generated by the omega network. Finally, a dictionary search is done to find a suitable cover word to conceal the generated two letters. However, to maximise the chance of finding suitable words, the two letters generated need not be adjacent in the cover word. Min Yang et al. proposed an approach for SMS steganography that uses mathematical equations as a cover medium to conceal and transmit private information. Consequently, the white-space steganography is used for concealing the position of the two letters in the selected cover word. This technique can conceal private messages on a single SMS transmission with a maximum of 140 characters [122]. The experiment of this method shows better performance than the current similar mechanisms, especially when we are trying to conceal text messages with long length [83].

Ahvanooey, Milad Taleby, et al. proposed a text steganographic system that provides end-to-end security during the transmission of text messages through SMS or social media platform between subscribers. The technique proposed in this work is suitable enough to conceal private messages with a large fixed-length into a short cover message to eliminate the trace of the stego-object, making the stego-object invisible to adversaries. This method achieves security by utilising mathematical encoding techniques and symmetric key algorithms (e.g., it can be any symmetric key-based algorithm such as AES, DES and RC5) [223].

4.4 Protocols used for Secure SMS based Mobile Banking

The key idea behind this niche research field is to adapt members of a protocol family initially devised for confidential communication through various social media channels [26, 47, 63, 170] to a mobile banking setting. In this section, these papers are reviewed, and besides various works within the broader context of SMS based secure mobile banking are covered. Studies such as this are an emerging research area, and the relevant literature base appears to be still relatively small.

4.4.1 SMS Banking Protocols based on Steganography

This subsection reviews specialist protocols for SMS mobile banking, employing steganography as the core cryptographic technique rather than the mainstream encryption approach.

The idea of using steganography to improve the security of SMS mobile banking was first presented in the study [207]. Subsequently, a text-based steganographic protocol was proposed in the [191]. The SMS containing the transaction details is "watermarked" using a "dummy text file" (DTF). However, if the DTF size increases, the covert information is vulnerable to attacks. The paper [6] describes a secure SMS payment method based on text steganography using sequences of white-space to encode positions in a shared look-up table that needs to be exchanged secretly.

There are researches within this specialised area of study that combine encryption and steganography to improve mobile banking security. In a study by Pawar Pratiksha Y., and S. H. Gawande, the confidential data is first encrypted using the AES cipher suite; then, the cipher-text is embedded using the LSB technique. This approach was implemented with the JAVA programming language and Microsoft SQL Server [162].

4.4.2 SMS Banking Approaches based on Encryption

Various studies have been proposed to strengthen the security of SMS mobile banking. However, most publications on securing SMS bank transactions focus on the use of encryption with third parties. The research in [88] described a Secure SMS Payment protocol suitable for small and macro payment services. This protocol utilises ECDSA (Elliptic Curve Digital Signature Algorithm) for non-repudiation and authentication, while AES is used for encrypting each session for SMS secure transactions. Authentication and encryption are done between the customer and the payment gateway. The encryption keys are installed on the customer's SIM card during the registration process. Updates for the session key were not described in the protocol. The paper in [227] SSMS is a secure certificate-based mobile banking protocol that requires participants to perform certificate and key validation. This protocol uses an Online Certificate Status Protocol (OCSP) server and ECC to establish end to end security. The private and public keys could be generated on a key generating server or on a mobile phone. However, mobile phones lack the capacity to generate random numbers that can be used to secure private keys. The OCSP server validates customers private key, and the corresponding public key, by utilising a zero-knowledge technique described in the research [85].

In the study [87], a secure and cost-effective SMS Payment protocol is described for macro transactions. A secure master secret key is generated inside the mobile phone and encrypted with a one-time secret code for secure SMS to be exchanged between the customer and the bank. The secure master key used in this protocol is a double-length key, used to generate a session key with a cyclic shifting technique described in this study [140]. A separate shift index is applied to each part of the double-length master key [119]. The research [39] described a secure SMS payment system that enables SMS payment to the bank through the Malaysian Electronic Payment System (MEPS). All customers' banking information is stored at MEPS. Any transaction request routed to the bank is encrypted with a symmetric key. The bank uses a digital certificate to identify connected authorised users. The study [114] proposed an SMS based mobile protocol based on Elliptic Curve Menezes-Qu-Vanstone (ECMQV) key agreement protocol and AES encryption algorithm, suitable for low-value transactions. In this protocol, the financial server is connected to a certificate authority for the verification of digital certificates. A certificate authority obtains the public key and digital certificate, and financial server, respectively.

The research in [34] presents an SMS banking protocol with ECDSA (Elliptic Curve

Digital Signature Algorithm) for digital signature and ECIES (Elliptic curve integrated Encryption Scheme) for encryption. The bank generates public and private keys with ECC. The bank's public key is embedded on a mobile application that encrypts and verifies SMS sent by customers. The customer's certificate is validated by the bank using the certificate validation procedure described in [220]. The study in [35] proposed a secure solution that can be applied in real-world environments. The main objective of this study is to develop an end-to-end SMS communication and reliable framework for SMS mobile banking. The verification of the security properties and framework correctness is achieved through formal methods. The automated validation of internet security protocol and Scyther tools were used to validate the protocol experimentally.

Security protocol designed with the use of encryption is reliable and secure; however, encryption can create a suspicion that sensitive data is transmitted across a network communication channel. To address this aspect, using the alternative cryptographic technique of steganography would be suitable.

4.5 Online Social Network-Specific Multi-Channel Protocols

Online Social Network (OSN) platforms have become popular amongst different age groups around the world; however, security and privacy remain a difficulty. Several works such as as[249], [52], [99] and [132] has been proposed and implemented to mitigate this challenging task. In accordance, the research in [46] described and implemented an Enhanced Virtual Private Social Networks (VPSN) based on reference [99], that enables OSN subscribers to share private generated content securely. The technique described is based on the use of hash functions and symmetric key encryption. The notion behind this approach is to openly transmit a private key through an insecure channel and a cipher-text via a private channel. In this study, a cloud storage provider is used as a private channel. The private key is a hashed string that can contain natural language sentences of any length. This approach makes the scheme secure against adversaries and does not raise suspicion. Further, this approach is made valid by several presumptions.

Security protocols for the systematic use of several channels have already been published in early works by [19], [76] and [210] in the context of ad-hoc networks. They rely on the existence of at least one authenticated channel in order to create a secure connection and to establish a symmetric key exchange.

The paper gives the formal definition of the communication models presented in Chapter 5, Section 5.4 - the high-entropy model using traditional steganography techniques for cover modification, selection or synthesis and the low-entropy model, based on specialised techniques for the usage in OSNs. A new approach was initiated by the paper [26], and earlier in paper [99] is to disguise user-generated content such as posts to an online social network through a specific form of steganography, which makes it “socially indistinguishable” and hence undetectable (under certain assumptions). In the corresponding protocol, an unsuspicious ”fake” short textual message t is published on the socially constrained channel, scrutinised by the OSN provider. In contrast, the secret message is encrypted with a secret key derived from the seed t.

This protocol is further explored in study [47] where two-channel protocols are proposed that enable users to authenticate messages on ad-hoc Social Media Platforms (SMPs).

In the first protocol, a message is transmitted to a receiver on the socially constrained channel. In contrast, the message digest used for authentication must be published in a contextually relevant manner through an out-of-band (OOB) channel. The second protocol requires a commitment scheme that needs communicating parties to have a shared Authentication Transaction Account (ATA) and password for authenticating transactions. A drawback is that the use of an ATA may violate the terms and conditions of some SMPs.

The studies [26], [47] and [63] inspired the design of the protocol presented in Chapter 5 and Chapter 6. Instead of using a secret sharing scheme in [63], which requires non-trivial computations, a simple binary XOR operation achieves the same level of security and the only small reduction in redundancy due to the use of secret splitting. Secondly, instead of using the low entropy steganographic approach in [26], the combination of both low and high steganography is a novel feature.

4.6 Game Theory for Steganography

Intuitively, the security of a steganographic communication between two principals lies in the inability of an eavesdropper to distinguish cover objects from stego-objects, that is, objects which contain secret messages. A system should be already considered insecure if an eavesdropper can suspect the presence of secret communication. Several definitions of steganographic security were proposed in the literature. However, they all consider only entirely secure steganographic systems, where even a computationally unbounded observer cannot detect the presence of a secret message exchange. Secondly, it might be challenging to construct secure schemes usable in practice following these definitions. Thirdly, they all require knowledge of the probability distribution of typical covers. However, it might be possible in some instances to compute this probability; it will, in general, be impossible to obtain.

In contrast to encryption, undetectability remains the primary purpose of steganography, i.e., the science of communicating a hidden message in a manner that is undetectable by unauthorised persons, apart from the sender and the intended recipients. Various studies have been enormously on steganography: In the following section, we review various studies relevant to steganography within the context of game theory.

4.6.1 Generic Security Games

4.6.2 Stego-Games

Researchers such as [40], [250] and [145] have focused on theoretical definitions of steganography. The study [40] proposed steganographic definitions and adversarial games for steganography. The security of the stego-system presented includes the relative entropy between the stego-text and the cover-text distribution. The work in [145] described a model which includes characterisation and definitions of two critical components of a steganographic system, the encoding process and the adversaries attack the stego-object. The definition of the two components is based on a requirement in the maximum distortion between cover-object, stego-object and the modified stego-object. In the study in [250], a model which enables evaluation of a stego-system's security against a known plain-text is presented.

Studies in [109] and [94] presented a formal definition and theoretical structures based on cipher based computational indistinguishability. The study in [109] provided definitions that reply on a probabilistic game, where an adversary is faced with a steganographic decision problem. In contrast, research [94] uses cryptographic and complexity-theory proof methods to describe conditions necessary for a secure stego-system.

Researchers have made efforts by proposing several steganographic methods using images as stego-covers, many of which utilise the Least Significant Bit (LSB) to reduce significant changes in the stego-cover to prevent suspicion. Methods proposed in studies such as [72] and [189] use the LSB technique to conceal secret messages. The F5 steganographic algorithm proposed in [238] follows the orthodox steganographic approach. The study in [239] shows that the F5 algorithm is resilient to statistical and visual attacks. A subsequent study in [189] proposed a new image-based steganographic algorithm, Selected Least Significant Bit (LSB), by improving the spatial domain of LSB hiding.

The paper in [138] proposed a steganographic technique that uses a specific method that prevents image downgrading; this approach makes the stego-object secure against all possible statistical and visual attacks. However, the security of this approach is achieved by using an encryption algorithm. An unconventional research in [43] uses X-Box mapping and LSB to conceal secrets in an image. However, the security of this approach is achieved by using an encryption algorithm.

Intuitively, the security of a steganographic communication between two principals lies in the inability of an eavesdropper to distinguish cover objects from stego-objects, that is, objects which contain secret messages. A system should be already considered insecure if an eavesdropper can suspect the presence of secret communication. Several definitions of steganographic security were proposed in the literature. However, they all consider only entirely secure steganographic systems, where even a computationally unbounded observer cannot detect the presence of a secret message exchange. Secondly, it might be challenging to construct secure schemes usable in practice following these definitions. Thirdly, they all require the knowledge of the probability distribution of typical covers; However, it might be possible in some instances to compute this probability; it will, in general, be impossible to obtain.

4.7 Summary

Due to the security challenges in SMS, a significant amount of studies has been made by researchers focusing on different security solutions for secure SMS transmission using steganography and encryption; however, most solutions are focused on the use of encryption. In the area of SMS based mobile banking, most research is focused on encryption-based protocol techniques. However, very few studies proposed the use of steganography for SMS banking purposes. Besides, most studies published in the literature focus on approaches that require a trusted third party. Throughout this thesis, the main focus is the security improvement of existing mobile banking frameworks by designing novel security controls in the area of cryptographic protocols, intending to mitigate fraud in mobile banking. The security controls presented in this thesis is inspired by the protocols proposed for Online Social Network security. These security issues are addressed in Chapter 5 and Chapter 6.

Chapter 5

A Multi-Channel Steganographic Protocol for Secure SMS Mobile Banking

The advancement in mobile technologies and wireless communications has led to a rapidly growing number of users benefiting from mobile banking services. SMS banking offers a convenient mobile banking solution that is easy to implement and frequently used in many parts of the world. However, it is only viable under the assumption of secure SMS services. In this chapter, a novel secure SMS banking protocol is proposed. The approach is based on a multi-channel security protocol combining low and high entropy steganography. One of the distinct advantages of this protocol is its confidentiality property against the Mobile Network Operator, which, to our knowledge, is a novel feature. Furthermore, the required architecture is simple and only involves GSM services and one additional internet connection, which can be insecure. As such, it offers security and low deployment costs and would be suitable, for example, in rural areas or countries without individual secure home internet connections.

5.1 Motivation

Though traditionally, goods and services have been paid for using physical currency, this has steadily been replaced by electronic payment systems. The ubiquity of mobile phones and wireless technologies such as GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for GSM Evolution) and 3G (Third Generation) have led to the emergence of mobile banking [23, 101] which has been widely accepted by customers over traditional electronic banking [101, 245].

The mobile banking industry has become the fastest and largest growing industry, given certain factors like cost and ease of use. Prominently, the usability of cellular subscriptions worldwide in 2011 reached approximately 6 billion and has led to an increase in mobile banking usage [66]. Some studies were conducted in various countries in Africa with regards to mobile banking adoption, and Nigeria is a country regarded as the most populated in Africa is considered a leading market player for mobile banking applications [21, 4].

Mobility is a significant benefit of mobile banking since smart mobile devices are always with the customer. The customer does not have to visit the bank's branch or use the

ATM (automated teller machine) to utilize the bank services [2]. A study indicates that the number of customers who visit the bank has reduced drastically after installing ATMs. Banks will need fewer staff due to the cost affordability of mobile services. Bank customers will no longer visit bank branches apart from essential occasions.

In some countries, affordable mobile network services such as SMS (Short Message Service) are currently in use for mobile banking [104, 21, 39]. SMS is a GSM (Global System for Mobile Communications) service that transmits and receives plain text messages up to 160 characters of 7-bit encoding [38].

There are other methods of payment, such as Reverse SMS Billing (Premium SMS). In this payment, the customer initiates the purchase by sending an SMS to get information such as product requirements and digital service from the merchant. An SMS regarding billing information is sent back to the customer by the merchant. The customer then acknowledges the payment by sending an acknowledgement SMS back to the merchant. Subsequently, the merchant then sends an SMS to the mobile service provider about the payment details. Finally, the customer is charged premium SMS rates on the next billing cycle by the mobile service provider. Traditionally, this payment mode is currently in use to purchase digital content like music, ringtones and videos. The payment is popular because of simplicity and ease of use because it does not require a customer to install specific software on a smart mobile device [23], [213].

The nature of wireless communication leads to several issues regarding performance and transaction security; for example, SMS messages transmitted over wireless networks are easily eavesdropped on, intercepted, or modified [196], and the A5 symmetric stream cipher utilized to provide protection is vulnerable to attacks [107].

In this chapter, we are motivated by the following scenario: Amara wants to implement secure SMS banking to pay money into Ebere's account. However, she is in an insecure and inadequate infrastructure area, where there is no Internet connection in people's homes. There are public cybercafes in the neighbouring town, which offers access to the Internet. Amara has a (dual-SIM) mobile phone that is a low-powered device, not connected to the Internet, so she cannot install mobile banking apps.

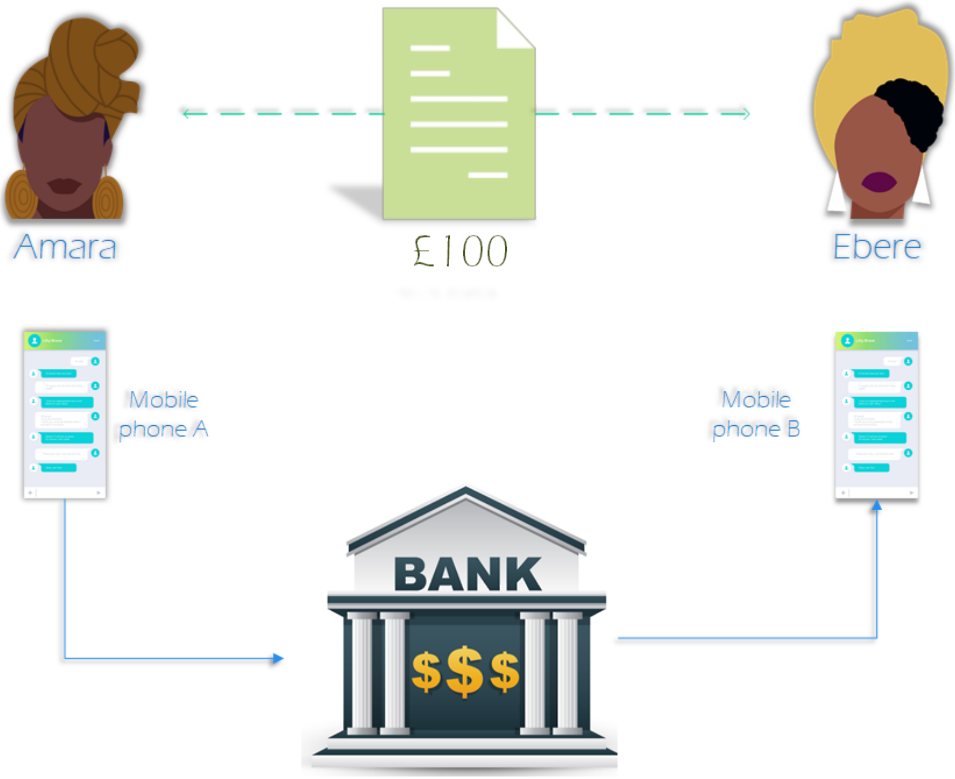


Figure 5.1: Amara wanting to transfer money to Ebere through a bank.

The bank is considered to be trusted. On the other hand, the cybercafé and the mobile operator environments are not – there could be a range of passive or active attacks such as eavesdropping, spoofing, delay, replay or man-in-the-middle attacks carried out by adversaries external or internal to the system. Furthermore, steganalysis by passive or active wardens also needs to be considered. One individual adversary could make attacks, or adversaries could conspire together (collaborative attack). The security analysis in this paper will highlight the security properties of our protocol concerning the most realistic ones among these different attacks.

5.2 Chapter Contribution

The main research contribution of this thesis is the design of a novel cryptographic protocol based on steganography, achieving covert communication using multiple channels. The steganographic technique of the protocol could be considered a hybrid, as it combines both steganography by cover synthesis and cover modification. When used in a mobile banking setting, compared to previous proposed secure SMS banking protocols, one of its main advantages is that the need for key exchange or trusted third parties does not arise. Another advantage of this protocol is its confidentiality property against the Mobile Network Operator, which, to our knowledge, is a novel feature. An extended version of the protocol could easily allow for additional integrity verification of the SMS transaction.

The organisation of this chapter is as follows: Section 5.3 presents the security technology relevant to this paper. Secondly, section 5.4 presents entropy in cryptography and steganography. Furthermore, section 5.5 presents the system models used in this chapter. The systems models include the passive and active adversarial models. Section 5.6 describes our main contribution, the security protocol. Finally, the following section, 5.7, analyses its security, and Section 5.8 concludes with a summary and items for future research.

5.3 Security Terminology and Setting

In this section, essential terminology related to steganography and encryption is described with a distinction between the two methods. In addition, two steganographic models presented in [26] are examined and adopted. The description of these terminologies sets the foundation for this chapter.

5.3.1 Security Goals

In cryptography, the purpose of achieving data confidentiality is to ensure that private information is not disclosed to unauthorised persons. Data integrity ensures that a private message transmitted between two participating entities has not been altered, and validation is issued by the sender (e.g. message digest). When an intended recipient can identify that private data is coming from an expected *claimant* (i.e. the sender) and an adversary has not modified the private data, this is known as origin integrity. In this chapter, the focus will mainly be on confidentiality.

5.3.2 Encryption and Steganography

Encryption and steganography are cryptographic concepts that are used to protect sensitive information. However, their techniques of data protection are distinct from each other. Encryption is a technique that converts a plain-text to cipher-text with a secret key. This technique scrambles or encodes the message from attackers but not the message's existence. Encryption techniques can be considered in two main categories: "symmetric encryption" and "asymmetric encryption" [215].

Steganography, on the other hand, is a cryptographic technique that hides (or "camouflages" the existence of a payload (secret message) m within an unsuspicious cover medium c. Both the message and the cover medium can take various formats. These include text, image audio and video files, for example, [73]. Once a secret message has been embedded into a cover medium, it is referred to as a *carrier object* o (sometimes called a stego-gram).

A principle objective of steganography is that the act of sending and receiving a hidden payload is only known to participate senders and recipients. Additionally, a hidden payload should only be accessible and detectable by authorised parties, and unintended parties should not be aware that secret communications are taking place. Ideally, a carrier medium should be able to withstand *steganalysis* (i.e. detailed scrutiny, detection and analysis for a payload or carrier-medium traits).

The critical point to note on encryption and steganography is that each technique has its advantages and limitations, especially in its effectiveness and utilisation in certain situations. No cryptographic technique is a perfect solution as one technique may be more beneficial than another for specific reasons. In the following subsection, a description of two steganographic models presented in the study [26] is described.

5.4 Entropy in Cryptography and Steganography

In information theory, the term entropy is defined as the measure of uncertainty or unpredictability of information in a message. In other words, it is the anticipated value of the information within a message. This uncertainty can be measured with the level of randomness, and it is applied to the information entropy concept. Shannon initially proposed the concept of entropy (H) as part of his data communication theory. A system contains three elements: a source of data, a communication channel, and a receiver. The fundamental problem of communication is for the recipient to identify what the source generated data based on the signal it receives through the communication channel. Subsequently, the source coding technique was devised to encode, compress and transmit messages from a data source [187].

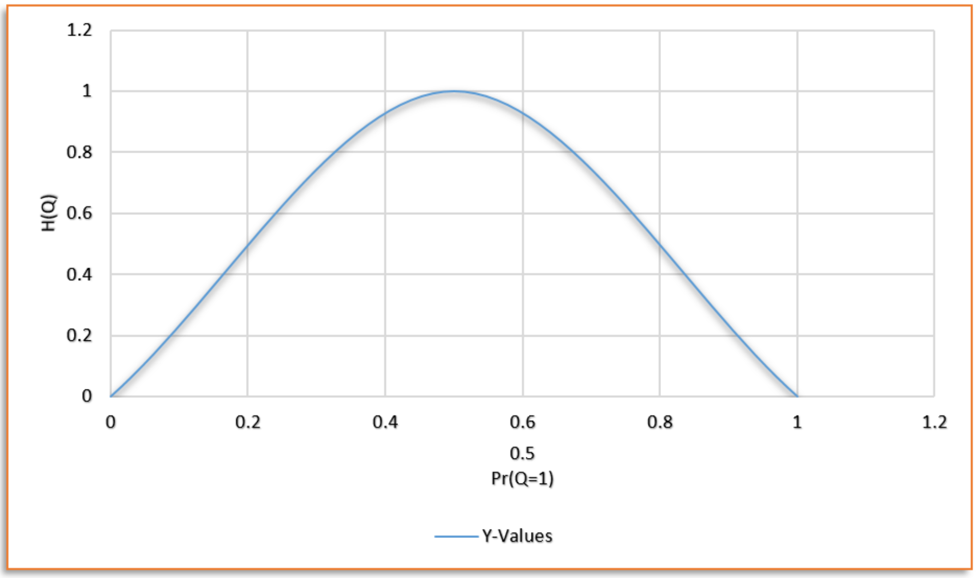


Figure 5.2: Entropy $H(Q)$ on the flip of a coin flip, measured in bits, graphed versus the bias of the coin $Pr(Q = 1)$, where $Q = 1$ represents a result of heads.

To compute entropy, it is presumed that Q is a set of unique characters found in a given word existing the in cover-medium. We consider that $P(q^i)$ is the occurrence of probability of the q_i^{th} component. Then, the entropy is defined as:

$$H(Q) = -\sum_{qi} log_2 P(q_i).$$

In the following subsections, the basic concept of entropy in cryptography and steganography are discussed.

5.4.1 Entropy in Cryptography

In a cryptographic setting, entropy is defined as the randomness collected by a system for use in algorithms that require random data. A cryptosystem is said to be vulnerable to attacks and unable to encrypt a message securely if there is a lack of sufficient entropy. However, suppose an adversary is computationally unable to extract information about the plain-text from the corresponding cypher-text then, there is sufficient entropy in the cryptosystem; this makes the system entropically secure. Cryptographic entropy is essential for two purposes [172, 137, 135]: at most times, it is used to measure the unpredictability of a cryptographic key; however, its fundamental uncertainty is challenging to measurable. Sufficient entropy in keys makes them more secure and difficult to guess, and sufficient entropy in messages make it challenging for an adversary to guess correctly. For instance, a randomly and uniformly generated 128-bit key has 128 bits of entropy, which means that it requires 2^{127} brute force attack. To a great degree, modern cryptographic systems rely on keys that are randomly generated with a Cryptographically Secure Pseudo-Random Number Generator, or CSPRNG. In the next section, we discuss entropy in steganography.

5.4.2 Entropy in Steganography

In steganography, entropy is defined as the statistical measure of randomness contained in an image. The information entropy of the image can reflect on the image quality. Shannon's entropy is used to measure and evaluate the randomness of stego-images [177] [84]. Secret messages are hidden in high entropy areas, and these areas are called the texture region. A perfectly flat image would have an entropy of zero, and the area of the image with higher values of entropy are least visible to the human. Hence, if the secret is embedded in high entropy areas of an image, then higher undetectability can be obtained [118] [117].

There are different techniques for implementation of steganography[221, 102, 222, 184, 153]; in this section, we discuss three techniques; significant bit (LSB), discrete cosine transform (DCT), and discrete wavelet transform(DWT) technique. These techniques hide the secret in the spatial domain and frequency domain. In the spatial domain, the processing is implemented directly on the pixel values of an image; however, in the frequency domain, pixel values are transformed into coefficients. The LSB stego approach is executed in the spatial domain, while DCT and DWT techniques are implemented in the frequency domain. In the LSB, every pixel of an image is transformed into binary values, and the secret is cautiously hidden into the least significant area. This process enables the integrity of the image to be undiminished. However, the LSB is vulnerable to image processing attacks such as cropping and compression. Steganography in DCT and DWT techniques are applied differently. Both techniques are algorithms that transform an image from the spatial domain to the frequency domain. In the DCT, when an image is transformed in the frequency domain, the secret message is hidden in LSB bits of the medium frequency components, while in DWT, the secret message is hidden in the high-frequency coefficients with Entropy Encoding EBCOT(Embedded Block Coding with Optimized Truncation), thus providing maximal robustness and undetectability against statistical attacks.

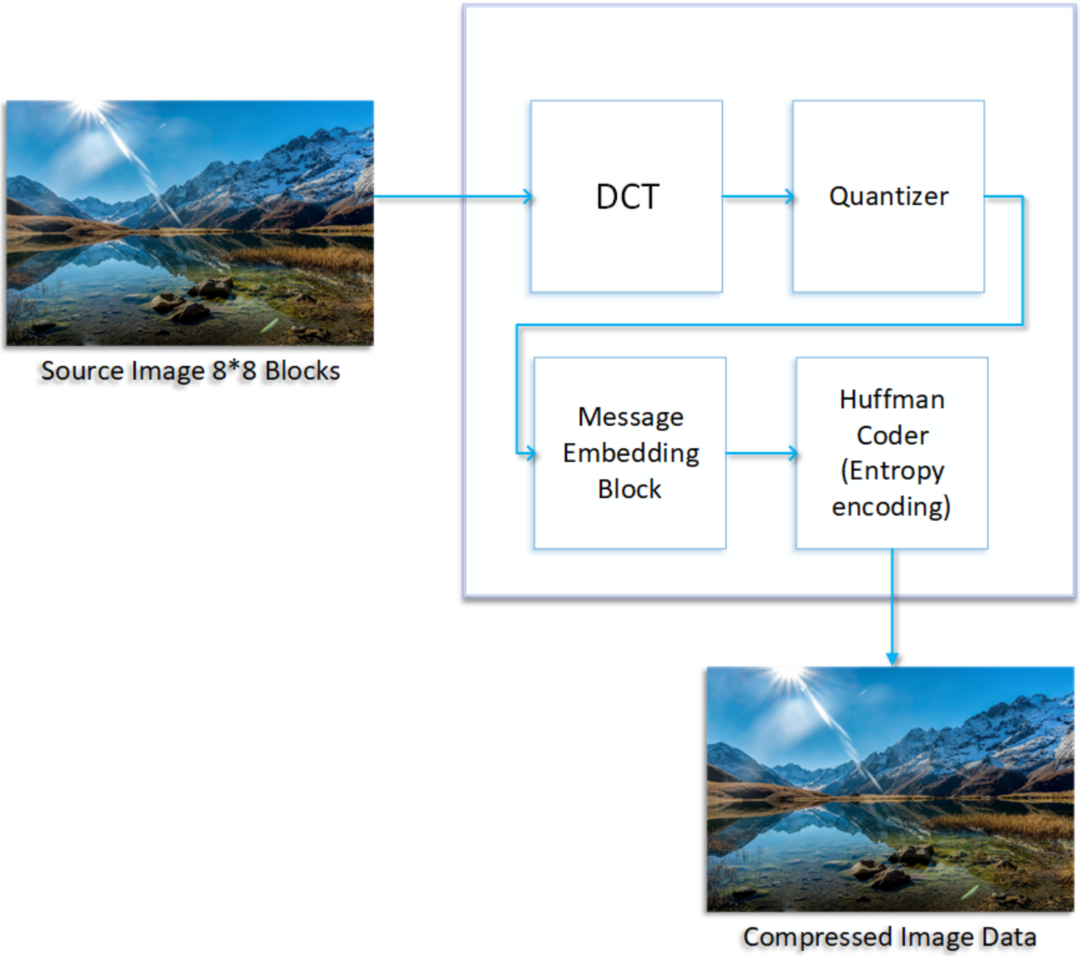


Figure 5.3: Basic Steganographic Method Using DCT (JPEG Compression)

The stego-images are compared with cover images to be used as an evaluation of image steganography. MSE (Mean Square Error), MAE (Mean Absolute Error), SNR (Signal

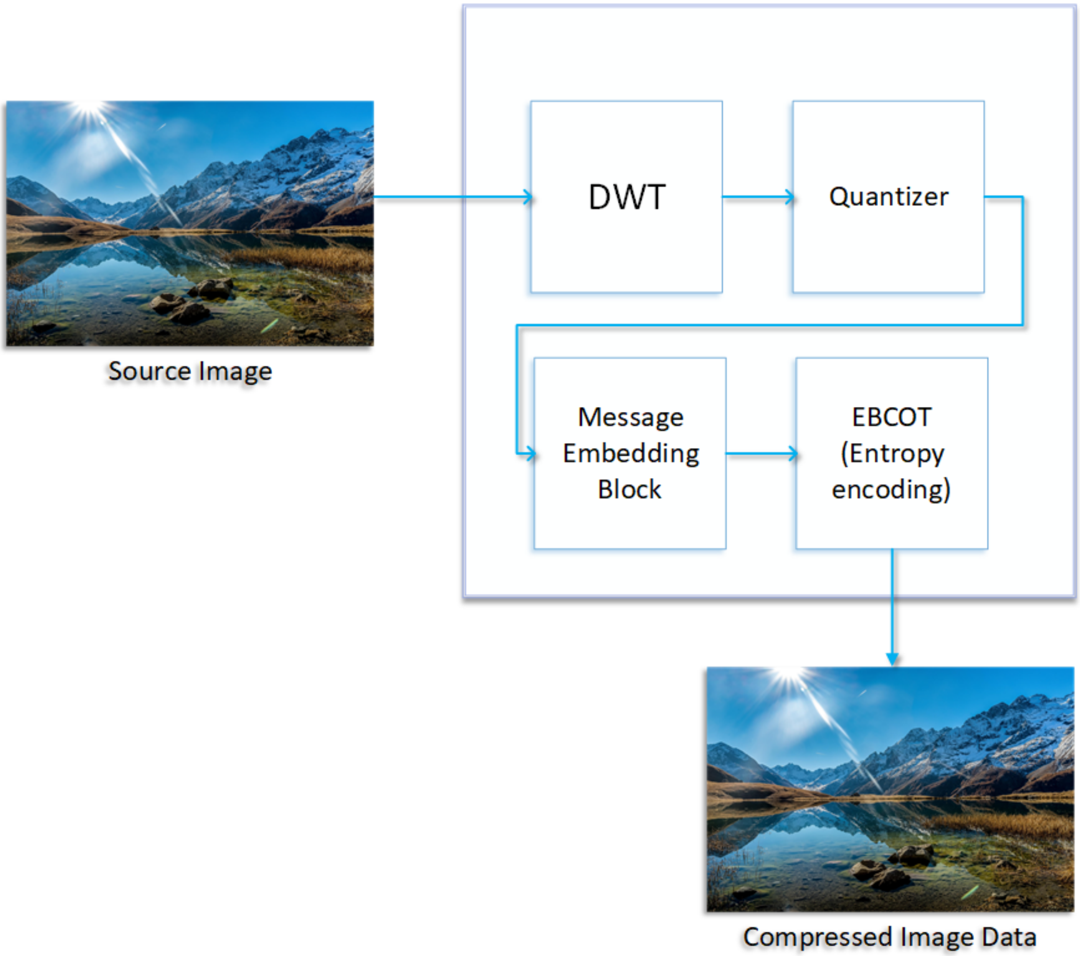


Figure 5.4: Basic Steganographic Method Using DWT (JPEG Compression)

to Noise Ratio), PSNR (Peak Signal to Noise Ratio), and capacity are parameters used to analyse the undetectability of stego-images. These parameters are also used to measure the difference between cover images and stego-images. Known steganographic algorithms include: EzStego, S-Tools, Steganos, Jsteg [239], OutGuess[244], F5 [238] and YASS [211]. The following subsection 5.4.3 presents the high and low entropy steganographic models.

5.4.3 High Entropy Steganographic Model

When considering the high entropy steganographic model, the cover-medium must have enough entropy to contain a payload [41, 42, 5]. This model mirrors the traditional concept of steganography as explained in subsection 5.4.2, and the stego encoding process may or may not require a conventional secret key. The resulting stego-object may require a secret key to extract the secret message. This is expressed in the following Definition 5.4.1 of a high-entropy stego-system:

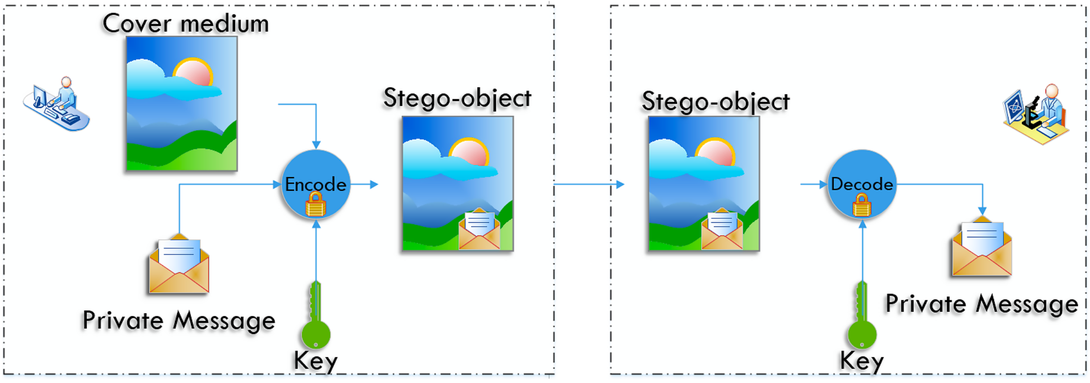


Figure 5.5: The high-entropy stego model

Definition 5.4.1. *A high-entropy steganographic-system* $\mathcal{S}^h$ *consists of three efficient algorithms: a probabilistic key generator* $\mathsf{Gen}(\cdot)$*, a probabilistic encoding function* $\mathsf{Enc}(\cdot,\cdot,\cdot)$ *and a deterministic decoding function* $\mathsf{Dec}(\cdot,\cdot)$.

- $\mathsf{Gen}(\lambda)$: *takes a security parameter* λ *as an input and returns a (symmetric in most cases) key such that* $k \in \{0,1\} \leftarrow \mathsf{Gen}(\lambda)$ *– in the simplified preliminary architecture of this thesis a symmetric key is not actually required. However, its use would make it challenging for an adversary to access the payload and further increase the protocol's security.*

- $\mathsf{Enc}(\cdot,\cdot,\cdot)$: *is a steganographic hiding (or embedding) algorithm that receives a secret message* m *(payload) and a cover-medium* c*, returning a carrier-object* o*. Formally,* Enc *takes* $k \in \{0,1\}$*, a string* $m \in \mathcal{M}$ *and* $c \in C^h$ *and returns a set of stego-objects* $(o_1,\ o_2....o_n)$ *such that* $o = \mathsf{Enc}(k\ , m\ , c)$.

- $\mathsf{Dec}(\cdot,\cdot)$: *is a deterministic algorithm that returns an embedded message (payload)* m *by extracting it from the carrier-medium. For simplicity, the decoding algorithm* Dec *takes* k*, stego-object* o *and return* m *such that* $m = \mathsf{Dec}(k\ , o)$.

For all messages m *of size bounded by a polynomial in the size of the cover medium, the following condition holds:* $\mathsf{Dec}(k, \mathsf{Eec}(k, c, m)) = m$. *Definition 2.4.1 follows the traditional steganographic system where an encoding function* Enc *is used to conceal a private message* m *within a specific plausible cover-object* o*. The result is a stego-object* s *which may or may not require a stego-key* k*. It also relates to the ineffectiveness of an adversary to detect the concealed message* m*.*

Security in the high-entropy steganography can be explained as the unfeasibility of an adversary to distinguish between a cover object and a stego-object. The cover object must have enough entropy to contain the secret message by default. Although, if the cover object lacks sufficient entropy to conceal the secret message (e.g., a large image cannot be embedded in a short text message. This is due to the lack of entropy contained in a text), then another approach has to be utilised [26]. Such an approach is discussed in subsection 5.4.4 as the low-entropy model.

5.4.4 Low Entropy Steganographic Model

The low entropy steganographic system was first described in the paper [26].

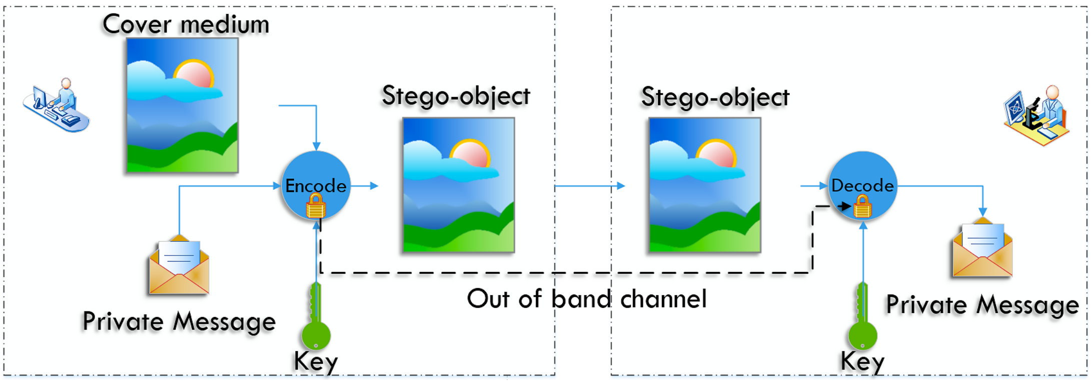


Figure 5.6: The low-entropy stego model

Definition 5.4.2. *A low-entropy steganographic system $\mathcal{S}^l$ consists of three efficient algorithms as in the high-entropy model but with a number of differences: a probabilistic key generator* $\mathsf{Gen}(\cdot)$, *a probabilistic encoding function* $\mathsf{Enc}(\cdot,\cdot,\cdot)$ *and a deterministic decoding function* $\mathsf{Dec}(\cdot,\cdot,\cdot)$.

- $\mathsf{Gen}(\lambda)$: *takes as input a security parameter λ, and returns a key $k \in \mathcal{K}$.*
- $\mathsf{Enc}(\cdot,\cdot,\cdot)$: *The embedding function* Enc *returns a carrier object o and additionally a secret message m' (which may be identical to m). In other words,* Enc *takes as input a key k, a cover object $c \in C^l$, and a secret message $m \in \mathcal{M}$, and returns a stego-object $o \in O^l$ and a secret message m'.*
- $\mathsf{Dec}(\cdot,\cdot,\cdot)$: Dec *takes as input a key k, a stego-object o, and a secret m', and returns the message m.*

The following property now holds for all messages m irrespective of their size: if $(o, m') = E(k, c, m)$, *then* $D(k, o, m') = m$.

The low entropy model is an alternative if the cover object lacks enough entropy to conceal the secret message. Rather than encoding a secret message in a cover object, a fake unsuspicious text disguised as a cover object could be published on a socially constrained channel, e.g., a text message that can be published on a Social Network Platform such as Twitter or Facebook. It is necessary to note that the cover object (e.g., a text message) is selected to represent the secret message rather than have the secret message encoded within the cover object. The real secret message is concealed by transmission over an Out-of-Band (OOB) Channel since, by definition, the stego-object cannot contain the secret. The operation of linking the stego-object to the message would possibly, or possibly not, require a key. When the recipient receives the stego-object, he will use it to determine the nature of the Out-of-Band Channel and eventually get the secret message.

5.5 System Model

This section introduces the adversarial models used throughout this chapter.

5.5.1 Adversary Model

An adversary model is considered a set of descriptions that specifies the aims and limitations of an adversary's computational knowledge and ability. An adversary can be considered an entity that wishes to hinder, detect or modify concealed content transmitted over covert communication. To identify in totality the security goals against omnipotent adversaries is impossible. Therefore, devising specific adversary models is essential [179]. For example, if an adversary knows a cover-object $o(0)$ (an image) for a specific communication channel C, a secret message $m \in \mathcal{M}$ can be detectable with probability $\mathsf{Prob}(m \neq 0)$ by comparing objects $o(0)$ and $o(m)$. $o(m)$ is a stego-object that contains a secret message m.

In this system model, adversaries are defined as entities attempting to passively and actively access the confidential information m by monitoring a particular communication channel, with and without the intent to interfere with the content. These entities are an External SMS Interceptor, employees at Mobile Network Operators (MNO), even the Internet Service Provider (ISP) and the Government. None of these entities should learn and modify the content of m else; confidentiality and integrity are compromised. The two types of adversaries described in this section are based on the amount of information they could access.

Adversaries have no control over the user's computing environments, such as the user's browser, mobile phone, and any other device that might be used in the protocol. As many companies through MNOs rely on SMS for targeted advertisement, data mining, marketing and sentimental analysis, financial and commercial interests frequently restrict MNO from using encryption techniques. Restriction such as this motivates the necessity for undetectability if users wish to transmit or exchange confidential content. Also, the government can rely on encryption restrictions to attempt a systematic monitoring process on its SMS subscribing citizens, besides totally or partially monitoring subscribers' traffic. Without authorisation, the governments' authorities can often obtain subscribers data from MNO providers, for example, through wiretapping without a warrant.

To this end, it is essential to define two realistic and durable adversary models. In the following subsections, the capacities of the adversaries are discussed.

5.5.2 Passive Warden

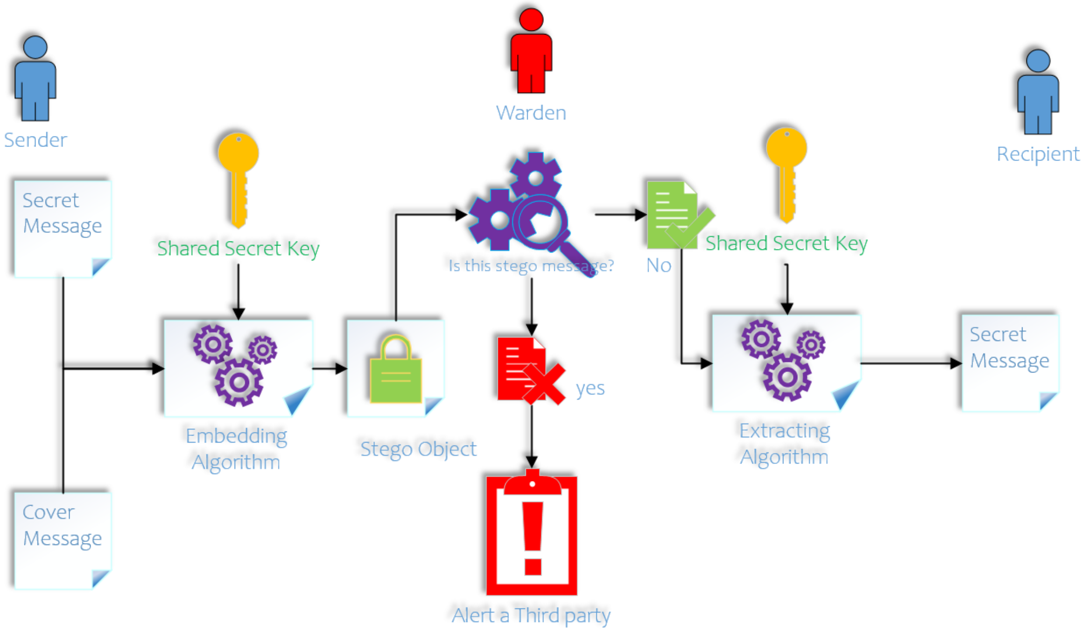


Figure 5.7: Passive Warden.

Steganography is a communication technique used to communicate secretly; as such, it motivates investigation by the human mind. The approach that concerns developing techniques for detecting and eventually extracting stego messages is known as steganalysis. In steganography, steganalysis is the job of a warden. When one individual positions himself into the role of a passive warden who has read-only access to a communication C, the goal is to use a detection function $D^{\mathcal{F}}$ to identify the existence of a secret message m and decide if a message is considered a stego-object o, utilising this approach could be used to prove to a third party (e.g. the Active Warden) about the usage of steganography on a communication channel. Besides, when analysing digital images, the passive warden is allowed to visually inspect exchanged images and use statistical analysis to experiment on the distribution of colours in the image and check if it follows the expected statistics of natural images. An example of a passive adversary is an eavesdropper.

The Passive Wardens considered in the proposed protocol are described:

- **Mobile Network Operators-Employees and Management:** The Mobile Network Operators are adversaries that have access to text messages of network subscribers. Without subscribers' knowledge, the employees can passively monitor private text message transmissions and sell this data to unwarranted third parties companies. For instance, In 2018 and 2019, United States MNOs such as Verizon, T-Mobile, Sprint and AT and T sell customers' real-time location information to unauthorised persons, companies and including law enforcement agencies that, without legal consent [151]. In 2010, Malte Spitz, a German privacy advocate, used privacy legislation to get his mobile operator to publish his records for education purposes. His reason behind his actions was to enable the public to understand how the MNOs can monitor users [65]. In another instance, the value chain in SMS marketing, subscriber information is sold to companies involved [78].
- **Internet Service Provider (ISP) of Cybercafe:** The ISP is considered as a passive adversary that can undermine the Confidentiality and privacy of the public. Privacy is considered to be a significant concern with the internet. In today modern society, most ISP (Internet Service Providers) continue to make efforts in monitoring the online activities of internet subscribers. The ISPs collect personal information such as search parameters, contact, and subscribers' product. At most times, this informa-

tion is used for commercial purposes, such as targeted advertising [188]. However, some studies show that personal information has been exploited for other reasons, including government surveillance, identity theft, determination of insurance coverage, price discrimination [143, 144, 86] and assessment of financial credibility.

Studies have revealed that the prevalence of third-parties tracking on the internet is considered as dangerous[139] [127] [188]. For instance, when an online user visits CNN.com, the visitor's identity is tracked by Facebook through observing the like button on the CNN website.

5.5.3 Active Warden

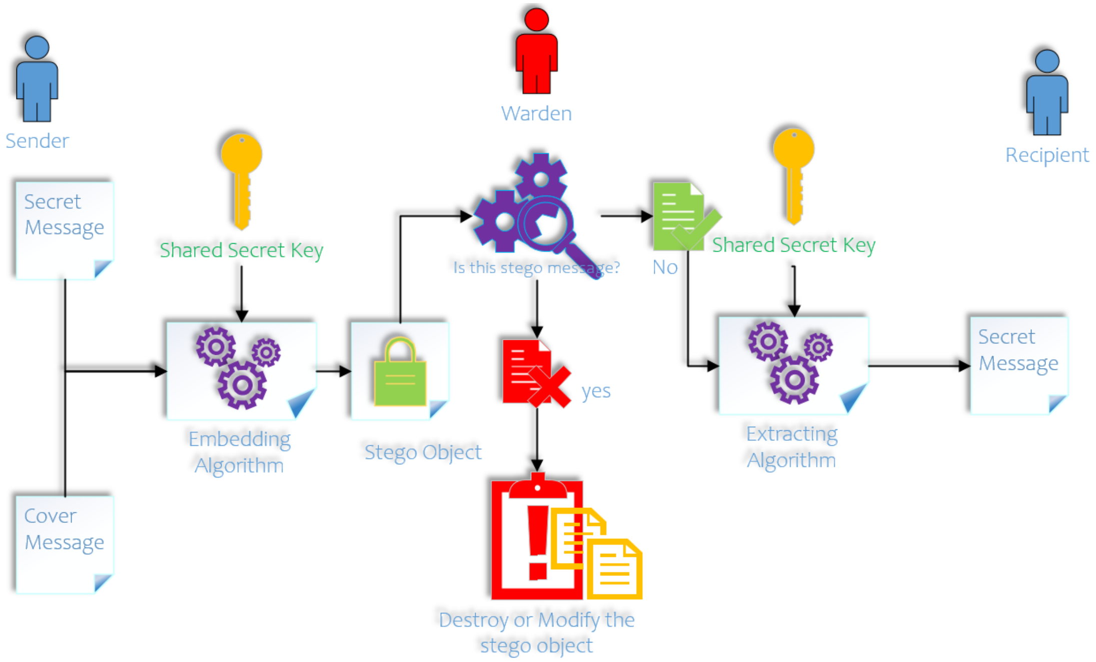


Figure 5.8: Active Warden.

Steganography is a technique considered insecure as soon as the presence of the secret message is detected. This reason is due to the main objective of steganography is to conceal communication. Most of the time, identifying the individuals who use the stego technique to communicate could be significant even though the hidden message may be unknown. If a warden discovers the use of steganography, he could decide to cut or distort the communication channel if he has such capacity.

An active warden is a steganalyst that has the capability to both read and write access to a communication channel C. The warden aims to hinder covert communication by reducing the channel's capacity with a distortion function D^*. Corrupting stego-objects with distortion might adversely affect the legitimate use of a communication channel (e.g. noise). Also, an active Warden can intercept and modify the content in a stego-object. For example, suppose communicating entities are encoding secret messages in images. In that case, the active warden may use statistical analysis in the images by moderately resizing, cropping, and recompressing to prevent the recipient from reading any secret messages.

The Active Wardens considered in the adversarial model are described:

- **External SMS Interceptor:** This entity is considered as an independent adversary (e.g., terrorists and criminals) that has the capacity and resources to intercept, modify and replay private text messages. This entity can use military-grade technologies and devices to actively monitor the complete transmission of SMS text messages without the knowledge of mobile phone users and law-abiding MNOs. This entity could use the StingRay technology device, an IMSI (International mobile subscriber identity) catcher. This technology can maliciously emulate legitimate mobile base stations by causing nearby mobile phones to connect and pass information through them instead of legitimate base stations. This technology is currently used in the United States

[231, 152].

The External SMS Interceptor can also delude subscribers through a spam email or malicious text message to download and install mobile phone spying software. The spying software can record all communications on the installed device [174, 71]. In 2017, the study in [59] proposed a system named Spying Mobrob that enables the tracking of mobile phone users from mobile network operators.

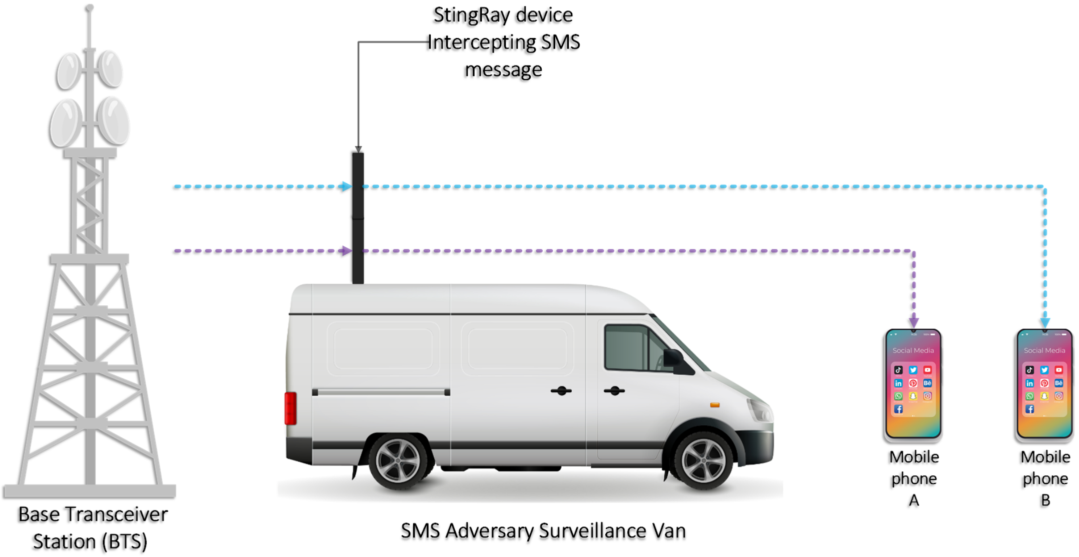

StingRay device Intercepting SMS message
Base Transceiver Station (BTS)
SMS Adversary Surveillance Van
Mobile phone A
Mobile phone B

Figure 5.9: The External SMS adversary in operation with a Stingray device

- **Government:** The government is considered an adversary with access to a wide range of technologies. Among these technologies are suitable for monitoring and intercepting communications on mobile devices. The government has the technological resources to monitor all mobile phone communications within a territory without the consent of mobile phone users. In this adversary model and the case of simplicity, the government is considered an active warden though they have access to passive technologies. For instance, since the early 1990s in the United States, the government has had access to passive telephone surveillance while the active surveillance technologies have been available as early as 1995 [163].

With the use of inexpensive and user-friendly surveillance technologies, most mobile phone surveillance is performed by Government agencies with the collaboration of Mobile Network Operators (MNO) and Internet Service Providers (ISP) [32, 190, 103, 218]. There are instances where the government will collaborate with a third party company such as the NSO group located in Israel. The spyware company sells a surveillance technology known as Pegasus to various governments. This spyware product can covertly infect a user's device and monitor all their activity. In most cases; usually, the adversary can access a target's text messages, phone calls, internet search, location, and stored data undetected. A challenging aspect of the Pegasus spyware is the ability to be undetected by antivirus and anti-malware [242, 51].

However, there are some situations where the government would want to perform direct, unmediated mobile phone surveillance themselves [124, 163, 165]. These situations include Identifying unknown phones currently used by a known target, Locating devices that cannot be found by the wireless carriers, blocking devices or dialled numbers selectively and performing foreign intelligence and military operations. In cases by assumption where the MNOs refuse to collaborate with the government, they can be forced to do so.

5.6 Protocol Design

This chapter recalls from Chapter 4 that the essential idea that supports this novel research domain is to adopt systematic protocols that were initially developed to provide confidential communication through medial social platforms [26, 47, 63, 170] to an SMS mobile banking environment.

Though the publications [63], [47] and [26] inspire the protocol described in this section with significant differences. Instead of using a secret sharing scheme in [63], which requires non-trivial computations, a simple binary XOR operation achieves the same level of security and the only small reduction in redundancy due to the use of secret splitting. Secondly, instead of using the combination of the low entropy steganography and encryption approach in [26], the protocol described in this chapter combines both the low entropy steganography and high steganography without the use of symmetric nor asymmetric key infrastructure and trusted third parties. Thirdly, instead of using the dual non-colliding channels as in [47], the protocol described in this chapter uses three independent non-colliding channels. The additional channel adds a layer of security to make a challenging task for any adversary that wishes to hinder security. The low entropy approach adopted in this chapter can be classified as steganography by cover synthesis. In contrast, the high entropy steganography approach can be classified as steganography by cover modification described in Chapter 2.

In this section, we design our multi-channel SMS banking protocol. Our approach is, to our knowledge, the first work that achieves secure transactions using a combination of low- and high-entropy steganographic models.

5.6.1 System Overview

The system overview consists of the essential core participants such as the user customers (in our example, Amara and Ebere), the mobile network operators and the bank. Users may act as payers or payees and are required to register with the SMS banking service through their bank. The sim cards and phone numbers should be associated with their bank account during banking registration. Customers are also required to subscribe to the GSM network through the mobile network operator, providing customers with SMS services. All SMS payment requests are transmitted to the bank through two mobile phones, operated by two distinct mobile service providers. The third channel requires the issuer bank and customer to have a public Internet connection.

Our proposed protocol neither requires specific software to be installed on the mobile phone nor an expensive mobile phone (smart-phone) to be available. In order to be able to use our mobile banking protocol, customers only need access to an affordable dual SIM phone capable of sending SMS. For example, the Nokia 105 DUAL SIM is such a device, available for a reasonable price.

5.6.2 Protocol Description

Let Amara be a sender wanting to transfer money to Ebere's account through the Bank. Let $\mathcal{M}$ be the set of all possible messages, $\mathcal{B}$ a set of bit strings and C the set of all channels. The functions Enc and Dec are stego-encoding and stego-decoding functions respectively.

Let $m \in \mathcal{M}$ be an SMS message, and $b \in \mathcal{B}$ be a binary value used for the protocol.

$$\begin{tikzcd}
\mathit{Amara} & & \mathit{Bank} \\
\{m,\, m_1,\, m_2\} & & \\
m_1 \arrow[rr, "m_1", "C_1"'] & & m_1 \\
m_2 \arrow[rr, "m_2", "C_2"'] & & m_2 \\
b = m \oplus m_1 \oplus m_2 & & \\
m_3 = \mathsf{Enc}(b) & & \\
m_3 \arrow[rr, "m_3", "C_3"'] & & m_3 \\
 & & b = \mathsf{Dec}(m_3) \\
 & & m = b \oplus m_1 \oplus m_2
\end{tikzcd}$$

Figure 5.10: A Multi-Channel Steganographic Network Protocol Trace (a).

The channels $C_i \in C$ $(i = 1, 2)$ denote two independent mobile wireless channels, implemented through suitable Mobile Network Services. The channel $C_3 \in C$ is a (not necessarily secure) internet connection.

The messages m_1 and m_2 are pseudo, unsuspicious SMS messages and m_3 is a stego-object (e.g. image), using a suitable high-entropy stego-system, e.g. LSB hiding. We may use different mechanisms to implement C_3; we propose using a picture-upload facility on the Bank's public website, where users can share ”happy customers” pictures. This approach does not require a secure connection and would not raise suspicion.

If a payer Amara wishes to transfer money to a payee Ebere via her Bank, the following steps of our multi-channel protocol are executed:

1. Amara creates an SMS banking instruction message $m \in \mathcal{M}$.
2. She also generates two fake unsuspicious banking instructions m_1 and m_2.
3. The messages m_1 and m_2 are transmitted to the bank over two independent mobile wireless channels C_1 and C_2 respectively. An monitoring adversary trying to initiate a malicious activity will believe that the SMS banking instructions are genuine.
4. Subsequently, Amara will independently computes $b = m \oplus m_1 \oplus m_2$. The computation of b is independently implemented with a separate algorithm and system.
5. The binary value b is concealed in a stego object (image) using an LSB hiding map $b \longmapsto m_3$.
6. m_3 is sent to the bank over an insecure public network (through a cyber cafe) channel.
7. On receiving m_3 and extracting b, the bank can recover m by computing $b \oplus m_1 \oplus m_2$.
8. The bank can now transfer Amara's requested amount to Ebere's account.
9. Finally, an SMS notification is sent to Ebere.

The Figure 5.10 and Figure 5.11 illustrates protocol trace and system overview.

The messages m_1 and m_2, transmitted over C_1 and C_2 respectively, is considered a low entropy steganographic system. On the other hand, m, m_1 and m_2 concealed within the

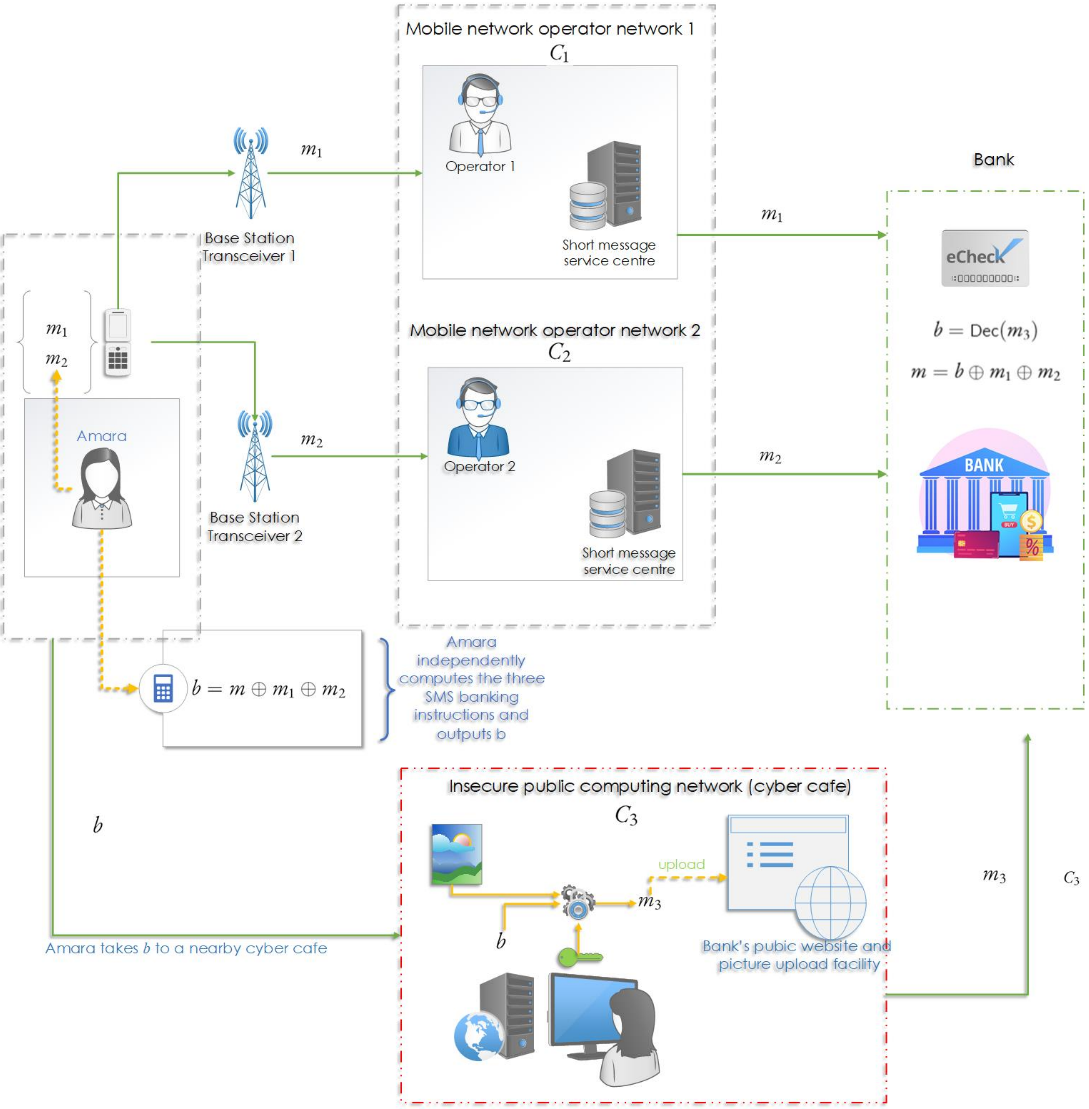

Mobile network operator network 1
C_1
Operator 1
Short message service centre
m_1
Base Station Transceiver 1
m_1
m_2
Amara
Mobile network operator network 2
C_2
Operator 2
Short message service centre
m_2
Base Station Transceiver 2
m_2
Bank
eCheck
$b = \mathrm{Dec}(m_3)$
$m = b \oplus m_1 \oplus m_2$
BANK
$b = m \oplus m_1 \oplus m_2$
Amara independently computes the three SMS banking instructions and outputs b
b
Amara takes b to a nearby cyber cafe
Insecure public computing network (cyber cafe)
C_3
upload
m_3
b
Bank's pubic website and picture upload facility
m_3
C_3

Figure 5.11: A detailed Multi-Channel Steganographic Protocol System Overview

cover object m_3 and transmitted over C_3 is considered a high entropy steganographic system. An important security property of this protocol is that it achieves the concept of indistinguishability presented in Chapter 3 of this thesis. In the steganographic protocol proposed in this chapter, indistinguishability is the inability of an adversarial entity to distinguish between a pseudo SMS banking instruction and a genuine SMS banking instruction. The task of distinguishing between a pseudo SMS banking instruction and a genuine SMS banking instruction is very challenging because the pseudo SMS banking instruction follows the format of a genuine SMS banking instruction. The reason for using a pseudo SMS banking instruction is to disguise the real banking information and hide payment information (for example, payment amount, payee and possibly bank name). If adversarial entities see payment details of banking transactions, this information can be used for malicious reasons (for example, marketing, targeted advertisement and data mining without authorisation).

Besides, it is possible only to use a cover object for steganography across a channel (e.g., an SMS text message transmitted on a socially constrained channel). If the adversary sees the message as unsuspicious, steganography has taken place without notice. In this instance, only a cover medium has been used for steganography. The adversary cannot distinguish between a stego-object, a cover medium and a generic message. The multi-channel steganographic SMS based banking protocol is defined and summarised in definition 5.6.1. The definition is a generic definition that combines the high entropy and low entropy steganographic system.

Definition 5.6.1. *(Multi-channel entropy scheme for SMS banking): A multi-channel secure SMS steganographic banking system is a Stego-system $\mathcal{S}$, that is considered a hybrid, a high entropy $\mathcal{S}^h$ and a low entropy stego-system $\mathcal{S}^l$. This hybrid entropy system consists of five efficient algorithms and three independent non colluding wireless channels. The five efficient algorithms consists of a generator* $\mathsf{Gen}(\lambda)$*, probabilistic encoding function* $\mathsf{Enc}(\cdot)$*, a deterministic decoding function* $\mathsf{Dec}(\cdot)$*, a deterministic transmission algorithm* $\mathsf{Trans}(\cdot,\cdot)$ *and an* $\mathsf{Xor}(\cdot,\cdot,\cdot)$ *algorithm.*

- $\mathsf{Gen}(\lambda)$: *According the security parameter λ outputs $\{m, m_1, m_2\} \longleftarrow \lambda$ through a* *mobile phone.*

- $\mathsf{Trans}(\cdot,\cdot)$: *$C_1$ and C_2 takes two pseudo banking instructions m_1 and m_2 respectively, and transmit to an intended recipient (Bank).*

- $\mathsf{Xor}(\cdot,\cdot,\cdot)$: *Takes as an input m_1, m_2 and the real message m, calculate with the algorithm* (Xor) *operator and return b.*

- $\mathsf{Enc}(\cdot)$: *Takes as input b and outputs m_3 such that $m_3 \longleftarrow \mathsf{Enc}(b)$.*

- $\mathsf{Dec}(\cdot)$: *Given a deterministic decoding function, b is extracted from m_3.*

- $\mathsf{Xor}(\cdot,\cdot,\cdot)$: *The secret message **m** is reconstructed by calculating $b \oplus m_1 \oplus m_2$.*

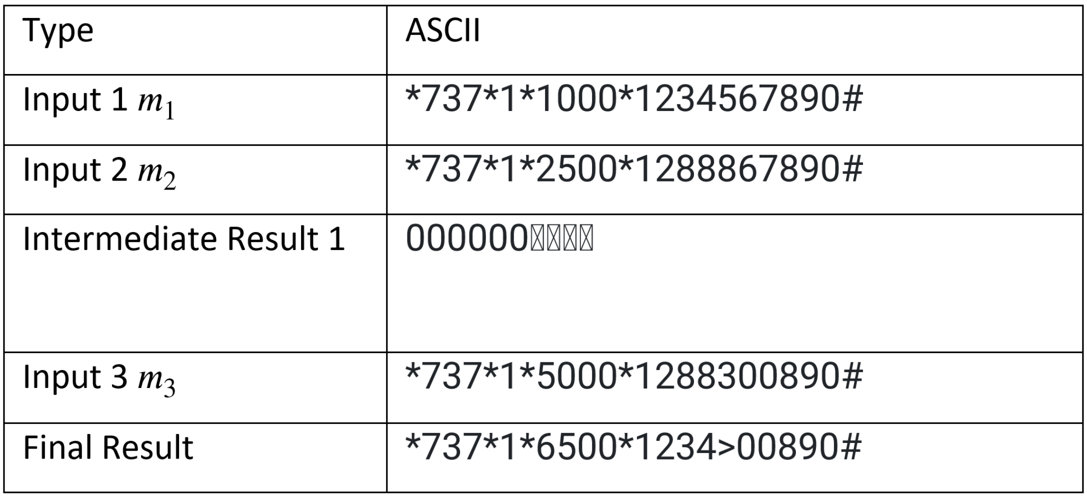
An SMS banking instruction (usually called Unstructured Supplementary Service Data (USSD) Codes) has various specific formats, depending on the bank [98] [216] [70] [1] [64] [230] [79]. For instance, in a developing country like Nigeria, the Guaranty Trust Bank (GTB) SMS banking instruction for money transfer within the same bank has the following format: $^*737^*1^*$*Amount***NUBAN Account Number*# (e.g. $^*737^*1^*1000^*1234567890$ #) from the phone number you registered with GTBank. While the format for money transfer to another bank is $^*737^*2^*$*Amount***NUBAN Account Number*# (e.g. $^*737^*2^*1$ $000^*1234567890$#) from your registered phone, then authenticate the transfer with a hardware token, create 737 PIN, or last four digits of your GTBank debit card [79]. An SMS banking instruction in such a format would be suitable for the proposed protocol. Table 5.1 describes the SMS banking format from various banks.

In the steganographic protocol, the messages m_1 and m_2 can be encoded in such a manner that makes it challenging for an adversarial to distinguish. In the worked example in table

BANKS	Fund transfer to same bank	Fund transfer to other banks
Union Bank	*826*1*Amount*Account Number#	*826*2*Amount*Account Number#
Stanbic IBTC Bank	*909*11*Amount*Account Number#	*909*22*Amount*Account Number#
First Bank Nigeria	*894*Amount*Account Number#	*894*Amount*Account Number#
Access Bank	*901*1*Amount*Account Number#	*901*2*Amount*Account Number#
United Bank for Nigeria	*919*3*Account Number*Amount#	*919*4*Account Number*Amount#
Guaranty Trust Bank	*737*1*Amount* Account Number#	*737*2*Amount*AccountNumber#

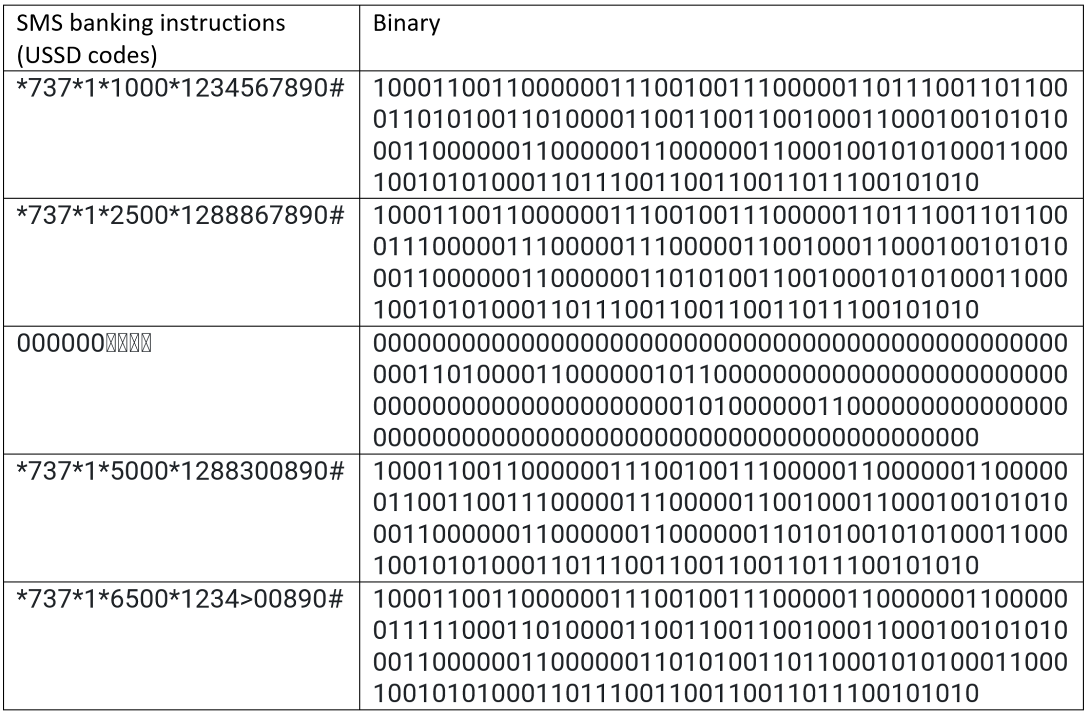
Table 5.1: SMS Banking Unstructured Supplementary Service Data (USSD) Codes

5.12 and 5.13, the pseudo USSD codes *737*1*1000*1234567890#, *737*1*2500*1288867890# can be XORed with an actual USSD code *737*1*5000*1288300890# to produce *737*1*6500*1234 > 0089#. Though the resulting output *737*1*6500*1234 > 0089# may not be random enough and could result in an attack such as brute force or guessing attacks. Therefore results such as 0*737*1*2200*912 <: 47 :>?) in the figure would make a more challenging task for an adversary to break or guess correctly.



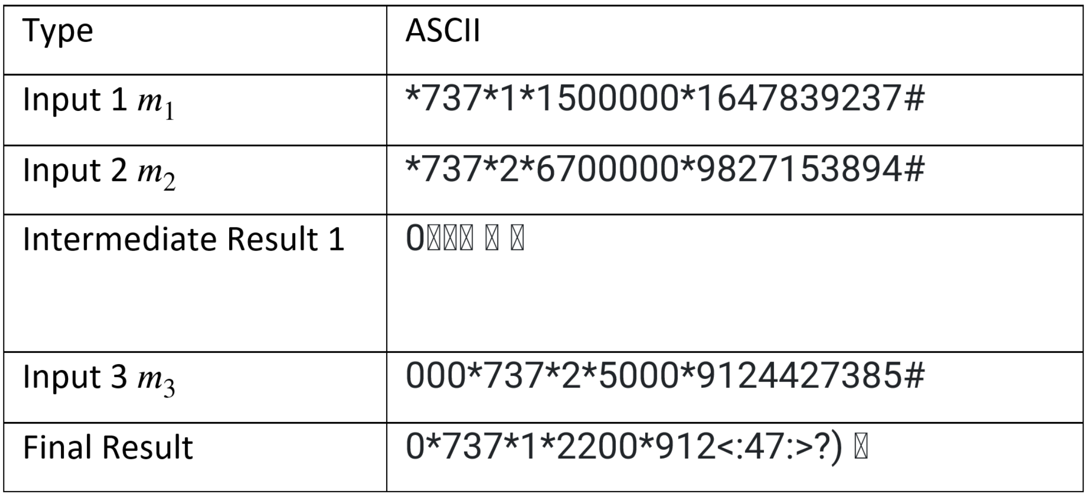
Type	ASCII
Input 1 m_1	*737*1*1000*1234567890#
Input 2 m_2	*737*1*2500*1288867890#
Intermediate Result 1	000000⊠⊠⊠⊠
Input 3 m_3	*737*1*5000*1288300890#
Final Result	*737*1*6500*1234>00890#

Figure 5.12: A Multi-Channel Steganographic Protocol Worked Example (a).



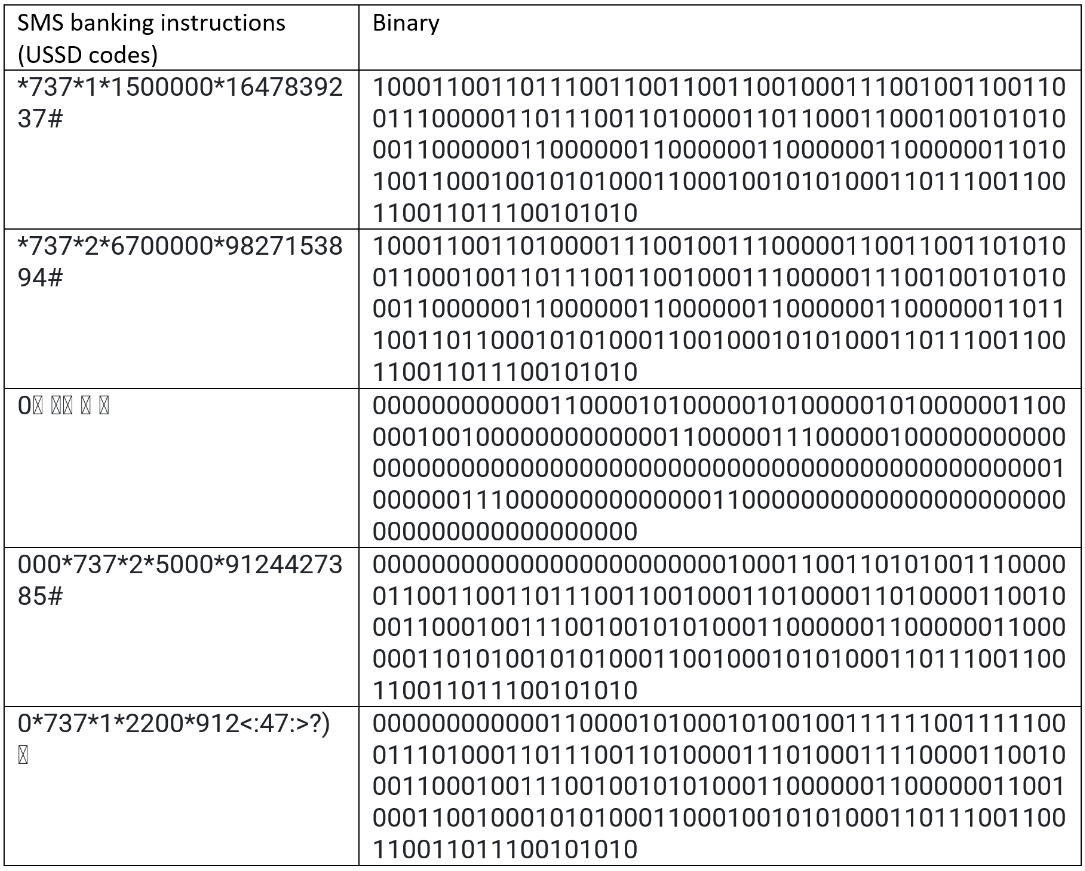
SMS banking instructions (USSD codes)	Binary
*737*1*1000*1234567890#	1000110011000000111001001110000011011100110110001101010011010000110011001100100011000100101010001100000001100000001100000001100010010101000110001001010100011011100110011001101110010101 0
*737*1*2500*1288867890#	1000110011000000111001001110000011011100110110001110000001110000001110000001100100011000100101010001100000001100000001101010011001000101010001100010010101000110111001100110011011100101010
000000⌧⌧⌧⌧	0000000000000000000000000000000000000000000000001101000011000000101100000000000000000000000000000000000000000000001010000001100000000000000000000000000000000000000000000000000000000000000
*737*1*5000*1288300890#	1000110011000000111001001110000011000000110000001100110011100000011100000011001000110001001010100011000000011000000011000000110101001010100011000100101010001101110011001100110111001010 10
*737*1*6500*1234>00890#	1000110011000000111001001110000011000000110000001111110001101000011001100110010001100010010101000110000000110000001101010011011000101010001100010010101000110111001100110011011100101010

Figure 5.13: A Multi-Channel Steganographic Protocol Worked Example (b).



Type	ASCII
Input 1 m_1	*737*1*1500000*1647839237#
Input 2 m_2	*737*2*6700000*9827153894#
Intermediate Result 1	0⌧⌧⌧ ⌧ ⌧
Input 3 m_3	000*737*2*5000*9124427385#
Final Result	0*737*1*2200*912<:47:>?) ⌧

Figure 5.14: A Multi-Channel Steganographic Protocol Worked Example (c)



SMS banking instructions (USSD codes)	Binary
*737*1*1500000*1647839237#	10001100110111001100110011001000111001001100110011100000110111001101000011011000110001001010100011000000011000000110000001100000011000000110101001100010010101000110001001010100011011100110011001101110010101 0
*737*2*6700000*9827153894#	100011001101000011100100111000001100110011010100110001001101110011001000111000001110010010101000110000000110000001100000011000000110000001101110011011000101010001100100010101000110111001100110011011100101010
0⌧ ⌧⌧ ⌧ ⌧	000000000000110000101000000101000000101000000110000010010000000000000011000000111000000100000000000000000000000000000000000000000000000000000100000001110000000000000011000000000000000000000000000000000000000
000*737*2*5000*9124427385#	000000000000000000000000100011001101010011100000110011001101110011001000110100001101000011001000110001001110010010101000110000000110000001100000011010100101010001100100010101000110111001100110011011100101010
0*737*1*2200*912<:47:>?) ⌧	000000000000110000101000101001001111110011111000111010001101110011010000111010001111000011001000110001001110010010101000110000000110000001100100011001000101010001100010010101000110111001100110011011100101010

Figure 5.15: A Multi-Channel Steganographic Protocol Worked Example (d)

In order to successfully encode an SMS banking instruction in an image, the stego-medium should have the capacity to contain the banking instruction as explained in definition 5.4.1. Also, the SMS banking instruction length needs to be optimally small enough to be contained in an image. In the first instance, the maximum payload of a single SMS is 160 characters of 7-bit encoding. That is 1120 bits / (7 bits/character) = 160 characters for a single SMS message for GSM, and it also means that 7-bits is used to encode a single character. In UTF-16, 16 bits are used to encode a character while, in UTF-8, 8 bits are used [38]. In this thesis, the use of the 7-bit encoding is considered since the protocol requires the customer to register for GSM services, which is cost-effective.

Since the SMS banking instruction examples in figures 5.12-5.15 has 23 characters, then the size of an SMS banking instruction transmitted independently across channel c_1 and c_2 will be 161-bits=0.0196 KB for storage and 0.020125 KB for network transmission and using the following formula:

$$TS = N_b \times N_c$$

The notation TS is the Text File Size, N_b is the number of bits per character, and N_c is the number of characters. Therefore, suppose an image of 800×600 with a size of 576KB or 1200×900 with a size of 1.14KB is used to encode a text, the optimal size of the text should be 175KB or 2.10KB to be contained effectively [75]. Any of these image sizes would be suitable for the practical implementation of the protocol.

5.7 Security Analysis

In this section, we analyse the security of our protocol against various adversaries that would be to be expected in a real-world scenario.

The fundamental security assumptions of the protocol are that the bank is considered to be trusted, and we exclude attacks by its customers as well. On the other hand, the cyber-café, the mobile operator(s) and potentially even the government cannot be trusted as they might wish to access communication records. They could carry out passive or active attacks such as eavesdropping, man-in-the-middle attacks or steganalysis. One individual adversary could make attacks, or adversaries could conspire together (collaborative attack).

The security analysis of our protocol is presented by measuring the advantage the adversaries have in winning the STEGO-game. The four adversaries analysed in this section has access to an oracle $\mathsf{O}(\cdot,\cdot)$, this will give them an advantage in winning the STEGO-game. The External SMS interceptor analysis is initially analysed, followed by the mobile network operators-employees and management. Afterwards, the cybercafe users and owners are analysed. Finally, we analyse the ISP of the cybercafe and the government.

5.7.1 External SMS Interceptor

The External SMS Interceptor is an adversary that could intercept or modify our SMS banking instruction in an insecure GSM network. Without loss of generality, this adversary is assumed to have the capacity to monitor only one channel externally. However, due to the genuine-looking format of the banking instruction, the adversary will not suspect its content to be pseudo, and the intercepted information will be believable. If this adversary pretends to be a legitimate sender and modifies m_1 to $\hat{m}_1$, he will, at the worst, interrupt the scheme. The bank will detect this attack, as the reconstructed real message m will not make sense. Also, it means that the External SMS interceptor can win the STEGO-game with a probability of $\frac{1}{2}$, and the protocol is secure under this adversary.

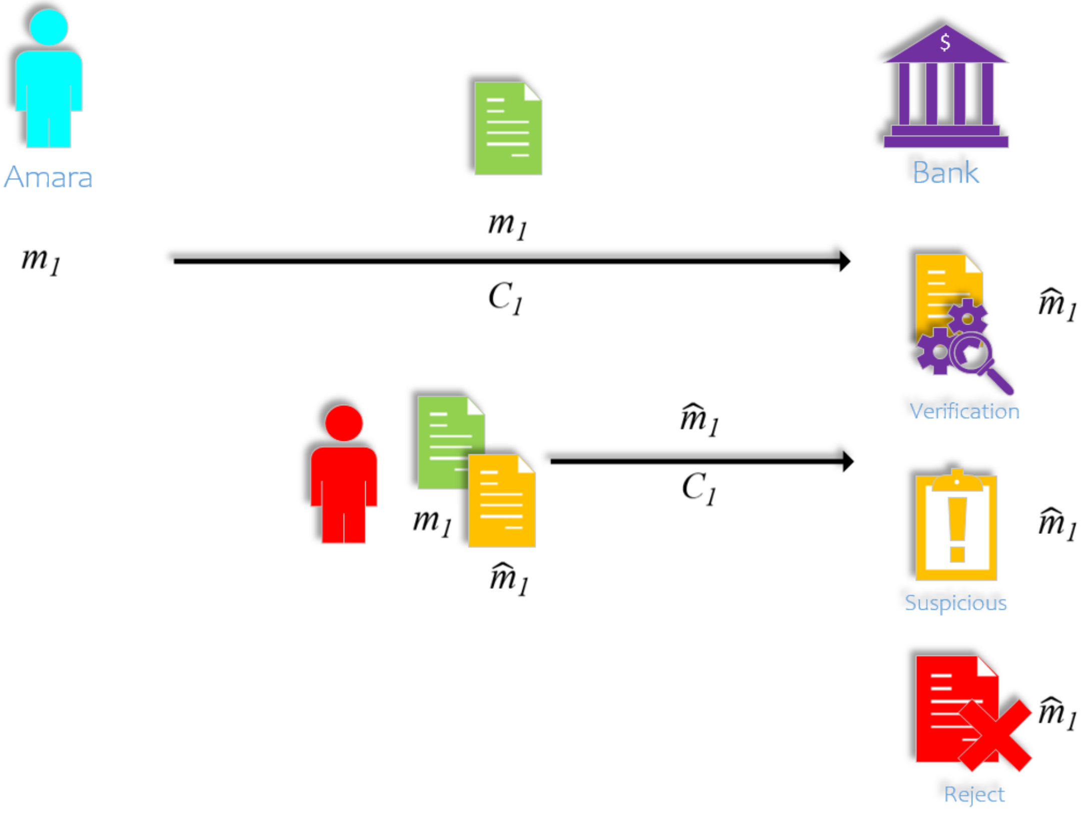


Figure 5.16: External SMS Interceptor Replay Attack

Game 1: Let a Multi-channel-entropy stego-scheme $\prod \leftarrow (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Xor})$ be STEGO secure against an attack, if no probabilistic polynomial time adversary (PPT) A has a non-negligible advantage against the challenger Chal.

Let Amara be the challenger Chal and the External SMS Interceptor adversary be A. The game proceeds as follows:

- Init : The challenger uses $\mathsf{Gen}(\cdot)$ to output a security parameter λ.
- Setup : *The adversary* A *has access to a channel oracle* $\mathsf{O}(\cdot,\cdot)$ *which samples one after another, blocks from the channel distribution* C_1 *and it's history* h*. The adversary is allowed to make as many draws from* $\mathsf{O}(c,h)$ *as it wishes.*
- $\mathsf{Phase\,1}$: *The adversary* A *issues* q *queries to* $\mathsf{O}(c,h)$ $m_1.....m_q$*, where each query* m_i *is a hidden text in* $\mathcal{M}$.
- $\mathsf{Challenge}$: *Eventually, the challenger* Chal *submits to* A *a pseudo banking messaging instruction* m_1.
- Guess : A *is faced with a stego-decision problem which is to discern if the message* m_1 *is a genuine banking instruction or a pseudo banking instruction.*
- A *outputs a bit b, where* $b = 1$ *if he wins the game*

5.7.2 Mobile Network Operators – Employees and Management

This adversary entity has access to all text messages transmitted across the mobile network channel. Suppose the management of the mobile network operators is genuine and not aware of the malicious activities that an employee could commit. In that case, unauthorised modification and interception of transmitted data could be achieved. However, if both adversaries intercept m_1 and m_2 independently or even when colluding, m_3 remains secret, they can only cause a (detectable) interruption of the protocol.

The security analysis of this adversary is further explained in the following STEGO game. The game expresses the inability of this adversary to distinguish between pseudo banking instruction and real banking instruction.

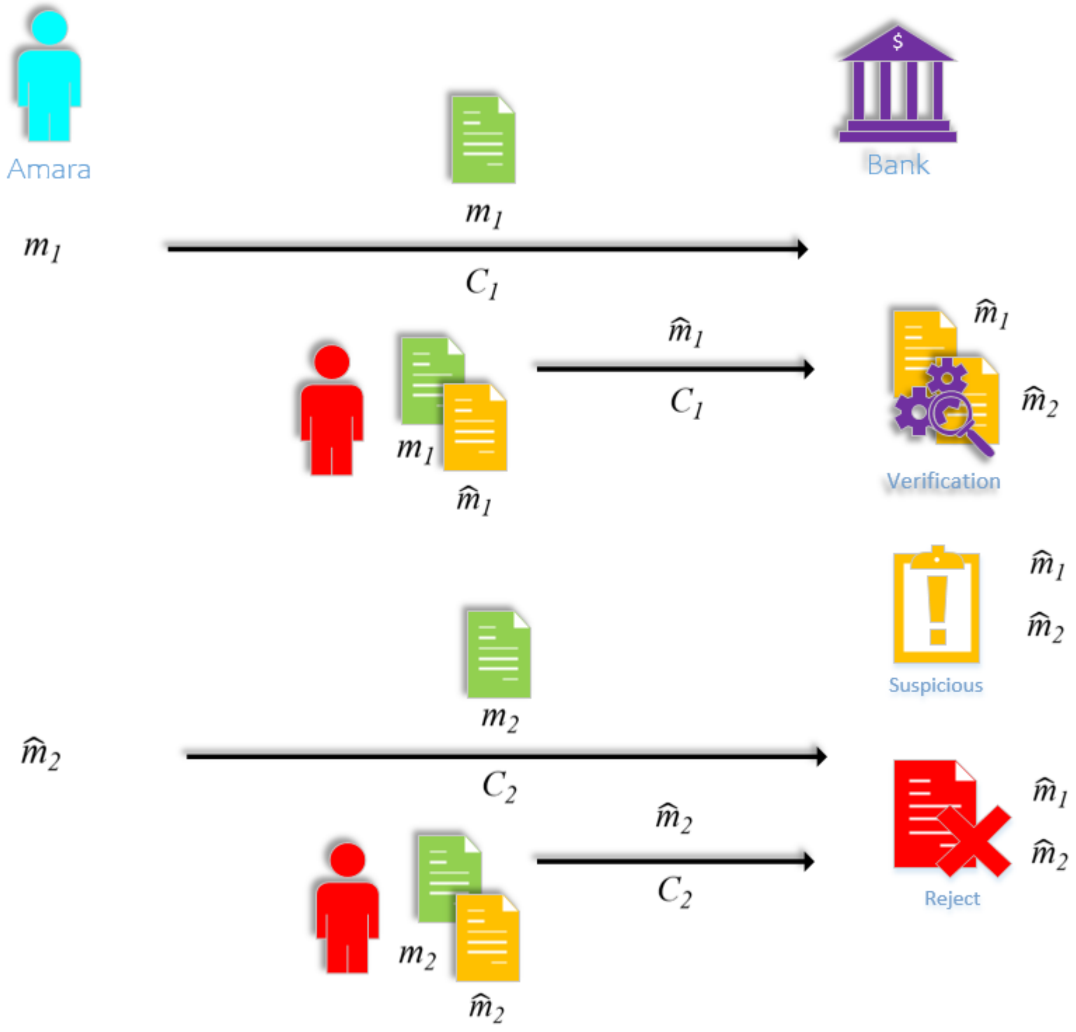


Figure 5.17: Mobile Network Operators – Employees and Management Replay Attack

Game 2: Let a Multi-channel-entropy stego-scheme $\prod \leftarrow$ (Gen, Enc, Dec, Xor) be STEGO secure against an attack, if no probabilistic polynomial time adversary (PPT) A has a non-negligible advantage against the challenger Chal.

Let Amara be the challenger Chal and the Mobile Network Operators adversary be A. The game proceeds as follows:

- Init : *The challenger* Chal *uses a function to output a security parameter* $\lambda \leftarrow \mathsf{Gen}(\cdot)$.
- Setup : *The adversary* A *has access to a channel oracle* $\mathsf{O}(\cdot,\cdot)$ *which samples one after another, blocks from the channel distribution* C_1, C_2 *and their history* h. *The adversary is allowed to make as many draws from* $\mathsf{O}(c,h)$ *as it wishes.*
- $\mathsf{Phase\ 1}$: *The adversary* A *issues* q *queries to* $\mathsf{O}(c,h)$ $m_1.....m_q$*, where each query* m_i *is a hidden text in* $\mathcal{M}$.
- $\mathsf{Challenge}$: *The challenger* Chal *outputs two pseudo banking messaging instructions* m_1 *and* m_2.
- $\mathsf{Phase\ 2}$: *The adversary* A *performs a series of computation*.
- Guess : *The adversary is faced with a stego decision problem which is to distinguish if the messages* m_1 *and* m_2 *are stego-messages or cover-messages.*
- A *outputs a bit* b*, where* $b = 1$ *if and only if he wins the game*.

Though the Mobile Network Operators has full access to the pseudo banking instructions, it is impossible to distinguish if the text messages are stego-messages or cover-message. A pseudo banking instruction sent by an SMS subscriber to a bank can be seen as a generic innocent message that does not raise suspicion. The MNO can only win with a probability of $\frac{1}{2}$, and the stego-system is secure under the MNO adversary.

5.7.3 Cybercafé Users and Owner

Various attacks could be carried out by other users of the cybercafé, or potentially its owner. Negligence could potentially contribute to various threats. These threats could be malware that could lead to unauthorised disclose in public cybercafés. Amara could be monitored by a malware or hardware device such as a key-logger.

However, the impact of these attacks is the same as that of the SMS interceptor attack.

5.7.4 ISP of Cybercafé and Government

The most potent attackers, however, are the Internet Service Provider (ISP) of the Cybercafé or even the Government, who might, using relevant legislation, have access to connection details and traffic information. This thesis assumes that the ISP and Government have all the capabilities to monitor specific traffic of users connected to the internet; this thesis further assumes that the ISP and Government monitor the channel C_3. It is possible for both adversaries will see that Amara connects to a specific internet connection at a public and insecure cybercafe. These two adversarial entities will collaborate by using available technologies to recover the secret banking instruction m.

Game 3: Let $\prod \longleftarrow (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a Multi-channel-entropy stego-scheme that is STEGO secure against a capable adversary A. However, A is bounded within a probabilistic polynomial time (PPT) with a negligible advantage against the challenger Chal.

Let Amara be the challenger Chal. Let the ISP and Government adversary be A with

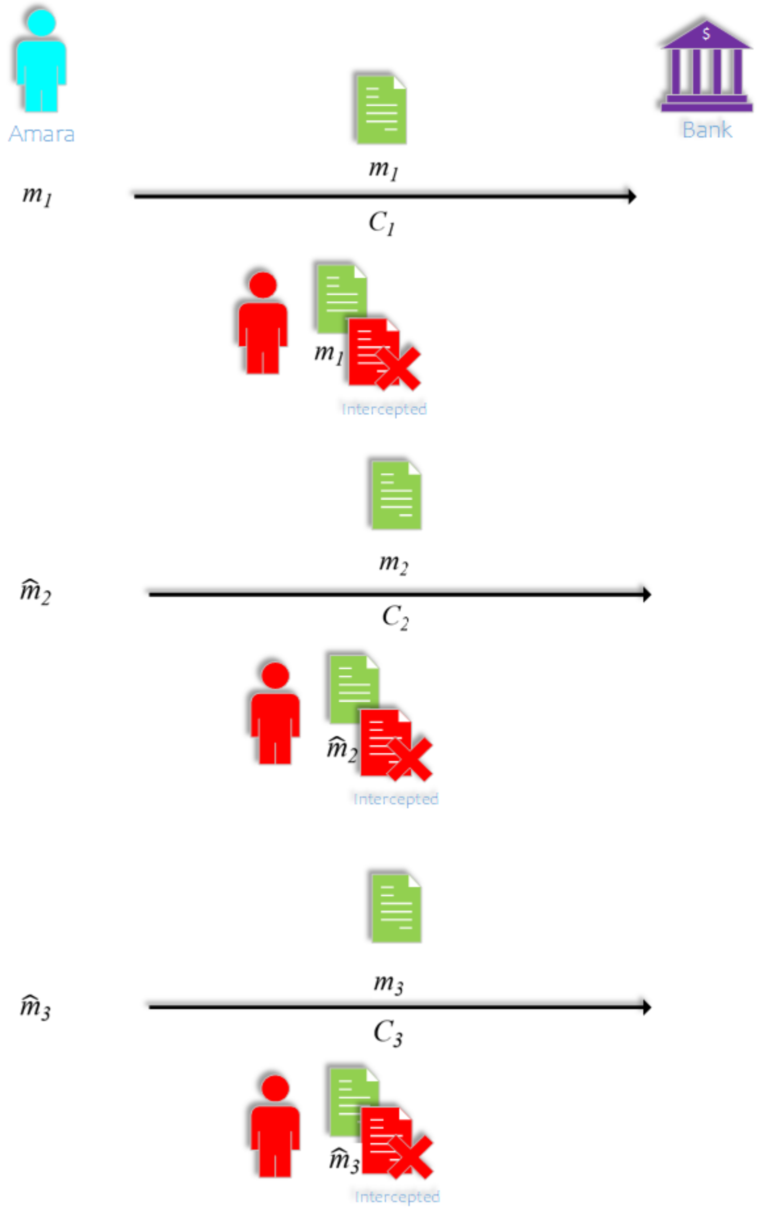


Figure 5.18: Multi-channel man in the Middle Attack.

access to a stego-oracle O. The game proceeds as follows:

- Init: *The challenger* Chal *uses a crypto function* $\mathsf{Gen}(\cdot)$ *and a security parameter* λ *to output a symmetric stego-key* $k \longleftarrow \{0,1\}^{\lambda}$*.* Chal *gives the resulting key* k *and the* *params to the adversary* A.

- Setup: *The adversary* A *has access to a stego-oracle* $\mathsf{O}(c, h)$ *that has* $s_i \longleftarrow \mathsf{Enc}(\cdot,\cdot,\cdot)$ *and* $m_i \longleftarrow \mathsf{Dec}(\cdot,\cdot,\cdot)$ *capabilities, were h is the history of* c_3.

- $\mathsf{Phase\ 1}$: *The adversary* A *issues* q_1 *queries to* $\mathsf{O}(C, h)$ $o_1.....o_q$, *where each stego-object* o_i *is drawn from* $\mathsf{Enc}(k, m_i, h)$.

- $\mathsf{Phase\ 2}$: *The challenger* Chal *independently computes* $b \in \{0, 1\} \longleftarrow m \oplus \cdot \oplus \cdot$.

- $\mathsf{Challenge}$: *The challenger* Chal *picks a random bit* $n \in \{0, 1\}$, *independently uses* $\mathsf{Enc}(\cdot,\cdot)$, *a deterministic function to output* $m_3 \longleftarrow \mathsf{Enc}(k, b)$ *and publish* m_3 *to the adversary* A.

- $\mathsf{Phase\ 3}$: *The adversary* A *initiates decoding queries* q_2 *to* $\mathsf{O}(c, h)$ *in order to retrieve* m.

- Guess: *The adversary outs a bit* n' *and wins if he successfully retrieves* m *else, the advantage of* A *is negligible.*

However, if all three channels C_1, C_2 and C_3 can be intercepted simultaneously, the message m can be reconstructed or altered, and the protocol is compromised.

5.8 Summary

This chapter proposes a novel secure SMS banking protocol that combines low and high entropy steganography. This approach has been influenced by previously suggested OSN multi-channel security protocols and protocols used in ad-hoc networks. One of the critical features of this protocol is its steganographic confidentiality property against the malicious mobile network operator, malicious employees at the mobile network operators and the external SMS interceptor, which, to our knowledge, is a novel feature.

The summary of the advantages and limitations of this protocol are as follows.

5.8.1 Advantages

1. Our steganographic protocol does not use encryption and hence does not require the bank to exchange a secret key with customers. The need for a security infrastructure such as Trusted Third Parties or cryptographic Public-key Infrastructures does not arise.

2. The architecture is straightforward and cheap to implement and could be deployed very rapidly. In terms of infrastructure, it only requires GSM (2G) services and one additional internet connection, which can be insecure. It would be suitable, for example, in rural areas or countries without individual secure home internet connections for users who do not have access to modern smartphones and more sophisticated secure banking mobile apps.

3. One would wonder why SMS banking subscribers would want to initiate secure trans-

actions using our protocol instead of using an encrypted channel or encrypted SMS. Although, aside from convenience, one might want to use our approach. Initiating transactions directly at the bank might not be available at all times. Given that a payer wants to transfer money to a payee, the money could be transferred via traditional online banking or a secure native mobile banking application. There are various scenarios where this would be convenient. Nevertheless, if the payer and payee want to conceal that they are initiating secure transactions, then our protocol is suitable.

5.8.2 Limitations

1. For this protocol to be successful, users require a dual SIM phone (or two mobile devices).

2. If an attack is made only on one or two channels, then the private SMS banking instruction m remains secret. However, if adversaries could collude and intercept or modify all three channel c_1, c_2 and c_3, then the secret message m can be reconstructed or altered, and the protocol is compromised.

3. The protocol can be interrupted by modification attacks on the individual channels; however, the bank will detect the interruption if implemented appropriately.

Chapter 6

Ensuring Message Freshness and Integrity in A Multi-Channel SMS Steganographic Banking Protocol

In this chapter, we improve on the SMS banking protocol presented in Chapter 5. After analysing the security of this prototype protocol, we address the threat of a multi-channel replay attack and multi-channel man-in-the middle attack. We postulate that the resulting, strengthened protocol is secure and robust for use in real-world scenarios.

6.1 Motivation

The Short Message Service (SMS) is a popular and fundamental service in mobile cellular networks, which is supported by 7.4 billion mobile devices as of 2014 [229]. This mobile service is not only for personal usage, but also used by various industrialised SMS powered services such as social networking (e.g., Facebook, Twitter, Whatsapp), Transport Information Systems [13], health [232] [116], Election Participation [56] [54], Crime Scene Investigation [147], and Mobile Banking [34].

Specialised Mobile Banking Services such as SMS based banking enable banks to offer their customers the flexibility of financial and non-financial transactions which can be classified as Push and Pull services respectively. Although SMS messages are designed by default to transmit non-sensitive messages over a mobile communication network and the SMS encryption algorithm (A5 stream cipher) is insecure. This insecurity, however, has induced a legacy of security concerns, many of which pertain to the confidentiality and integrity of SMS transmission [77] [150] [160]. The research in [228] presented some concerns regarding the extensive functionality of SMS which can incapacitate all voice communications in a metropolitan area, and in [247], threats such as SMS-based mobile bot-net known as Android bot-net [82] were discussed. SMS messages are transmitted on mobile networks as plaintext between the SMS Centre (SMSC) and Mobile Subscriber (MS).

The SS7 is a mobile network component that interconnects mobile networks together. Companies and researchers have described several attacks on the SS7-MAP protocol. For example, a time interrogation technique is used to gain and disclose subscriber information which enables an adversary to send malicious SMS to victims. Technologies such CAMEL enables an adversary to intercept SMS during transmission [67] [182] [91]. Additionally, SMS contents are stored in the systems of network operators and can be read by their personnel [196].

To mitigate these security concerns in SMS, the study in [196] described an end-to-end secure EasySMS protocol based on MAES (modified AES). The protocol sends less number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption. Subsequent solutions in [45] proposed a secure Verifiable Hash Convergent Group Signcryption (VHCGS) framework for group-to-group SMS transmission. In this protocol, the service provider makes a ciphertext verification with a specific protocol. The service uses a protocol that is known as Partial-Unsigncryption Protocol.

In Chapter 5 of this thesis, a novel cryptographic protocol based on steganography was described, which achieves covert communication using three insecure channels. The steganographic technique of the protocol combines both steganography by cover synthesis and cover modification. When used in a mobile banking setting, compared to previous approaches, one of its main advantages is that encryption is not utilized, therefore, the need for a secret key exchange or trusted third parties does not arise. Another advantage of this protocol is its confidentiality property against the external SMS adversary and mobile phone operator. However, there are significant security threats regarding SMS messages transmitted across all three channels.

Networks and data are vulnerable to different types of threats such as replay attack, man-in-the-middle attack, eavesdropping, compromised-Key attack, and spoofing if there are no security schemes in place. To Prevent such threats in a system will require techniques such as encryption, steganography and secret sharing could be utilized. In this paper, we are concerned with a cryptographic protocol design to prevent threats such as the multi-channel replay attack and multi-channel man-in-the middle attack.

6.2 Chapter Contributions

The main research contribution of this paper is a more robust version of the protocol that we initially presented in Chapter 5. The new design aims to mitigate three-channel replay attack and three channel man-in-the-middle attack, as a result of this providing messaging freshness and integrity for the SMS banking transactions. At first, it takes into account the limitations and security issues described in our previous approach. This research establishes security analysis of the extended protocol in order to prevent attacks such as the Multi-Channel Replay Attack by introducing server-side nonces and making the protocol interactive. Also, the Hashed message authentication code is used to prevent the Multi-Channel Man-in-the-Middle Attack. Finally, in the process, we establish some open challenges that call for further research.

The organisation of this chapter is as follows: Section 6.3 presents the security technologies relevant to this chapter. Section 6.4 describes the security concerns of the protocol presented in Chapter 5. Section 6.5 describes the main contribution of this chapter, while section 6.6 briefly presents steganographic Protocols using nonce sharing. The following Section 6.7 analyses its security properties, while Section 6.8 and 6.9 presents discussion and summary to this chapter with some areas for future research respectively.

6.3 Related Terminology

In this section, terminologies that are essential for this paper are presented.

6.3.1 Semantically Constrained and Insecure Channels

The term channel could be described as a communication link C that is established between two or more communicating entities. This channel C could be wire, wireless, secured and unsecured. The channel C can have specific properties that classify it as constrained, consequently making them suitable to transmit a specific type of messages. The constraint imposed on a channel may include format, encryption algorithm, capacity or content restrictions. For example, according to the Global System for Mobile Communication standard (GSM), SMS can only transmit 160 (octets) characters of 7-bit encoding per transmission. Depending on the protocol used by a Mobile Network Operator, the SMS transmitted across a channel could be less than 160 characters. In cases were SMS encryption is used, only 64 (ASCII) characters are supported. There are some countries where SMS encrypting communication is not permitted [114]. Constraint such as these renders a channel insecure and therefore vulnerable to attacks. A constrained channel may be secure; however, in this chapter, all three channels used are considered to be semantically constrained and insecure.

6.3.2 Data Integrity and Authentication

Data integrity and authentication are security services that are essential to any network protocol. Message integrity can be referred to certain conditions when a message m is transmitted across a secure connection-oriented channel C without modifications, replays and duplication. Authentication can be used to identify a user's identity, and it can be achieved with four means: what an individual knows (e.g., PIN), what an individual possesses (e.g., cryptographic keys), what an individual is (e.g., static bio-metrics), what an individual does (e.g. dynamic bio-metrics). If these methods are correctly implemented, they can be used to provide secure message authentication [215].

Various authentication protocols have been proposed. These protocols normally utilise cryptographic challenge and response approaches which involve trusted third parties to agree on a type of authentication and some agreed function. For instance, a server S will send a challenge Ch and expects a valid reply from a client. A correct reply will convince the server that authentication is achieved. Some authentication protocols such as in [149], [193] and [157] use a nonce as a challenge, while in [217] suggest use a pre-shared secret to generate a challenge. In other cases where the nonce is not encrypted in the challenge message, the valid response could be used to construct a message that contains the nonce and encrypted with a shared secret key. In this paper, we are concerned with extending the protocol described in Chapter 5 by including message integrity and authentication mechanisms. This approach will enable the protocol to be robust against unauthorised modifications, replays, and intersection: we are concerned with the detection and prevention of attacks since message integrity services are related to active attacks.

6.3.3 Message Freshness

In a network protocol, a message is deemed fresh if it has never been used in a protocol's previous trace. The notion of message freshness has become an essential principle in the design of network security protocol. Otherwise, replaying old messages can lead to protocol failure, as explained in Section 6.4. Cryptographic nonces, time-stamps or sequence numbers are used for message freshness in many security protocols.

6.4 Our previous protocol

In this section, we briefly recall our previous protocol published in Chapter 5. We then discuss the security concerns pertaining to our previous approach. The security concerns discussed in this section are mainly on the data integrity of transactions that are transmitted across all three channels. Confidentiality is essential in our scheme but not sufficient for correctness. We introduce illustrations of replay attacks in two parts. The first part describes illustrations of the message flows between communicating principals, which is followed by the descriptions of action performed by communicating entities.

We recall the following notations: Let Amara be a sender wanting to transfer money to Ebere's account through the Bank. Let $\mathcal{M}$ be the set of all possible messages, $\mathcal{B}$ a set of bit strings, $\mathcal{N}$ a set of nonces, C the set of all channels and A be a set of adversaries. The functions Enc and Dec are encoding and decoding functions respectively. Let $m \in \mathcal{M}$ be an SMS message, $b \in \mathcal{B}$ be a binary value and the nonce $N_i \in \mathcal{N}(i = 1, 2)$ used for the protocol.

The channels $C_i \in C(i = 1, 2)$ denote two independent mobile wireless channels, implemented through suitable Mobile Network Services. The channel $C_3 \in C$ is a (not necessarily secure) internet connection. The messages m_1 and m_2 are faked, unsuspicious SMS banking messages and m_3 is a stego-object (e.g. image), using a suitable high-entropy stego-cover, e.g., LSB embedding. Different mechanisms could be used to implement C_3. In Chapter 5 we proposed the use of a picture-upload facility on the bank's public website, where users can share pictures of "happy customers". This does not require a secure connection and would not raise suspicion.

6.4.1 Single-Channel Replay attack

In traditional cryptographic approaches, encryption uses a shared secret key to prevent session keys and important information from being compromised. Threats such as the replay attack could, allow an adversary to impersonate legitimate principals or compromise session keys. A replay attack can interrupt operations by presenting principals with malicious messages that appear genuine. The simplest replay attack is one in which the adversary simply copies a message and replays it later [215]. The conventional approach of steganography does not necessary require the exchange of a secret key and our approach follow this notion. For an example, let us consider during an exchange of confidential instructions and C_1 has been compromised by an adversary (A) (e.g., External SMS Interceptor or Mobile Network Service Provider) as illustrated in Figure 5.9. This attack is a single-channel replay attack explained in the following game.

Game 4: Let $\prod \longleftarrow (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Xor})$ be a Multi-channel-entropy stego-scheme for sms based banking that is STEGO secure against an adversary A. The adversary A is however bounded within a probabilistic polynomial time (PPT) with a negligible edge against the challenger Chal.

Let Amara be the challenger Chal. Let the adversary be A with access to a stego-oracle O. The game proceeds as follows:

- Setup: A *is given access to* Chal*'s previous messages and history of* C_1 *through the help of an* $\mathsf{O}(c, h)$.
- Challenge: *The challenger outs a faked banking instruction and gives it to the bank.*
- Phase1: A *queries* $\mathsf{O}(c, h)m_1....m_q$*, where each query* $m_i \in \mathcal{M}$.
- Phase2: A *intercepts a copy of* m_1 *with the help of* $\mathsf{O}(c, h)$ *and performs a series of computation.*
- Phase3: *Eventually,* A *replays* m_1 *to the bank through* C_1.
- A *wins the game if and only if the banking instruction is accepted by the bank.*

The adversary eavesdrops on channel C_1, but does not attempt immediately to alter the message m_1. The adversary sees and records m_1, then tries to replay the message later to the bank. This could deceive the bank to think that Amara wants to initiate another transaction. However, the adversary could be unaware that the protocol uses three channels and m_2 transmitted across C_2 should be transmitted secondly. Thus, the bank will detect the presence of an attack.

6.4.2 Multi-Channel Replay attack

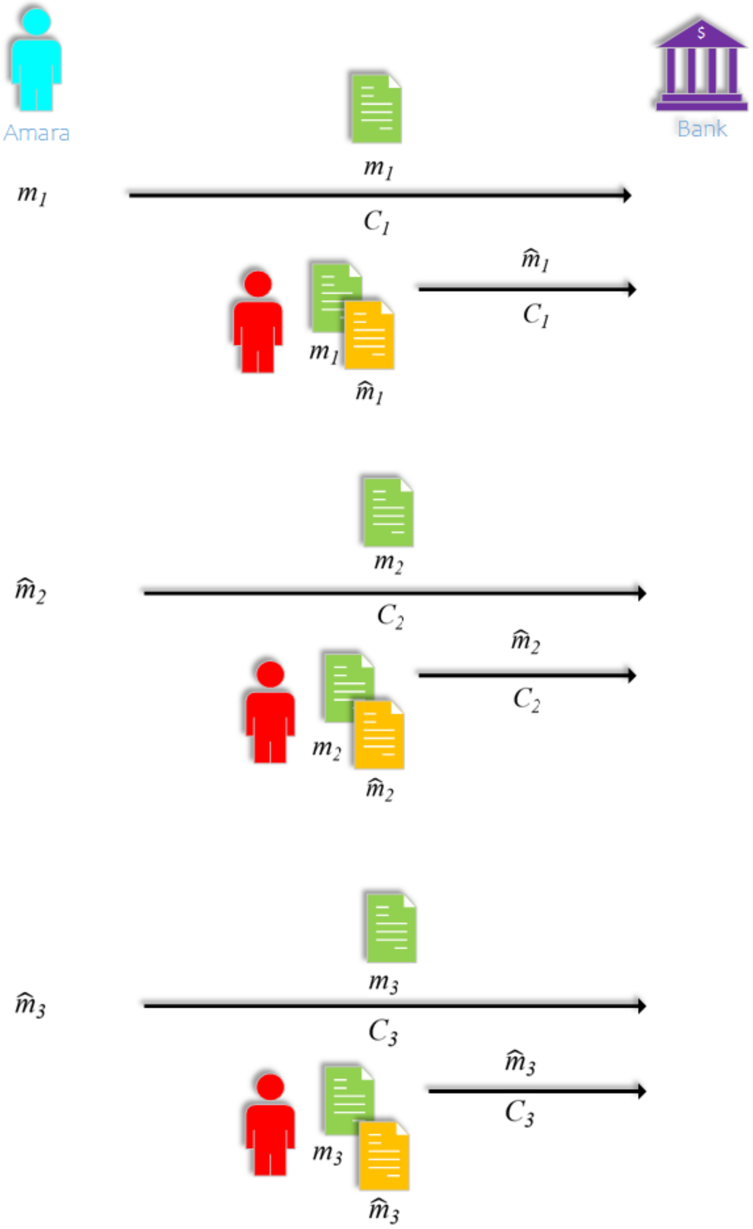


Figure 6.1: Multi-Channel Replay Attack

Let us consider another attack. Suppose that one or more adversaries know that our protocol uses three channels, then the protocol can be compromised this is illustrated in Figure 5.10. The replayed message would make the bank believe that Amara wishes to carry out the same transaction again: This attack could arise as many times as an attacker could plausibly implement it, on the same message set (or new ones).

In cases were time-stamps are used to prevent replay attacks according to [215], an adversary can replay a time-stamped message within the valid time window. However, if the original and the replay message arrive at the same time, within the time window, this incident can be logged by the bank's server. If eventually a replay attack is successful on a time stamped SMS within a valid time window, at the same time suppressing the original message, the replays cannot be detected by the bank's server.

6.5 Strengthened Approach

6.5.1 New Protocol Description

In this section the improved protocol is described. Our goal is to ensure message freshness in our protocol in order to prevent a multi-channel replay attack. To fix the protocol threat we include a cryptographic server nonce for this purpose as illustrated in Figure 6.2.

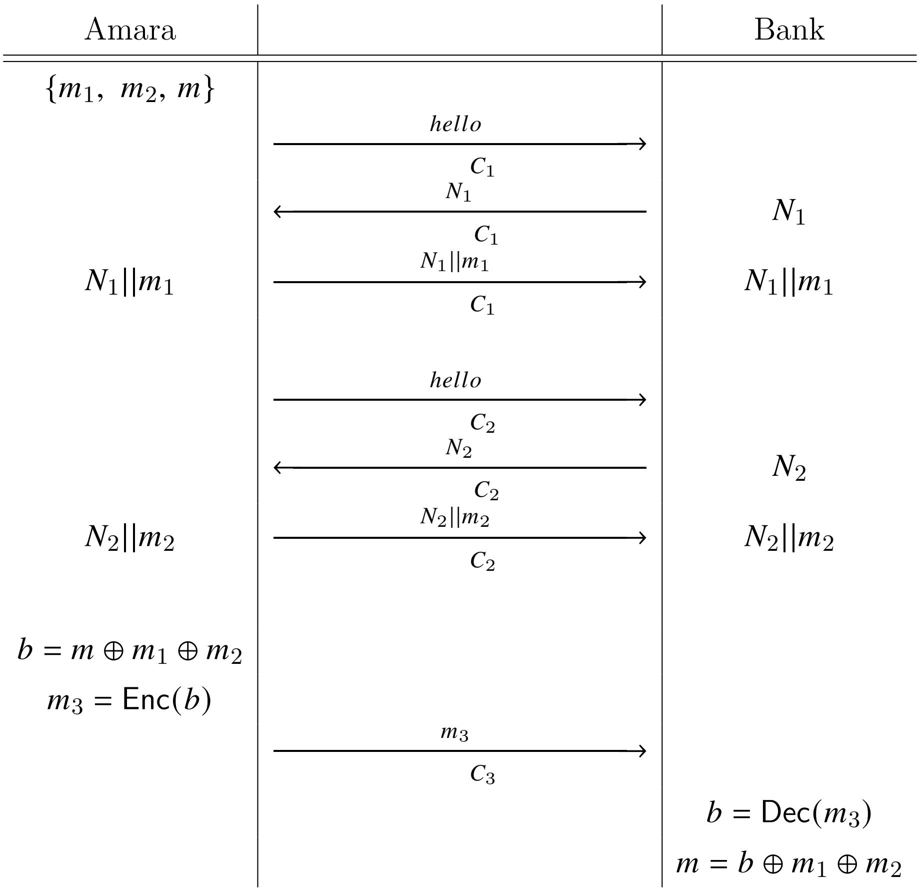


Figure 6.2: A Multi-Channel SMS Mobile Banking Protocol secure against multi-channel replay attack

We recall from Section 6.3-6.33 that a cryptographic nonce is used to make each transaction unique so that an adversary is unable to replay old communications or an unauthorized transaction in a distinct context. In our distributed protocol, the bank's server generates a nonce at least once for each channel. A cryptographic nonce should include properties of unpredictability or pseudo-randomness and could include a time-stamp Ts to ensure exact timeliness. Although, [121] argues that time-stamps should not be used for connection-oriented application due to the challenges that occur with clock synchronization among communicating processor clocks. We propose the use of pseudo-random numbers. In our improved approach, the protocol runs as follows:

1. Amara creates an SMS banking instruction message m.
2. She also generates two fake unsuspicious banking instructions m_1 and m_2.
3. Amara contacts the bank to identify the run through C_1 and C_2 respectively.
4. The bank generates two nonces N_1 and N_2 and forwards them to Amara.
5. Amara attaches N_1 and N_2 to the unsuspicious messages m_1 and m_2 and sends it to the bank.
6. Amara computes $b = m \oplus m_1 \oplus m_2$, embeds b using a steganographic embedding algorithm E and transmits the stego-object to the bank.
7. On receiving and extracting b using a steganographic decoding algorithm D, the bank can recover m by computing $b \oplus m_1 \oplus m_2$.
8. The bank can now transfer Amara's requested amount to Ebere's account.

The new and improved Multi-channel stego-system for sms based banking is summarised as follows:

Definition 6.5.1. ***(Multi-channel entropy scheme for SMS banking)****: A multi-channel secure SMS steganographic banking system is a Stego-system $\mathcal{S}$, that is considered a $\sum$ of the high entropy $\mathcal{S}^h$ and a low entropy stego-system $\mathcal{S}^l$. This dual entropy system consists of five efficient algorithms and three independent non colluding wireless channels. The five efficient* *algorithms consists of a generator* $\mathsf{Gen}(\lambda)$*, probabilistic encoding function* $\mathsf{Enc}(\cdot,\cdot,\cdot)$*, a deterministic decoding function* $\mathsf{Dec}(\cdot,\cdot,\cdot)$*, a deterministic transmission algorithm* $\mathsf{Trans}(\cdot,\cdot)$ *and an* $\mathsf{Xor}(\cdot,\cdot,\cdot)$ *algorithm.*

- $\mathsf{Gen}(\lambda)$: *According the security parameter* λ *outputs* $\{m, m_1, m_2\} \longleftarrow \lambda$ *through a mobile phone.*
- $\mathsf{Trans}(\cdot,\cdot)$: *takes two separate request through* C_1 *and* C_2 *respectively, and transmit to an intended recipient (Bank). Secondly, the bank generates two nonces* N_1 *and* N_2 *and forwards them to Amara. Finally, Amara attaches* N_1 *and* N_2 *to the unsuspicious messages* m_1 *and* m_2 *and sends it to the bank.*
- $\mathsf{Xor}(\cdot,\cdot,\cdot)$: *Takes as an input* m_1*,* m_2 *and the real message* m*, calculate with the algorithm* (Xor) *operator and return* b*.*
- $\mathsf{Enc}(\cdot)$: *Takes as input* b *and outputs* m_3 *such that* $m_3 \longleftarrow \mathsf{Enc}(b)$.
- $\mathsf{Dec}(\cdot)$: *Given a deterministic decoding function,* b *is extracted from* m_3*.*
- $\mathsf{Xor}(\cdot,\cdot,\cdot)$: *The secret message* $\boldsymbol{m}$ *is reconstructed by calculating* $b \oplus m_1 \oplus m_2$.

The Multi-Channel Man-in-the-Middle Attack is a major threat to our protocol. A typical man-in-the-middle attack enables an adversary to intercept all relevant messages, and to alter and insert new messages between two communicating entities [215]. In our distributed protocol, if adversaries collude they could intercept all communications transmitted across all three channels. However, this threat could be mitigated with an HMAC (sometimes expanded as either hash-based message authentication code or keyed-hash message authentication code). The HMAC uses a shared secret key which could be exchanged during the SMS banking registration or sent through mail.

In figure 6.2, a third nonce N_3 is generated. The nonces N_1, N_2, N_3 and b are concatenated together, then they are hashed with the HMAC.

6.6 Steganographic Protocols using Nonce Sharing

In section 6.5, we described an approach which nonces can be utilised for message freshness. In this section, we describe two steganographic nonce sharing techniques called the active nonce sharing and passive nonce sharing. Both techniques described in this section are similar to the protocol in section 6.5; however, there are distinctions.

The active nonce sharing requires three non-colluding channels C_1, C_2 and C_3, which can be Mobile Network Service Providers or text messaging services. Compared to the previous approach described in section 6.5, here m_1 and m_2 are the nonces. In this technique, the sender Amara creates nonces m_1 and m_2 and sends them to the Ebere through the channels C_1, and C_2 respectively. The nonces are combined with the secret message m to form $b = m_1 \oplus m_2 \oplus m$. This is encoded into the stego-cover o to create stego-object $m_3 = \mathsf{Enc}(b)$ which is transmitted through the third channel C_3. The receiver extracts $b = \mathsf{Enc}^1(m_3)$ and recovers the original message $m = m_1 \oplus m_2 \oplus b$. This technique is illustrated in Figure 6.4.

The nonces transmitted across the channels should have properties of pseudo-randomness by the Amara. There are several possibilities of which the nonces can be implemented:

Amara		Bank
$\{m_1,\ m_2,\ m\}$		
	$\xrightarrow[C_1]{hello}$	
	$\xleftarrow[C_1]{N_1}$	N_1
$N_1 \Vert m_1$	$\xrightarrow[C_1]{N_1 \Vert m_1}$	$N_1 \Vert m_1$
	$\xrightarrow[C_2]{hello}$	
	$\xleftarrow[C_2]{N_2}$	N_2
$N_2 \Vert m_2$	$\xrightarrow[C_2]{N_2 \Vert m_2}$	$N_2 \Vert m_2$
$b = m \oplus m_1 \oplus m_2$		
N_3		
$H_K = HMAC_K(N_1 \Vert N_2 \Vert N_3 \Vert b)$		
$m_3 = \mathsf{Enc}(H_K \Vert N_3)$		
	$\xrightarrow[C_3]{m_3}$	
		m_3
		$N_3 \Vert H_K = \mathsf{Dec}(m_3)$
		$b = H_K(N_1 \Vert \check{N}_2 \Vert N_3 \Vert b)$
		$m = b \oplus m_1 \oplus m_2$

Figure 6.3: A Multi-Channel SMS Mobile Banking Protocol secure against multi-channel man-in-the middle attack

1. The text messaging application installed on Amara's phone should generate random numbers automatically and transmits them to the receiver as SMS text messages. However, this could create suspicion that important information is transmitted.

2. The second approach requires Amara to manually type seemingly meaningful messages on her phone, which are again transmitted to Eberer as text messages.

3. The third option requires the application to automatically formulates seemingly meaningful random sentences which are transmitted again to the receiver as texts.

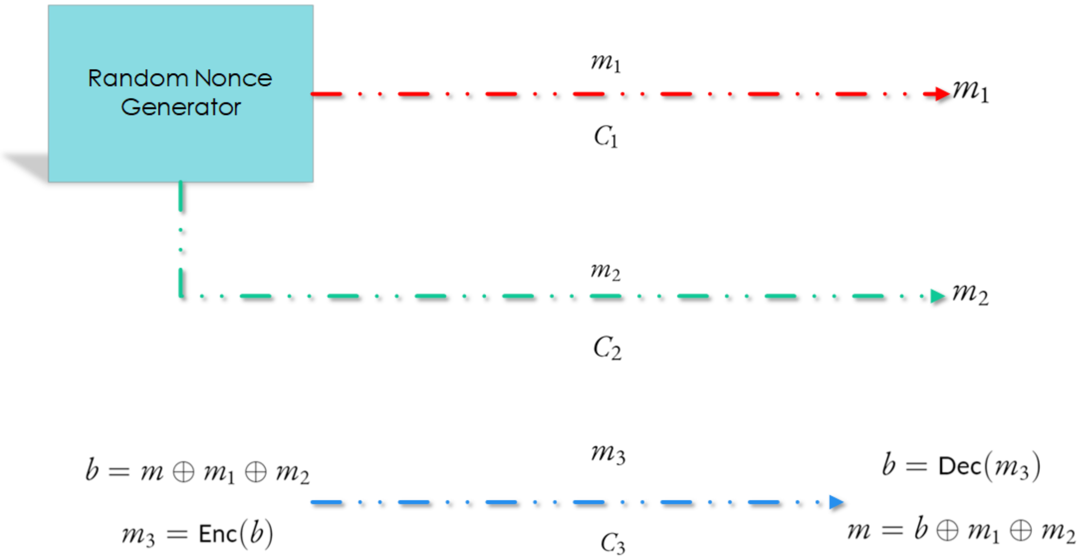


Figure 6.4: Active Nonce Sharing

The initial approach would not be difficult to implement and given adequate entropy, and repetition of any given nonces would be improbable. Though, the frequent transmission of raw random numbers on text messaging channels such as SMS could notify an adversary that secret communication is taking place. The second approach is potentially less suspicious; the nature of the SMS messages could be reasonably deluding. The adversary can be tricked into believing that the text messages transmitted across the channels are generic and unsuspicious communication. However, this option requires more effort on the part of Amara who may become negligent with time and repeatedly send previous messages. As a result, the embedded payload (were it to be discovered) will be more vulnerable to steganalysis, and the protocol will be compromised. The third option combines first and the second approach, however, it requires an algorithm that has the capacity to generate random indistinguishable sentences and high in entropy.

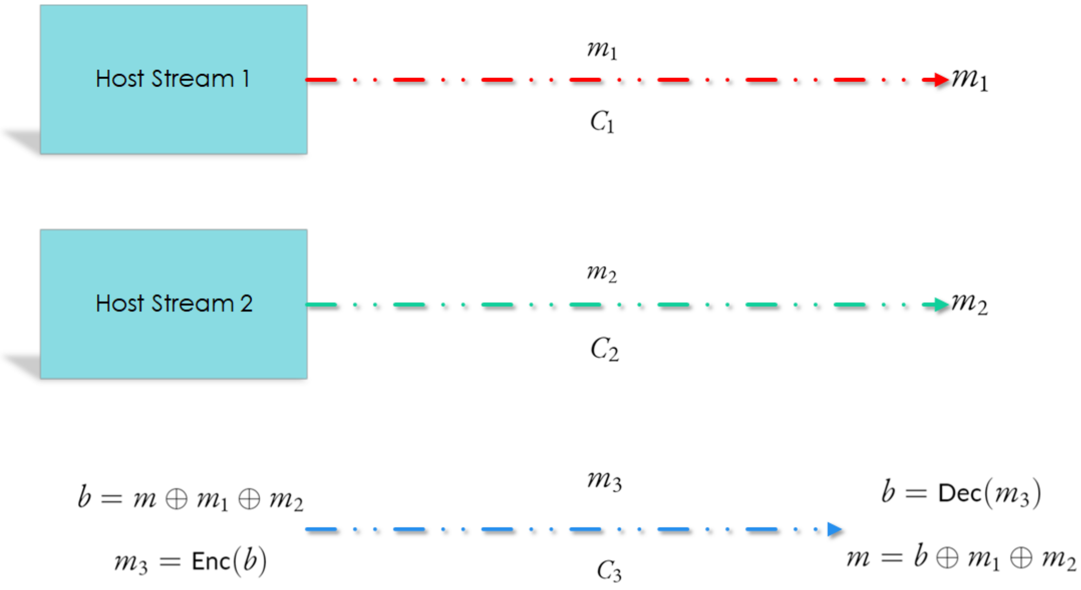


Figure 6.5: Passive Nonce Sharing

Another approach can also be considered, which could be called "Passive Nonce Sharing" as illustrated in Figure 6.5. In this approach, there are two "host" data streams. Various sources can be used as streams, though in this chapter, we consider well-established news or Twitter-feeds accessed by both parties, who thus have a common sequence of nonces. This method has the following advantages: the nonces now resemble genuine human communications that eliminates the requirement for pseudo-sentence generation. The entropy (particularly of a news stream) is likely to be high and requires only one direct channel of communication C between Amara and Ebere. The disadvantage of this option, however, is that the system is absolutely dependent upon the “host” streams. If the host stream fails, then communication is interrupted until restoration, or else both communicating parties will agree to a new host. Besides, communication with the use of this approach depends upon the host streams generating new messages at an adequate rate in order to keep up with the transmission pace.

Techniques used for automatic sentence generation has necessarily long been recognised as part of any natural language interface. It also relies upon formal grammars; however, the focus in section 6.6 is to transform some specific semantic message into an understandable form, rather than random sentences with irrelevant meaning. With the advancement of computing technology, artificial sentences can easily be generated with the use of predictive text algorithms such as T9. For example, starting from the word “hello” and always choosing the first suggestion yields “hello again this is the first time I have much fun” or with a different seed “what is your favourite place in the UK”.

The concept of automatic sentence generation is far from new: Shannon [204] used probabilistic word prediction in 1948 to demonstrate the nature of discrete information sources. The technique was able to demonstrate a “first-order” model in which words were independently generated and a second-order “Markovian” model in which each word was chosen according to the probability that it followed the preceding word. Noting that the latter often generated four (and sometimes as many as ten) consecutive words without grammatical error, Shannon suggested the possibility of higher-order approximations. However, the process involved made this approach unfeasible at that time. The rise of capable computers has enabled further experiments with Markov-sentence generation. Masurel [161] published a "third-order" Markovian sentence generator to produce placeholder text for website testing. This is an alternative to "lorem ipsum" while subsequently Branton [37] proposed the use of Markov-generated sentences that can be used for summarising documents. Most approaches used presently for automatic sentence generation are not purely Markovian; however, are based on formal grammatical models.

6.7 Security Analysis

This section presents the security analysis of our improved protocol. We analyse the security of our protocol against multi-channel replay attack and multi-channel man-in-the middle attack. The fundamental security assumptions of the protocol is that the bank is considered to trusted. We consider two types of adversaries: The Internet Service Provider (ISP) and the Mobile Network Operator (MNO).

6.7.1 Security Assumptions

An individual Mobile Network Operator has the ability to read SMS messages transmitted across his mobile network. On the other hand, the internet service provider has the joint abilities of all involved mobile network operators. He also has the ability to monitor all connections and activities of certain users.

6.7.2 Collaborative Mobile Network Operator (MNO) Replay Attack

It is possible to initiate a collaborative attack between different Mobile Network Operators. It is also possible that the unsuspicious nature of the messages m_1 and m_2 could be detected and replayed. This collaborative attack is explained in the Game 5.

Game 5: Let $\prod \longleftarrow (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Xor})$ be a Multi-channel-entropy stego-scheme for SMS based banking that is STEGO secure against an adversary A. The adversary A is however bounded within a $probabilistic\ polynomial\ time\ (PPT)$ with a negligible advantage against the challenger Chal.

Let Amara be the challenger Chal and let the adversary be A with access to a stego-oracle O. The game proceeds as follows:

- Setup: A *is given access to* Chal*'s previous messages and history of* C_1 *and through the help of* $\mathsf{O}(c, h)$.
- Challenge: Chal *sends two separate request through* C_1 *and* C_2 *respectively, and transmit to an intended recipient (Bank). Secondly, the bank generates two nonces* N_1 *and* N_2 *and forwards them to Amara. Finally, Amara attaches* N_1 *and* N_2 *to the unsuspicious messages* m_1 *and* m_2 *and sends it to the bank.*
- Phase 3: A *intercepts a copy of* $N_1||m_1$ *with the help of* $\mathsf{O}(c, h)$.
- Phase 4: *Eventually,* A *replays* $N_1||m_1$ *to the bank through* C_1.

- A *wins the game if and only if the banking instructions is accepted by the bank.*

However, without the inclusion of a nonce N on each channel, or even if the messages are replayed with the old nonce, the presents of an attack will be detected by the bank as presented in our improved approach.

6.7.3 Multi-Channel Replay Attack

Suppose all principals involved in the protocols are observed, we might need a closer analysis. However, we assume that Amara will be the one observed by the adversaries. The colluding adversaries (Adv) will observe that Amara is connected to the bank's server. They will see all messages m_1, m_2 and b transmitted during the trace. The adversaries could try and use this knowledge to take advantage, reply the messages and initiate an unauthorised transaction.

Game 6: Let $\prod \longleftarrow (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Xor})$ be a Multi-channel-entropy stego-scheme for sms based banking that is STEGO secure against an adversary A. The adversary A is however bounded within a $probabilistic\ polynomial\ time\ (PPT)$ with a negligible edge against the challenger Chal.

Let Amara be the challenger Chal. Let the adversary be A with access to a stego-oracle O. The game proceeds as follows:

- Setup: A *is given access to* Chal*'s previous messages and history of* C_1 *through the help of an* $\mathsf{O}(c, h)$.

- Challenge: *The challenger outs a faked banking instruction and gives it to the bank.*
- Phase1: A *queries* $\mathsf{O}(c,h)m_1....m_q$*, where each query* $m_i \in \mathcal{M}$.
- Phase2: A *intercepts a copy of* m_1 *with the help of* $\mathsf{O}(c,h)$ *and performs a series of computation.*
- Phase3: *Eventually,* A *replays* m_1 *to the bank through* C_1.
- A *wins the game if and only if the banking instruction is accepted by the bank.*

We assume the adversaries will attack the protocol as follows: (1) Adv has access to Amara's messages including all previous messages. (2) Adv pretends to be Amara Adv_{Am} and replays previously sent messages m_1, m_2 and b to the bank through C_1, C_2 and C_3 respectively. If the replayed messages (m_1 and m_2) do not contain a freshly generated nonce sent by the bank, the bank will detect the presence of an attack.

6.7.4 Multi-Channel Man-in-the Middle Attack

In this form of attack, similar conditions can be applied.We assume that the colluding adversaries (Adv) will observe that Amara is connected to the bank's server and they could try and take advantage, intercept the messages, modify and initiate an unauthorised transaction. However this attack is negligent due to the HMAC used.

6.8 Discussion

Our improved approach described in Section 6.5, is secure against multi-channel replay attacks. However, our protocol is vulnerable to other attacks, in particular traffic analysis.

In this section, we discuss potential ways of further strengthening our protocol in order to reduce the impact of these attacks.

6.8.1 Traffic Analysis

The security analysis in Section 6.6 excluded the threat of traffic analysis [185]. Traffic analysis can assist colluding adversaries to observe if principals are communicating a secret message. For example, suppose both the mobile channels and the bank web server are monitored. If traffic analysis reveals that Amara repeatedly sends messages to the bank, using the two mobile channels, and also uploads information to the bank's website, her use of the steganographic protocol can be detected. Threats such as traffic analysis have always been a major challenge [115]. Whilst studies such as [243] proposed a solution to cope with this issue in a general Internet setting, they seem difficult to apply in our scenario. The challenge of low entropy steganography has already been acknowledged in [26]. Further research will be required to investigate this aspect.

When considering attacks based on traffic analysis, security of our protocol requires the assumption that an adversary will be unable to detect the steganographic nature of our cover message. In the literature, this relates to concepts developed in [109] and [93], or more specifically in the context of an online social network, to *social indistinguishability* [26].

Defining precisely what social indistinguishability means can be very difficult. Sending fake SMS banking messages as proposed in our protocol is indistinguishable, if we assume that the eavesdropper is already aware of Amara's intention to engage in mobile banking. In this instance, our aim is not to conceal the nature of the banking protocol, but to disguise information about payment recipient, bank account details and similar, or perhaps to hide the precise type of banking transaction (for example, to disguise a money transfer with a request for a bank statement). However, we could broaden the scope of our information hiding protocol by aiming at hiding the fact that the secret message is indeed a banking instruction. In fact, the fake messages could contain any content but in order for this to remain indistinguishable, the recipient (the bank) needs to cooperate and hide its true identity to the mobile operators. This might be problematic with regards to illegality.

The following subsection 6.9 presents the requirement for implementing a Proof of Concept (PoC) for the protocol.

6.9 Requirements for a Proof of Concept Implementation

To demonstrate the practicality of the multi-channel steganographic protocol described in Chapters 5 and 6 of this thesis, a Proof-of-Concept (PoC) working prototype is required. This section describes the practical requirements of implementing the system.

6.9.1 Proof of Concept

The Proof of Concept or PoC is a software development terminology that is used to describe a project. The project is designed to demonstrate the practicability of a software system or protocol to meet the target requirements by testing that a set of desirable software functions will function as expected when the chosen technical system or architecture is implemented. When Implementing a PoC, it is necessary to consider and establish stakeholder requirements by describing use cases. Secondly, the software designer should define the system function and technology necessary to satisfy the stakeholders' needs. A PoC should include sufficient analysis, design, and coding to make the proposed solution testable. Finally, a successful PoC will enable the project designer to test the feasibility of the proposed solution and functionality; also, it will enable the stakeholders to analyse and decide whether the proposed software design can satisfy their requirements [33].

6.9.2 Objective

The objective of implementing a PoC for the multi-channel steganographic protocol is to demonstrate how SMS based banking subscribers can perform SMS banking transactions securely by using a dual SIM mobile device (mobile phone) and an internet connection.

The protocol used for the PoC will be implemented with certain considerations:

- The Android Virtual Device (AVD) will simulate a dual SIM mobile phone on a computer without the need for a physical device. This approach will aid in implementing a basic system that will demonstrate how SMS banking subscribers would perform banking transfers.

- Leverage existing programming systems such as javascript or python to implement a banking website prototype where users would complete transactions through an internet connection.

The PoC will be deemed successful if the proposed system is able to successfully complete an SMS banking transaction request to a server (Bank).

6.9.3 Implementing a Proof of Concept: detailed description

This section aims to focus on the protocol PoC users descriptions; therefore, a set of use cases is proposed to meet the needs of the SMS banking subscribers.

SMS banking subscriber

- **Motivations**: The fundamental motive is to be able to securely perform SMS banking transactions without an adversary discovery and modifications the contents of my transactions.
- **Privacy and Security Concerns:** The main privacy and security concerns are performing SMS banking transactions while an adversary discovers the contents of my transactions and sell them to authorised entities

  While users perform SMS banking transactions an adversary modifies or replays the contents of my transactions.

Use case 1 (Assertions)

- It will be possible for subscribers to use a dual SIM mobile phone to transmit two pseudo banking instructions m_1 and m_2 to a bank server.
- Demonstrate that it is possible for users to compute $b = m_1 \oplus m_2 \oplus m$ using an independent XOR device.
- The system will allow subscribers to publish m_3 on the bank's web page by creating register and login functionality.
- Demonstrate that it is possible for the bank's server to compute $m = m_1 \oplus m_2 \oplus b$ using an XOR functionality.

Use case 2: Exposing data

- Create a visual design to illustrate what the bank public interface would look like, including register, login interface and steganographic input interface.
- Create a visual design with AVD to illustrate what the physical mobile device would look like.
- Create clickable prototypes of the protocol front-end.
- Setup the back-end of the system.

6.9.4 Tasks for the Proof of Concept

The PoC will consist of implementing the steganographic protocol in a development environment, using the technical system overview described in Chapters 5 and 6 of this thesis, in order to test the use case. The environment will be limited to testing the use case in a minimal way in order to demonstrate the feasibility of the proposed approach. For example, in a real-world environment, the steganographic protocol's back-end would have some features designed to implement the security of the protocol; similarly, the protocols' front-end would provide a basic and user-friendly experience to users as they upload the SMS banking transactions through the bank website. In the following sections, the hardware and software requirements are explained and will include the following:

- Web Application
- hardware Requirements
- networking Requirements
- Supported Web browsers
- Transport Layer Security (TLS) Requirement
- HTML Editor
- A Graphics Editor
- FTP Client

Component	Recommended	Minimum
Processor	3.3 gigahertz (GHz) with SSE2 instruction set	1.9 gigahertz (GHz) x86- with SSE2 instruction set
Memory	at least 4-GB, 8-GB RAM or more	2-GB RAM
Display	Super VGA with a resolution of 1024 x 768	Super VGA with a resolution of 1024 x 768

Table 6.1: hardware Requirements

Hardware Requirements

This section lists the hardware requirements for implementing the protocol: Implementing the multi-channel steganographic protocol (For example; the bank web application) on a computer with inadequate recommended requirements could result in poor performance. Besides, better performance could be achieved and experienced when running the protocol that use a higher system configuration. For example a computer with a recent core processor, more RAM and lower clock speed.

Network Requirements

The protocol will be designed to operate properly over networks that have the following requirements:

- The network bandwidth should be greater than 50 KBps (400 kbps)
- Latency under 150 ms

In a realistic setting, these network recommendations might not guarantee a performance that is satisfactory. Though, for the protocols' Proof of Concept (PoC), this should provide adequate performance. During the hardware system setup network capacity and throughput needs to be verified.

Software Requirements

Mobile Phone: In Chapter 5 of this thesis, the proposed protocol does not require specific software to be installed on the mobile phone and the use of an expensive smartphone is not required. The subscribers of this protocol could use an affordable mobile device such as the Nokia 105 DUAL SIM phone and Nokia 106-Dual SIM. These phones cost as little as č9.95 and č18.49 on eBay respectively. However, to demonstrate the protocols' a Proof of Concept the use of an Android Emulator is sufficient. There are advantages of using the Android Studio emulator. The Android Emulator can simulate various Android devices on a computer so that an application on different devices and android APIs without the need for a physical device. Secondly, the emulator provides various capabilities of a real android device. It is possible to simulate incoming calls and text messages, simulate network speeds, specify the device location and much more. When comparing the use of a physical device with the emulator, the emulator is faster. For example, data can be transferred faster to the emulator than a device connected to a computer through a USB.

The Android Emulator has additional requirements beyond the basic, which are described below:

- SDK Tools 26.1.1 or higher
- 64-bit processor

- Windows: CPU with UG (unrestricted guest) support
- HAXM 6.2.1 or later (HAXM 7.2.0 or later recommended)

The use of hardware acceleration has additional requirements on Windows and Linux:

- Intel processor on Windows or Linux: Intel processor with support for Intel VT-x, Intel EM64T (Intel 64), and Execute Disable (XD) Bit functionality
- AMD processor on Linux: AMD processor with support for AMD Virtualization (AMD-V) and Supplemental Streaming SIMD Extensions 3.
- AMD processor on Windows: Android Studio 3.2 or higher and Windows 10 April 2018 release or higher for Windows Hypervisor Platform functionality

Supported Web Browsers: The web application can run in any of the following web browsers running on the specified operating systems:

- Microsoft Edge running on Windows 11, Windows 10, Window 8.1.
- Google Chrome running on Windows 11, Windows 10, Windows 8.1

Text Editor: For this PoC,the Mobirise system is a free HTML editor that does not require coding. This system includes theme, drag and drops elements on the page. For this system to be used, users need to add text in the available text editor, insert images or icons.

FTP Client: The file transfer protocol (FTP) is necessary to transfer HTML supporting images and files to web servers. The FTP can be used through the command-line interface in operating systems such as Windows, Linux and Macintosh, but a dedicated FTP client is much easier to use. For this PoC, the FTP clients considered is the Cyberduck. The Cyberduck is free, open-source, cross-platform software known for its seamless integration with external editors and its attractive user interface

Transport Layer Security (TLS) requirement

Web browsers and other client applications that use Transport Layer Security (TLS) versions earlier than TLS 1.2 won't be able to connect to their Dynamics 365 (online) environments and the admin center.

6.10 Cost and Benefits Analysis

In this section, the protocol's cost and benefits analysis is calculated against an existing mobile banking app solution. The main consideration is the financial cost that has to be invested by the users of either the multi-channel steganographic protocol or the mainstream mobile banking application.

The cost-benefit analysis involves comparing the costs to the benefits of a project. It aids to decide if a project should be implemented or not. The costs and benefits of the project are quantified in monetary terms after adjusting for the time value of money, which gives an accurate picture of the costs and benefits. However, an alternative to Cost and Benefit Analysis (CBA) is cost-effectiveness analysis (CEA). CEA is used for various reasons; it can be used to analyse and decide whether it is necessary to spend capital on a novel system or invention. If a new system or invention is chosen to replace outdated or insufficient systems, then this is known as opportunity cost. Though if the cost of developing a new invention is more expensive than existing systems, then it would be necessary to invest elsewhere. Secondly, it can aid decision-makers in understanding the cost and benefits. When considering Cost-Effectiveness analysis in decision making, it is essential to consider relative cost and effects. For example, new inventions should not be evaluated in isolation; they should be relatively evaluated to an alternative. Unlike other standards such as CBA, it bypasses three constraints:

- It does not require the total cost and benefits to be financial value.
- The measure does not represent the total benefits that are accrued.

- It could be used to analyse intermediate goods though the outcomes might not be clear.

As such, no constraint limits the need to apply monetary values to certain variables. There are alternatives that CEA considers about the ratio between the costs associated with each alternative though not a financial effective measure. This represents a difficulty of CEA as costs. The costs are represented by financial values, while effectiveness could be measured in terms of time savings or other measures that can be quantifiable. This reason necessitates the motive in the calculation of the CEA ratio. There are two forms of ratio that can be expressed [192] [16]:

- Cost-Effectiveness Ratio: dividing costs of an alternative by the measure of effectiveness.

$$CER_a = \frac{C_a}{E_b}$$

- Effectiveness-Cost Ratio: dividing effectiveness measured by costs of alternative.

$$ECR_a = \frac{E_a}{C_a}$$

- Using these ratios two project alternatives can be compared as follows:

$$CE_{ab} = \frac{C_a - C_b}{E_a - E_b}$$

Where, C_i= Costs of alternative i, C_j = Costs of alternative j, E_i = Effectiveness units of alternative i, E_j = Effectiveness units of alternative j.

6.10.1 Assumptions

The steganographic protocol described in this thesis uses three channels; two channels for SMS banking instruction and an internet connection. Currently, the cost of a single SMS banking transaction in Nigeria is ₦6.98 (where ₦ = naira) and it is equivalent to \$0.0183, while performing banking transactions with a mobile banking application would typically require a data subscription, and the cheapest data subscription is ₦50(\$0.088). In order to compare both alternatives, it is necessary to calculate the long term use of both approaches. This aid to decide if the novel steganographic protocol is worth implementing. Successfully calculating the cost-effectiveness of the new approach will require a parameter; therefore, this section uses an effectiveness parameter. The effectiveness parameter used for this cost-effectiveness analysis is the Mobile Banking Service Usage Profile presented in the study [20]. The study analyses the total number of respondents that used mobile banking services; in this instance, SMS banking (USSD) 69.7% and mobile banking 68.5% (For example, using apps).

The cost of SMS banking transactions yearly is ₦2, 547.7 if it is assumed that USSD subscribers perform transactions daily. Since the steganographic protocol uses two mobile network channels c_1 and c_2, the annual cost will be ₦5, 095.4. The cost for a cyber-cafe internet connection is ₦100 (about \$ 1) per hour [158]; therefore, if transactions are performed daily, the annual cost is ₦36, 500. If the assumptions are accurate and reasonable, the total yearly cost for using the steganographic protocol would be ₦41, 595.4.

For subscribers that use mobile banking applications for transactions, the cheapest annual data bundle subscription is ₦120, 000 for $400GB$ regardless of whether transactions

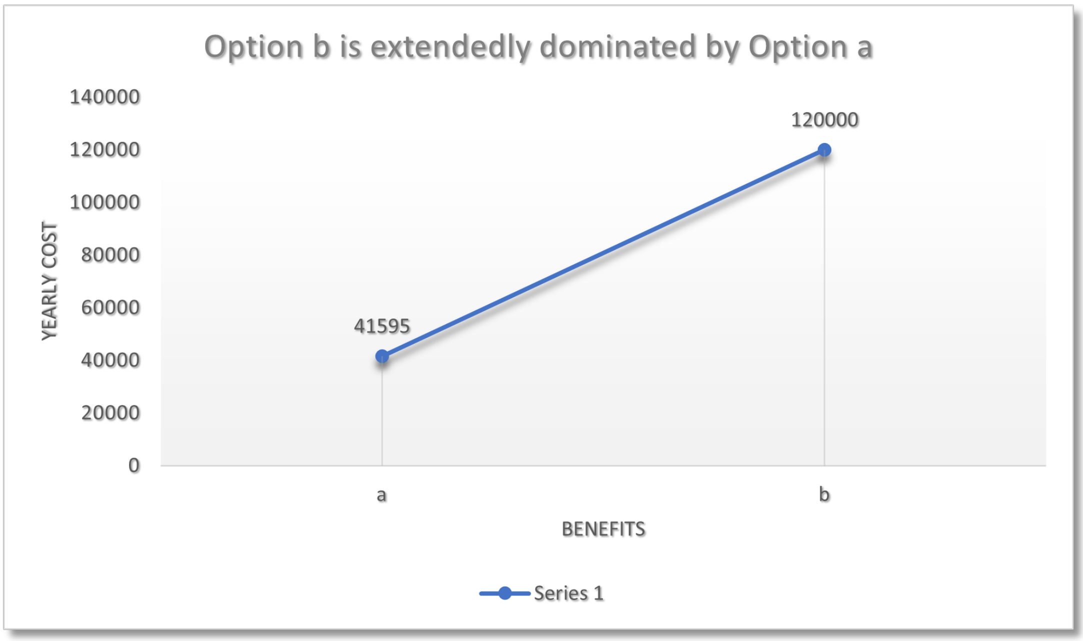


Figure 6.6: The Cost-Effectiveness Analysis of Option *a* and *b*

are performed daily or not [50]. By assumption, this information is valid if subscribers use the MTN mobile network operator service. Consequently, the cost-effectiveness ratio and effectiveness-cost ratio is calculated as follows:

$$CER_a = \frac{C_a}{E_a}$$

then, ₦596.7 $= \frac{C_a}{E_a}$ for the novel steganographic protocol, $ECR_a = 0.001$. For existing mobile banking schemes

$$CER_b = \frac{C_b}{E_b}$$

then ₦$1,3574 = \frac{C_b}{E_b}, ECR = 0.0007.$

Using these ratios the two alternative mobile banking approaches can be compared as follows:

$$CE_{ab} = \frac{C_a - C_b}{E_a - E_b} = \frac{\Delta C}{\Delta E}$$

$$\text{₦}1,92.7 = \frac{C_a - C_b}{E_a - E_b}$$

Based on the tables 6.2 and 6.3, if the cost effectiveness threshold is below N4192.7 then we choose option a.

Table 6.2: Cost Effectiveness Analysis

Options	Costs (Naira)	Effects	$\frac{C}{E}$	$\frac{E}{C}$	ΔC	ΔE	$\frac{\Delta C}{\Delta E}$
a	41,595	69.7	596.7	0.001	–	–	–
b	120,000	88.4	1,357.4	0.0007	7,8505	18.7	4192.7

Table 6.3: Cost Effectiveness Threshold and Option

Cost Effectiveness Threshold	Choose Option
less than ₦41, 92.7	*a*

In deciding on the cheapest SMS banking solution, the cost minimisation rule formula can be used:

$$CM\, where \frac{MP_L}{w} = \frac{MP_K}{r}$$

It is obvious that the solution with the least cost is the multi-channel steganographic protocol since both solutions aim to solve the same problem and the corresponding cost is

₦$41,595.4$.

According to table 6.2, option a dominates option b, where option a is the multichannel steganographic protocol and option b is the existing mobile banking app. The multichannel steganographic protocol has a lower cost-effectiveness Ratio of ₦596.7 when compared to the option b which is ₦$1,357.4$. However, option b has a lower Effectiveness-Cost Ratio of 0.0007. The figure in column ΔC suggest that if users subscribe to option a, they will be able to save ₦$78,405$ when compared to option b, which cost a total of ₦$120,000$, even though option b has higher effectiveness than a. The incremental Cost-Effectiveness Ratio is ₦$4,192.7$ in comparison to option b. Table 6.3 suggest that if the cost-effectiveness threshold is less than ₦$4,192.7$ per effectiveness, choose option a.

6.11 Summary

This chapter proposes an improved multi-channel steganographic SMS banking protocol already developed in Chapter 5 of this thesis. Conventional techniques have influenced our approach to ensure message freshness in distributed and reciprocal authentication protocols. Our security analysis shows our improved protocol can counteract threats such as the multi-channel replay attack and multi-channel man-in-the-middle attack. Secondly, section 6.9 of this chapter presents a practical requirement that is necessary to develop a functional Proof-of-Concept. Thirdly, this chapter provides a justification for why this protocol is essential through a Cost-Effectiveness analysis. When the protocol is compared to an existing solution, the Multi-Channel Steganographic protocol is feasibly cost-effective. Areas that call for further research within this subject includes improving indistinguishability through machine learning algorithms and preventing threats such as traffic analysis.

Chapter 7

Game-Theoretical Decision Models for Entropy-based Steganographic Techniques

7.1 Introduction

Traditionally, game theory is the study of decision making in situations involving multiple players (called agents) who behave rationally. Game theory has recently been applied to network security scenarios that involve attack and defence type interactions. In a security game, each agent decides whether to take specific actions and try to optimise their outcomes (often called "maximising utility") in various situations. These games and their so-called equilibrium solutions (if those exist) are used as a foundation for choosing the most appropriate strategies. They can also be used to predict the behaviour of various adversaries, assuming they behave rationally.

Furthermore, game theory can readily be applied to various cryptographic concepts [108]. Such settings include intrusion detection in network security [11], forecasting the probability of cyberattacks [159], and managing the security of information in organisations [22]. A crucial concept in the theory of non-cooperative games is that of a Nash Equilibrium (NE) [12], a state of stability players in a non-cooperative environment do not have the incentive to change their strategy, considering their payoff are optimal. Although, not all games show a “pure” Nash Equilibrium, where combinations of decisions produce such a local optimum. However, they all possess a “mixed” Nash Equilibrium such that there exist a set of strategies such that, if player i uses strategy s with probability P_{is}. The weighted sum corresponding to the overall expected utility over all the players will have a local maximum, in the sense that if any single player changes their mixed strategy (their distribution of probabilities concerning the individual strategies), the overall utility across all players will not increase. The Nash Equilibrium (NE) identifies the optimal strategies used in game theory. Nash’s theorem states that nonzero-sum games always admit a mixed strategy Nash-Equilibrium. Interpreting Nash Equilibrium may be challenging for practical applications, and environments [15]. However, game theory has not been extensively applied to steganography to date.

The spectrum of cryptographic system design and game theory is concerned with the study of ”interactions amongst distrusting communicating entities with mutual interest. The interactions of game theory and cryptography could be seen as the application of correlated equilibrium in the unavailability of trusted arbitrators (mediators), and agents are rational and attempt to maximise their outcome (payoffs) instead of blindly following a cryptographic protocol [108].

Current research in the area of game theory and cryptography can be classified into two broad categories: applying the concepts of game theory models and definitions to the cryptographic protocol design setting and employing cryptographic protocols to game-theoretical problems [108]. In a real-life cryptographic environment, the situation in game theory is of multiple players with conflicting interests that attempt to initiate something in common regardless of those conflicts. Cryptography only attempts to develop network protocols to achieve a specific goal. However, game-theoretical modelling aims at adapting and predicting the outcomes of any given situation [156].

7.2 Chapter Contribution

The contribution of this chapter is a novel theoretical framework for models that applies the concept of game theory in an entropy-based steganographic protocol setting. The models described are based on the standard form of two-player non-zero-sum complete information games. This framework is then used to evaluate the entropy-based steganographic protocol described in Chapters 5 and 6 of this thesis. A range of use cases is designed using the Matlab scientific tool, simulating these game-theoretical models. Three steganographic games are presented: The first game, G_1, is a generic stego-game inspired by the well studied adversarial games [11]. The security game model provides an insight into an essential stego interaction and decision-making process between players. The objective of the second game is to design a use case and model that is considered suitable for real-world use. The use case and model described for G_2 aims to inform players in decision making while utilising stego strategies against active adversaries in an untrusted and constrained network environment. Finally, G_3 is an extension of the G_2 game. The fundamental objective of this game is to maximise the utility function of both players by introducing the notation of trust as a parameter T. T is defined as the degree of trust the player U has in an Online Stego Service provider (OSSP) where this provider claims to guarantee the security of secret messages. The trust parameter helps to understand unanticipated outcomes of the protocol in a best case and worse case type scenario and to predict the adversarial entities' behaviour further. In this instance, the third game could assist in uncomplicated solutions, a pure Nash Equilibra for the extreme values $T = 0$ and $T = 1$ instead of mixed strategies.

The remainder of this chapter is structured as follows. Section 7.3 presents the fundamental definition of a strategic game and Nash Equilibrium strategy. Section 7.4 describes the game-theoretical decision models, while section 7.5 presents the analysis of the game models. Finally, the summary of this chapter is presented in section 7.6, while section 7.7 presents the future research directions.

7.3 Context and Background

Game theory provides mathematical models and tools that can be used for investigating various decision proceedings that are strategic. In a game, each payer competes for limited resources; in other words, game theory enables predicting players behaviour and modelling situations. The mathematical cornerstone of game theory is widely applicable to security problems ranging from IDS (intrusion detection) to social networks, wired, and wireless networks. This section presents some game theoretical concepts and definitions pertinent to this research document. Finally, the system protocol scenario essential to this research paper is presented.

7.3.1 Strategic Game

Network security can be seen as a strategic game played between players. These players may be broadly classified as network administrators or authorised users defending the networks and malicious entities who wish to compromise the confidentiality, integrity and availability of systems and networks. The game is played on interconnected systems, where vulnerabilities of assets are trying to be exploited by attacks, and defensive measures constitute its strategic move [11]. This metaphorical game over control of a network and interaction associated between players has been formally presented in [136].

Definition 7.3.1. *A game $G \in \mathcal{G}$ is defined as a triple $(\mathcal{P}, \mathcal{S}, \mathcal{U})$, where $\mathcal{P}$ is the set of players, $\mathcal{S}$ is the set of strategies, and $\mathcal{U}$ is the set of payoff functions. The notation $u_i(s)$ is the payoff function that expresses the benefit b of player i, given the strategy profile s minus the cost c it has to incur: $u = b - c$.*

In a complete information game with n players , a strategy profile $s = \{s_i\}_{i=1}^{n}$ is the n-tuple of strategies of the players. The static (bi)matrix security game players are denoted by A and D, where A denotes the attacker and D for defenders. The finite action spaces are the set of attacks.

$$A := \{a_1, ..., a_{NA}\}$$

and the set of defence approaches

$$D := \{d_1, ..., d_{ND}\}.$$

The game's outcome is represented by the $N_A \times N_D$ game matrices G^A and G^D for the attacker and defender. The entries in the matrices represent the costs for players, which they minimise. In the instance of a zero-sum security game, i.e. when $G^A = G^D$, the matrix.

$$G := G^D = G^A$$

is said to be a game matrix. In this accord, P^A maximises its payoff while P^D minimises its cost based on the entries of the game matrix.

Definition 7.3.2. *Given a bi-matrix game with payoff matrices A and B, a mixed strategy for Player 1 (the row player) is a real vector s satisfying* $0 \leq s_i \geq 1$, *with* $\sum_{s_i} = 1$. *A mixed strategy for Player 2 (the column player) is a real vector y satisfying the same properties.*

On the outright, a mixed strategy should have all vector entries strictly greater than zero. In addition, the corresponding payoff for Player 1 is ${}^t sAy$, and it is ${}^t sBy$ for Player 2.

Definition 7.3.3. *A Nash Equilibrium strategy* (s^*, y^*) *satisfies:* $s^*Ay^* \geq sAy^* \quad \forall s$ *and* $s^*By^* \geq s^*By \quad \forall y$.

The strategies could be mixed or pure, and the correlated Nash Equilibrium is referred to as pure or mixed. Besides, if all the inequalities in definition 2.3 are strict, one has a strict Nash Equilibrium. Else, the Nash Equilibrium is non-strict.

Definition 7.3.4. *A strategy y^* is a Nash equilibrium best response to s^* (denoted $y^* \in \mathcal{BR}(s^*)$ in the sequel) is a strategy satisfying $s^*By^* \geq s^*By\,\forall y$. Hence, a Nash equilibrium strategy is a strategy pair (s^*, y^*) of mutual best responses: $s^* \in \mathcal{BR}(y^*)$ and $y^* \in \mathcal{BR}(s^*)$.*

Lemma 1. *If Player 1's mixed strategy s^* is the best response to the (mixed) strategy y of the other player, then, for each pure strategy e_i such that $s_i > 0$, it must be the case that ei is itself the best response. In particular, the payoff e_iAy must be the same for all such strategies.*

7.4 Game-Theoretical Decision Models

7.4.1 Motivation for Security Game Model

As technologies used for communications advanced, from fixed landlines to mobile communications and the internet, individuals worldwide have been given access to a wide range of communication technologies. However, with each advancement, communication surveillance technologies have become adequately sophisticated and efficient in collecting vast information. Communication surveillance is no longer limited to intercepting a message. Presently, there are four main methods used for communication surveillance: mobile phone interception, internet monitoring, fixed-line interception, and intrusion technologies. An example of these technologies used for conducting surveillance is IMSI (International mobile subscriber identity) catchers. This technology can maliciously emulate legitimate mobile base stations, collect information on nearby devices, and mass monitoring systems, such as the Zebra system sold by South African company VASTech, Gamma corporation of the UK, ZTE Corp of China SS8 in the United States.

Mobile, internet and fixed-line network surveillance can occur with or without the cooperation of the network service operator. In some instances, law enforcement agencies and authorities can request lawful assistance for surveillance from network operators requested [55, 29, 173, 186, 133, 69, 241, 74, 96, 61, 240, 105]. This surveillance is described in transparency reports released by telecommunication companies, such as Vodafone; however, not all methods of lawful access are disclosed to the public. Though, when the public is aware that they are being monitored online, they will engage in self-censorship or a hesitance to engage in societal activities[120].

7.4.2 Game Scenario

The game-theoretical models presented in this section are motivated by the following scenario: Amara wants to transmit a secret e-mail m to her sister through a home internet connection. However, she is in an environment where the intelligence agencies and the government monitor all mobile phones, landline phones and internet communications; they are not trusted. The government and security agencies have an arsenal of monitoring equipment and capacity. A collaborative effort with the mobile network operators enables the government to monitor all networks traffic using capable steganalysis equipment. From the government's perspective, the motive for the monitoring activities is intended to increase security and reduce terrorism.

It is assumed that the conventional security techniques used for e-mail security are insecure; therefore, they can not be trusted. Besides e-mail, encryption techniques such as (Pretty Good Privacy) and GPG (GNU Privacy Guard) in some cases are complicated to set up on a local computer. Amara has two steganographic approaches that she can apply to successfully transmit the secret message. The initial approach chosen by Amara is the use of an affordable and straightforward stego-technique that does not require the usage of a secret key. The subsequent approach is to use the low-entropy and high-entropy steganographic systems. Both techniques can be employed to transmit the secret e-mail securely. Before she proceeds and transmits the secret e-mail to her sister, she uses a game-theoretical approach. This approach will enable her to model all interactive decision-making processes to predict the government and security agencies behaviour and unanticipated outcomes. In this scenario, Amara considers the government and security agencies as adversaries.

The steganographic games presented in this research adopt a defence-oriented perspective rather than the success of transmitting the secret message. The games are concerned with the design of the fundamental decisions and analysis processes involved in steganography and steganalysis and the possible usage of game theory for developing control frameworks and formal decisions. Another main characteristic of the steganographic games described in this paper is that the payoff functions in G_1 are modelled in such a manner that Amara, the stego-user, only has an incentive to use steganography in the absence of the intelligence agencies and the government looking for hidden messages. The intelligence agencies and the government are also encouraged to look at hidden content if steganography is used.

Table 7.1: Matrix for the simple stego-game G_1.

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$look$	$\neg look$
$hide$	$-c_{hide}, -c_{look}$	$-c_{hide}, 0$
$\neg hide$	$-c_{leak}, b_{leak} - c_{look}$	0,0

7.4.3 A Simple Stego Game

Notations

Let $G_1(c, b) \in \mathcal{G}$ represent a simple stego game between player $\mathcal{U}$ and $\mathcal{S}$. The notation $\mathcal{U}$ is Amara, that wishes to transmit a secret message to her friend. On the other hand, $\mathcal{S}$ denotes the intelligence agencies and the government that wishes to monitor all network traffic. The strategies employed by each player are $s_i = (hide, \neg hide)$ for $\mathcal{U}$ and $s_i = (look, \neg look)$ for $\mathcal{S}$. The notation $hide$ is the strategy of hiding or transmitting secret messages using a simple steganographic approach, while $\neg hide$ is the strategy of deciding not to implement a steganographic approach. Depending on the strategy utilised, both players can either benefit b or endure a cost c. b is the benefit of using a certain strategy, and c is the cost of using a certain strategy.

Based on table 7.1, player $\mathcal{U}$ can procure individual payoffs. The payoff includes c : cost of hiding c_{hide} is the effort to find or purchase a simple stego tool on the internet and to utilise the tool with negligent success. In contrast, the cost of secret message leaking c_{leak} is the indirect cost that occurs if the government reveals the secret message and they decide to take action (e.g. arrest, interrogate and use other approaches).

For player $\mathcal{S}$, the payoff b : b_{leak} is the benefit of leaking the secret message. It enables the establishment of legal laws to prevent crimes. The cost of looking at the secret message denoted by c_{look} is the time and money that is required to contact an ISP in order to retrieve the message content. It is important to note that looking c_{look} is not the same as extracting stego-content. Finally, the zero entries in the matrix indicate a no cost or benefit to either $\mathcal{U}$ or $\mathcal{S}$.

In this game, it is assumed that the payoffs $c_{leak} > c_{hide}$ and $b_{leak} > c_{look}$.

7.4.4 Entropy-Stego Game

In this section, the entropy stego game is described. All strategies deployed by both players are essential in this game as we attempt to describe a more sophisticated model that can be applied in a realistic setting. All strategies have a significant impact on the outcome of this game.

Table 7.2: Matrix for an Entropy-Stego Game $G_2(\cdot,\cdot)$

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}$	$n^{\mathcal{U}}_{scan}$
$h_{entropy}$	$-c_{high}, b_{s-scan}$	$b_{high}, -c_{n-scan}$
$l_{entropy}$	$b_{low}, -c_{s-scan}$	$b_{low}, -c_{n-scan}$

Player Strategies

Let $G_2(c, b)$ denotes an entropy stego-game. The low-entropy approach is denoted by $l_{entropy}$ while the high entropy approach is denoted by $h_{entropy}$. The government $\mathcal{S}$ has two approaches: detecting hidden messages with sophisticated steganalysis and naive steganalysis. These strategy are denoted by $\mathcal{S} = (s^{\mathcal{U}}_{scan}, n^{\mathcal{U}}_{scan})$ where $s^{\mathcal{U}}_{scan}$ denotes sophisticated steganalysis and $n^{\mathcal{U}}_{scan}$ denotes naive steganalysis.

Utility Functions

Both players can procure individual payoffs. For $\mathcal{S}$, the notation b_{s-scan} is the satisfaction obtained when the use of sophisticated steganalysis technique has been implemented successfully, which eventually leads to the establishment of laws and further understanding on how to detect sophisticated stego-techniques. This payoff also means that the secret message is detected, analysed and extracted. The notation c_{s-scan} is the cost sustained when sophisticated steganalysis is used effectively though the outcome is a negligent success. The cost of not detecting the use of stego-messages with a naive steganalysis approach is denoted by c_{n-scan}.

For $\mathcal{U}$, the notation c_{high} denotes the effort to find and purchase a suitable high-entropy stego tool on the internet and implement steganography with negligence success. The benefit of transmitting the stego message with the low-entropy approach, which remains successfully undetected by the government and security agencies alike, is represented as b_{low}. Finally, b_{high} denotes the benefit of successfully transmitting the stego message with the high-entropy approach. The possibility of detection by the government and security agencies is negligent.

Though, specifying generically what naive and sophisticated steganalysis is can be difficult. Steganalysis techniques are classified as signature-based and statistical-based. Under this class, each technique can be broadly classified into specific and universal steganalysis [154, 246]. Statistical steganalysis techniques are more vigorous and precise in results

Table 7.3: Matrix for an Extended Entropy-Stego Game G_3 for $\mathcal{U}$ and $\mathcal{S}$

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}$	s^{O}_{scan}
$l^{O}_{entropy}$	$-c^{pay}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}, -c^{v}_{scan}$	$-c^{pay}_{\mathcal{U}} - c^{v}_{en}, b^{v}_{scan} - c^{v}_{scan}$
$h^{\mathcal{U}}_{entropy}$	$-c^{hide(v)}_{\mathcal{U}} - c^{v}_{en}, b^{v}_{scan} - c^{v}_{scan}$	$b^{hide}_{\mathcal{U}}, -c^{v}_{scan}$

Table 7.4: Matrix G_3 for $\mathcal{U}$ and $\mathcal{S}$ using the parameter T

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}$	s^{O}_{scan}
$l^{O}_{entropy}$	$-c^{pay}_{\mathcal{U}} - (1-T) \cdot c^{max*}, -c^{v}_{scan}$	$-c^{pay}_{\mathcal{U}} - (1-T) \cdot c^{max*}, (1-T) \cdot b^{v}_{scan} - (1-T)^{-1} \cdot c^{v}_{scan}$
$h^{\mathcal{U}}_{entropy}$	$-c^{hide(v)}_{\mathcal{U}} - c^{v}_{en}, b^{v}_{scan} - c^{v}_{scan}$	$b^{hide}_{\mathcal{U}}, -(1-T)^{-1} \cdot c^{v}_{scan}$

than signature-based steganalysis, considering the mathematical algorithms used to detect tiny image alterations. Universal techniques are less effective than specific techniques [234]. However, a subsequent study in [154] suggests that universal techniques mitigate the limitations of specific statistical steganalysis by detecting hidden messages without knowing the embedding technique used. Advanced methods such as deep learning have already been used in steganalysis [175]. This technique is considered a universal steganalysis method [24], and it is also designed to be scalable [25] and computationally cost-effective [141, 131, 25]. Despite this, deep learning is only valid when embedding keys are not reused (e.g. different images) [171].

7.4.5 An Extended Entropy-Stego Game

In this section, the strategic game G_3 in standard form using the trust degree is obtained by a matrix described in Tables 7.3 and 7.4. A fundamental objective of G_3 is to maximise the utility function of both $\mathcal{U}$ and $\mathcal{S}$.

It is essential that if the parameter T has to be known for both players, then G_3 is considered a complete information game.

The notion of trust is introduced in this extended model. Here, the stego message is exposed to steganalysis extraction by the adversary through a vulnerability v found in an online stego software that can be subscribed or purchased. Since acquiring a high-entropy steganographic software can be considered unchallenging, $\mathcal{U}$'s decides to purchase a low-entropy online software from an Online Stego Service Provider (OSSP) that claims to offer suitable protection against powerful adversaries. To a reasonable extent, this will aid in the safety of the stego message from $\mathcal{S}$'s steganalysis. On the other hand, the stego message may be vulnerable to internal malicious exploitation by the OSSP.

If the secret message is transmitted through $\mathcal{U}$'s local computer or a neighbourhood cyber cafe, she will use a capable high entropy stego software. Though, the government agencies will eventually attempt to detect the use of steganography regardless. The high entropy stego system cannot be seen as challenging to implement, considering it follows the standard notion of steganography. On the other hand, implementing the low entropy stego system effectively can be tasking and requires a high level of expertise to implement adequately since, in some instances, it requires independent non-colliding channels.

It is presumed that the OSSP can provide secure online stego software and service. Although, this depends on the trustworthiness of the OSSP. In an ideal instance, the OSSP should be a third player in G_3; however, modelling the behaviour and capacities of the OSSP and stego tool can be complicated. Instead, it is represented preferably by a T parameter interpreted as the trust degree $\mathcal{U}$ has in the service. This study inspires the notion of trust degree used in this paper in [176] and [134].

When the utility function of G_3 is observed, it becomes apparent that this is a nonzero-sum game. In addition, the adversary has no prior knowledge of how and when $\mathcal{U}$ will use the low entropy and high entropy steganographic approaches.

Assumptions

In this section, an assumption is required by the G_3 model. When considering the scenario, it seems reasonably justified.

- It is reasonable to presume that the OSSP has appropriate resources to protect its infrastructure against external adversaries. Therefore, on purchase or subscription, there should be a binding agreement that is provided to $\mathcal{U}$ which guarantees security against external adversaries. This agreement is a formal document that describes the mutual accord between $\mathcal{U}$ and OSSP. If used correctly, it should meet the needs of $\mathcal{U}$ and reduce complex difficulties.

- The OSSP will guarantee $\mathcal{U}$ that their stego service will deliver sufficient security against powerful adversaries. However, it is presumed that this guaranty can not be trusted completely, considering the OSSP can be a spy for the government offering malicious online software, and if so, this will aid the government security agencies to extract the stego message m. The effectiveness of the steganalysis depends on the T parameter, which should satisfy $0 \leq T \leq 1$. The parameter T is defined as the degree of trust $\mathcal{U}$ has in the OSSP. When $T = 0$, then $\mathcal{U}$ lacks complete trust, whereas $T = 1$ denotes a full trust from the perspective of $\mathcal{U}$. If $0 < T < 1$, an assumption can be made that the OSSP partially respects the agreement. To prevent a ruined reputation, the OSSP will fully compensate $\mathcal{U}$ in the event $\mathcal{S}$ successfully benefits from any lack of sufficient security. This game asserts that the strength of the trust parameter T is directly proportional to the efficiency of the OSSP (OSSP); hence if $T = 1$, then the efficiency of the OSSP =100% and vice versa.

Player Strategies

Both players have two sets of strategies in G_3. The use of naive steganalysis by $\mathcal{S}$ is eliminated, and only the use of sophisticated steganalysis is considered. The removal of the naive steganalysis strategy is due to the assumption that the adversary would be using sophisticated technologies for steganalysis in a realistic scenario. The strategies are $s_i = (s^{\mathcal{U}}_{scan}, s^{O}_{scan})$ for $\mathcal{S}$, where the notation $s^{\mathcal{U}}_{scan}$ is the strategy that enables the adversary to use sophisticated steganalysis directly on $\mathcal{U}$. The strategy s^{O}_{scan} enables the adversary to use sophisticated steganalysis while $\mathcal{U}$ is using steganography through the OSSP.

The stego user's strategies are $s_i = (l^{O}_{entropy}, h^{\mathcal{U}}_{entropy})$. The strategy $l^{O}_{entropy}$ enables the stego user to use the low entropy steganography through the OSSP. The notation $h^{\mathcal{U}}_{entropy}$ represents $\mathcal{U}$'s strategy to use high entropy steganography while at home.

Utility Functions

This section describes the utility functions of both players. $\mathcal{U}$'s inability to successfully transmit m while using high-entropy and low entropy stego approaches as a result of steganalysis from $\mathcal{S}$ through a vulnerability v is denoted by c^{v}_{en}. The cost for subscribing or purchasing the online stego tool obtained from the OSSP is denoted by $c^{pay}_{\mathcal{U}}$. While $\mathcal{U}$ is responsible for protecting m and implementing the high entropy steganography locally on her system, the cost to hide from steganalysis is denoted by $c_{\mathcal{U}}^{hide(v)}$. In contrast, the benefit is denoted by $b_{\mathcal{U}}^{hide}$. However, if $T = 0$, then the cost function $c_{\mathcal{U}}^{hide(v)}$ when exploited by $\mathcal{S}$ is presented as follows:

$$c_{\mathcal{U}}^{hide(v)} = (1 - T) \cdot c^{max*},$$

where c^{max*} presumed to be equivalent to the maximum steganalysis exploitation by $\mathcal{S}$.

For $\mathcal{S}$, the notation c_{scan}^{v} is the cost for attempting to use steganalysis for detecting of m through v. Note that the notation c_{scan} is used for both naive and sophisticated steganalysis. The lack of steganographic security $\mathcal{U}$ sustains while being exploited by $\mathcal{S}$ through a security vulnerability v is presumed to be equivalent to the maximum steganalysis exploitation c^{max*}:

$$c_{en}^{v} = (1 - T) \cdot c^{max*}.$$

This equation is reasonable if the OSSP is considered completely untrusted ($T = 0$) as the attack on v would have to be seen as the maximum steganalysis exploitation possible to m. In the instance of an ideal situation, when ($T = 1$) the stego tool is completely trusted, and therefore steganalysis will be unsuccessful.

The adversary's cost function when exploiting v is presented:

$$c^{v}_{scan} = (1 - T)^{-1} \cdot c^{v}_{scan}.$$

Note that the closer the parameter T comes to the value $T = 1$, the greater the cost will be if assumed that the OSSP will make steganalysis very challenging for the adversary. However, the model cannot be precisely used for the value $T = 1$ as the fraction contained in the equation would be undefined. In a realistic setting, it is hardly expected to have a completely trusted OSSP. In an instance where an OSSP is considered untrustworthy, it could be interpreted as contributory irresponsibility on the OSSP who is not optimising, updating and patching security vulnerabilities. This instance also means that the OSSP is a spy collaborating this the government.

For the benefit payoff, it is assumed that $b^{v}_{scan} > 0$. Using the T parameter, all benefit function are all related to each other:

$$b^{v}_{scan} = (1 - T) \cdot b^{v}_{scan}.$$

This equation is similar to the adversary's cost function with a distinction, the adversary benefits from exploiting vulnerabilities in the Online Stego Software. This is denoted by b^{v}_{scan}.

7.5 Justification For The Use of Game Theory

Due to the constant invention of system compromising techniques by adversarial entities [181] and the growing complexity of systems, a new perspective is needed to understand security from a strategic and decision-making perspective [248]. For instance, there is a need to capture scenarios where an adversary attacks a system while a defender aims to protect the system.

The traditional network security solutions have been used to provide security services (For example (CIA) confidentiality, integrity and availability) [248]. Though, the interconnected nature of devices and software makes protection challenging [226]. On the other hand, adversarial entities are constantly seeking new ways of penetrating systems [181] [248].

The limitations of current traditional solutions for network security is the use of complicated heuristics approaches [130] [226] and they are considered to be inadequate in dealing with advanced and sophisticated threats [10] [125] [128] [130]. These solutions lack dynamic interactions [212], [130] and quantitative decision framework [226] [9] [49]. According to the study in [199], the limitation of previous techniques and framework discussed in [7] and [8] is the lack of adequately modelling the behaviour of adversarial entities. Studies in [62] and [126] discussed instances where strategic controls treat adversaries as unintelligent and inactive agents.

Besides, the measurement of security is an essential aspect of network security; it is an evaluation of security services and security risks [146]. The categorization of network security is broad, and it includes the measurement of every aspect of network security. One aspect of this vital measurement is risk assessment [236]. Network security measurements require the interactions of adversaries and defenders, and the resulting measurements can be affected by their interactions. For instance, an essential standard in risk assessment for network security is the probability of the network being attacked.

There is a vital necessity to predict the behaviours of both adversarial and defenders. Since the interaction process between defenders and adversaries is considered a game process, game theory can be applied in every possible scenario to predict actions by modelling strategic interactions between the adversaries and defenders. Based on the study in [248], it can also be utilized to quantitatively analyze security assessment issues before determining the appropriate measures. This can greatly aid the decision-making process of (stego users)networks administrator's.

In this chapter, the use of game theory in a steganographic protocol environment is investigated. The use of game theory to quantitatively evaluate the protocol is vital in understanding the effectiveness of the security controls proposed in Chapters 5 and 6 of this thesis. Besides, it is used to predict the uncertain behaviour of adversarial entities described in Chapter 5 and unanticipated outcomes. The proposed framework captures the risks involved in using the low entropy steganography and high entropy steganography as a control mechanism by designing a use case in e-mail communication. The rationale for the use of e-mail communication as a use case is to demonstrate how the steganographic protocol can be applied and implemented in a different domain.

The range of models is designed in this chapter are simulated using the Matlab numeric computing environment. The Matlab program and linear optimisation are used to simulate and capture the best responses and optimal solutions (mixed Nash equilibrium strategies) of both the steganographic user and the adversarial entities. Furthermore, the Matlab game simulations capture the success rate of both players when choosing optimal mixed strategies.

7.6 Game Analysis

This section analyses the Nash Equilibrium of the three games presented in section 7.4. Note that the stego-games G_1 and G_2 does not admit a pure Nash Equilibrium solution whereas, in G_3, a pure Nash Equilibrium exist. The strategies and payoffs in these games are discussed in detail. The game models are further analysed are using numerical values that could correspond to those in a realistic circumstance.

7.6.1 Simple Stego Game Analysis

In order to solve the game G_1 and find the Nash Equilibria, all possible states are considered.

Table 7.5: Matrix for the simple stego-game $G_1(\cdot,\cdot)$ with $p-mix$ and $q-mix$.

$\mathcal{U}\downarrow\mathcal{S}\rightarrow$	$look\ (q)$	$\neg look\ (1-q)$
$hide\ (p)$	$-c_{hide}, -c_{look}$	$-c_{hide}, 0$
$\neg hide\ \ (1-p)$	$-c_{leak}, b_{leak}-c_{look}$	0,0

Theorem 1. *The security game has no pure Nash Equilibrium strategy.*

(a) State 1 $(hide, \neg look)$: In this state, the existence of pure Nash Equilibrium does not exist and therefore can not be asserted. Based on G_1, the strategy for player $\mathcal{U}$ is to hide the secret content, while for player $\mathcal{S}$, the strategy is not to look for hidden content. The ordinary properties of the payoffs are not optimal solutions.

Proposition 1: if $-c_{hide} > 0$, then the game G_1 does not admit a pure Nash Equilibrium strategy profile: $s = (hide, \neg look)$ and the correlated payoffs $s_{\mathcal{U}} = -c_{hide}$ and $s_{\mathcal{S}} = 0$ are not optimal.

Proof: Initially, when inspecting the game, verification is required when observing the strategy profile $(hide, \neg look)$, only player $\mathcal{U}$ benefits from remaining in that state. Since the payoff $-c_{hide} > 0$, this state is not suitable for $\mathcal{S}$ as $\mathcal{U}$ will successfully transmit the secret content in the context where $\mathcal{S}$ is $\neg look$; therefore there is no pure Nash Equilibrium solution.

(b) State 2 $(\neg hide, \neg look)$: In this state, the existence of pure Nash Equilibrium does not exist and therefore can not be established either. In this state, the strategy for player $\mathcal{U}$ and $\mathcal{S}$ is not hiding and not looking, respectively. This state is not stable, and it is not an optimal solution; hence the existence of Nash Equilibrium is prohibited.

Proposition 2: if $\mathcal{U}$ and $\mathcal{S}$ plays the strategy $\neg hide$ and $\neg look$, then the respective payoffs $s_{\mathcal{U}} = 0$ and $s_{\mathcal{S}} = 0$ are equal, however, this state is not stable and therefore not optimal.

Proof: The validation of this proposition is carried out similarly to that of*proposition 1* by comparing the changes in the payoffs. When observing the matrix, the payoff of $\mathcal{U}$ and $\mathcal{S}$ yield solutions that make both players indifferent from each other. It seems like an optimal solution; however, it is not the case. This state hinders pure Nash Equilibrium due to its unstable nature as both players can change their strategy to a desirable one. For example, the change of strategy to a more desirable payoff $\neg look \longrightarrow look$ will yield the payoff $b_{leak} - c_{look}$ for $\mathcal{S}$, will necessitate $\mathcal{U}$ to change strategy from$\neg hide \longrightarrow hide$ and yield the payoff $-c_{hide}$. Likewise, vice-versa if $\mathcal{U}$'s decides to change strategy, the game's outcome can be affected.

(c) State 3$(\neg hide, look)$: Slightly similar to the previous state, one derives a non-optimal solution. Based on G_1, $\mathcal{U}$ plays with the strategy $\neg hide$, while $\mathcal{S}$ play the $look$ strategy. The result produced is similar to *state 1*.

Proposition 3: If $-c_{leak} < b_{leak} - c_{look}$ then the game G_1 does not admit a pure Nash Equilibrium with the strategy $s = (\neg hide, look)$ and the corresponding payoff $s_{\mathcal{U}} = (-c_{leak})$ and $s_{\mathcal{S}} = (b_{leak} - c_{look})$.

Proof: It needs to noted that when observed closely the strategy $s_{\mathcal{S}} = (b_{leak} - c_{look})$ will yield a payoff u. Formally, $u = b_{leak} - c_{look}$, where $u < b_{leak}$ and $u > c_{look}$. However, a closer inspection on *State 3* will reveal that $b_{leak} - c_{look} > -c_{leak}$, therefore a pure Nash Equilibrium can not be achieved in this state.

(d) State 4$(hide, look)$: Here, the Nash Equilibria does not exist if the players, $\mathcal{U}$ and $\mathcal{S}$ apply the current strategies $s = (hide, look)$.

Proposition 4: If $-c_{hide} < -c_{look}$, then the game does not admit a Nash Equilibria as in the other states, therefore the respective payoffs $s_{\mathcal{U}} = (-c_{hide})$ and $s_{\mathcal{S}}(-c_{look})$ are not optimal.

Proof: It is clear that the payoff $-c_{hide}$ for $\mathcal{U}$ is lesser than $-c_{look}$ as the effort to purchase a simple stego tool and utilise with a negligent success is not an optimal payoff. The player, $\mathcal{U}$, would prefer to change the current state to a more favourable state, such as using the $hide$ strategy when $\mathcal{U}$ is not looking $(\neg look)$. On the other hand, $\mathcal{S}$ would prefer to remain in this current state.

Theorem 2. *A mixed Nash Equilibrium strategy* $(s^*_{\mathcal{U}}, s^*_{\mathcal{S}})$ *is obtained, where* $p^* = \dfrac{b_{leak} - c_{look}}{b_{leak}}$ *and* $q^* = \dfrac{c_{hide}}{c_{leak}}$ *are the probability of hiding and looking respectively.*

Table 7.6: A mixed strategy Nash Equilibrium game

	L	R
U	a_1, a_2	b_1, b_2
D	c_1, c_2	d_1, d_2

Proof: When solving for Mixed-Strategy Nash Equilibria, consider the game in the table II. To check for a completely mixed-strategy equilibrium, we use the fundamental Nash theorem. Suppose the column player uses the strategy $\sigma = qL + (1 - q)$ (that is, plays L with probability q). Then, if the row player uses both U and D, they must both have the same payoff against q. The payoff to U against q is $qa_1 + (1 - q)b_1$, and the payoff to D against σ is $qc_1 + (1 - q)d_1$. Equating these two, we find

$$q = \frac{d_1 - b_1}{d_1 - b_1 + a_1 - c_1}.$$

The denominator must be nonzero, and the right-hand side must lie between zero and one for this to make sense. Note that the *column* the requirement determines player's strategy that *row* player's two strategies be equal.

Now suppose the row player uses strategy $\tau = pU + (1 - p)$ (that is, plays U with probability p). Then, if the column player uses both L and R, they must both have the same payoff againstτ. The payoff to L against τ is $p_{a_2} + (1 - p)c_2$, and the payoff to R against τ

is $pb_2 + (1-p)d_2$. Equating these two, we find

$$p = \frac{d_2 - c_2}{d_2 - c_2 + a_2 - b_2}.$$

The MNE (Mixed Nash Equilibrium) strategy for G_1 is computed and explained below. Let p and q respectively denote the probabilities that $\mathcal{U}$ and $\mathcal{S}$ decides to use the mixed strategies $i \in \{1,2\}$ so that:

$p = P[hide]$ and consequently, $P[\neg hide] = 1 - p.$

likewise for $\mathcal{S}$,

$q = P[look]$ and $q = P[\neg look] = 1 - q$

At first we solve for $\mathcal{U}$'s mixed strategy

$$EU^{look}_{\mathcal{S},mix} = EU^{\neg look}_{\mathcal{S},mix}$$

$$EU^{look}_{\mathcal{S},mix} = f(P_{hide})$$

$$EU^{\neg look}_{\mathcal{S},mix} = f(P_{\neg hide})$$

where $f(\cdot)$ is the function of a mixed strategy. $f(P_{hide})$ and $f(P_{\neg hide})$ are the probabilities that $\mathcal{U}$ will use $hide$ and $\neg hide$ as strategies. If player $\mathcal{S}$ plays $look(q)$ then he is at the mercy of player $\mathcal{U}$'s decision in choosing between $hide$ or $\neg hide$. The expected utility EU of $\mathcal{U}$ can be defined as:

$$EU_{\mathcal{S},mix}^{look} = -c_{look} \cdot p + b_{leak} - c_{look} \cdot (1-p)$$

$$EU_{\mathcal{S},mix}^{\neg look} = 0 \cdot p + 0 \cdot (1-p)$$

since

$$EU_{\mathcal{S},mix}^{look} = EU_{\mathcal{S},mix}^{\neg look}$$

then

$$-c_{look} \cdot p + b_{leak} - c_{look} \cdot (1-p) = 0 \cdot p + 0 \cdot (1-p)$$

Correspondingly, solving for $\mathcal{S}$'s mixed strategy,

$$EU_{\mathcal{U},mix}^{hide} = EU_{\mathcal{U},mix}^{\neg hide}$$

$$EU_{\mathcal{U},mix}^{hide} = f(Q_{look})$$

$$EU_{\mathcal{U},mix}^{\neg hide} = f(Q_{\neg look})$$

$$EU_{\mathcal{U},mix}^{hide} = -c_{hide} \cdot q + -c_{hide} \cdot (1-q)$$

$$EU_{\mathcal{U},mix}^{\neg hide} = -c_{leak} \cdot q + 0 \cdot (1-q)$$

$$-c_{hide} \cdot q + -c_{hide} \cdot (1-q) = -c_{leak} \cdot q + 0 \cdot (1-q)$$

$$\implies p^* = \frac{b_{leak} - c_{look}}{b_{leak} - c_{look} + c_{look}} = \frac{b_{leak} - c_{look}}{b_{leak}}$$

$$\implies q^* = \frac{c_{hide}}{c_{hide} - c_{hide} + c_{leak}} = \frac{c_{hide}}{c_{leak}}$$

Table 7.7: A Numerical Simple Stego-game G_1.

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$look\ (q)$	$\neg look\ (1-q)$	
$hide(p)$	$-30, -70$	$-60, 0$	$-30q + -60(1-q)$
$\neg hide\ (1-p)$	$-70, 30$	$0, 0$	$-70q + 0(1-q)$
	$-70p + 30(1-p)$	$0p + 0(1-p)$	

Based on G_1, $\mathcal{S}$ plays $look$ with q and $\neg look$ with $1 - q$. On the other hand, $\mathcal{U}$ plays $hide$ with p and $\neg hide$ with $1 - p$. If $\mathcal{U}$ best responds with a mixed strategy, then $\mathcal{S}$ must make $\mathcal{U}$ indifferent between playing $hide$ and $\neg hide$. The only way that $\mathcal{U}$ can be indifferent from $\mathcal{S}$ is by playing c_{hide}/c_{leak}. This means that some percentage of the time $\mathcal{U}$ gets a payoff of c_{hide} and gets c_{leak} some percentage of the time regards of choice, $\mathcal{U}$ will end up with the same utility. The mixed strategy $q^* = c_{hide}/c_{leak}$ makes $\mathcal{U}$ indifferent from $\mathcal{S}$.

7.6.2 Quantitative Example A

In this section, the $p-mix$ and $q-mix$ mixed NE solutions of our model G_1 are ascertained using numerical evaluation. Using these numerical values, the summary of the matrix for this scenario is presented in table 7.7. In this table, it is assumed that the payoff $s_{\mathcal{S}} = (b_{leak} - c_{look})$ under the strategy $s = (look)$ can be represented in a numerical manner $s_{\mathcal{S}} = (70 - 40)$.

Row player Optimal choice of p

$\mathcal{U}$ solve for the value of p that equates $\mathcal{S}$ payoff when positioned with $look$ or $\neg look$ strategy. The role player optimal choice of p is presented graphically in figure 7.1.

$$-70p + 30\,(1-p) \;= 0p + 0\,(1-p)$$

$$p = \frac{3}{10} \qquad (p = 0.3)$$

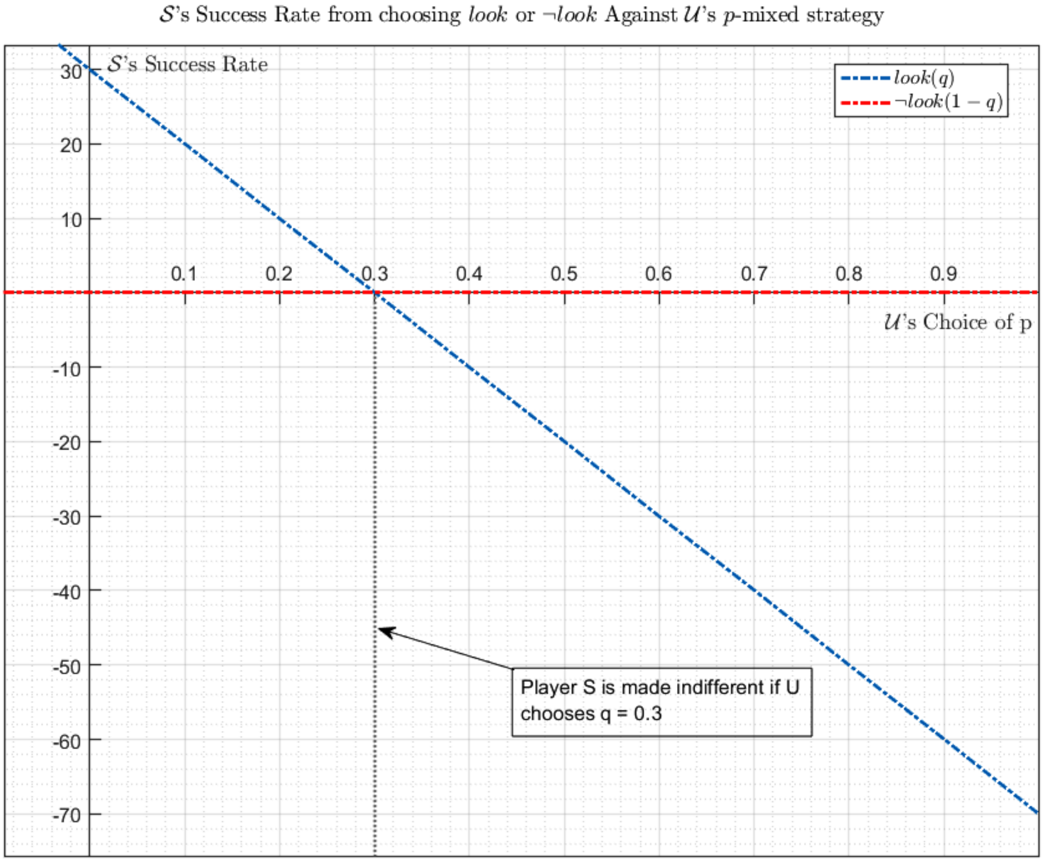


Figure 7.1: $\mathcal{S}$'s Success Rate from choosing $look$ or $\neg look$ against $\mathcal{U}$'s p-mixed strategy

If $\mathcal{U}$ plays *hide* with the probability $p = 0.3$ and $\neg hide$ with the probability of $1-p = 0.7$, then $\mathcal{S}$ success rate from

$$look = -70(0.3) + 30(0.7) = 0\%$$

$$\neg look = 0(0.3) + 0(0.7) = 0\%$$

$\mathcal{U}'$s success rate is 100%-$\mathcal{S}$ success rate = $100 - 0 = 100\%$

Column Players Optimal Choice of q

Here, $\mathcal{S}$ choose q in order to equalise the payoff of his opponent from playing a strategy. This necessitates the discernment on how $\mathcal{U}$'s payoff varies with $\mathcal{S}$'s choice of q. The column player optimal choice of q is represented in figure 7.2.

$\mathcal{S}$ solves for the value of q that equates to $\mathcal{U}$ payoff from playing *hide* or $\neg hide$:

$$-30q + -60(1-q) = -70q + 0(1-q)$$

$$q = \frac{3}{5} \quad (q = 0.6)$$

If $\mathcal{S}$ positions himself for *hide* with probability $q = 0.6$ and $\neg hide$ with probability $1 - q = 0.4$, then $\mathcal{U}'$s success rate from:

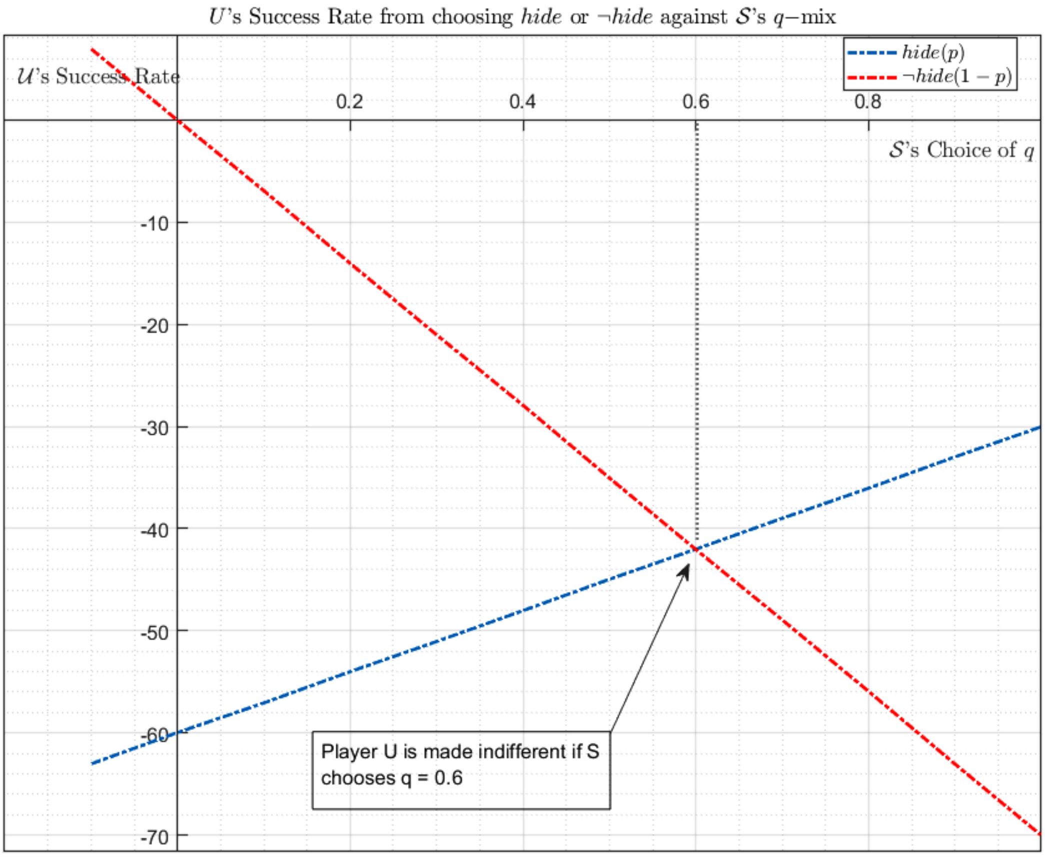


Figure 7.2: $\mathcal{U}$'s Success Rate from choosing *hide* or ¬*hide* against $\mathcal{S}$'s q-mix

$$hide = 30\,(0.6)\ + 60\,(0.4) = -42\%$$

$$\neg hide = 70\,(0.6)\ +\ 0\,(0.4) = 42\%$$

$\mathcal{S}$ success rate is $100\% - \mathcal{U}$ success rate: $100 - -42\% = 142\%$

$\mathcal{S}$ success rate is $100\% - \mathcal{U}$ success rate: $100 - 42\% = 58\%$

7.6.3 Combining the Best Response Functions Reveals the Mixed Strategy Nash Equilibrium

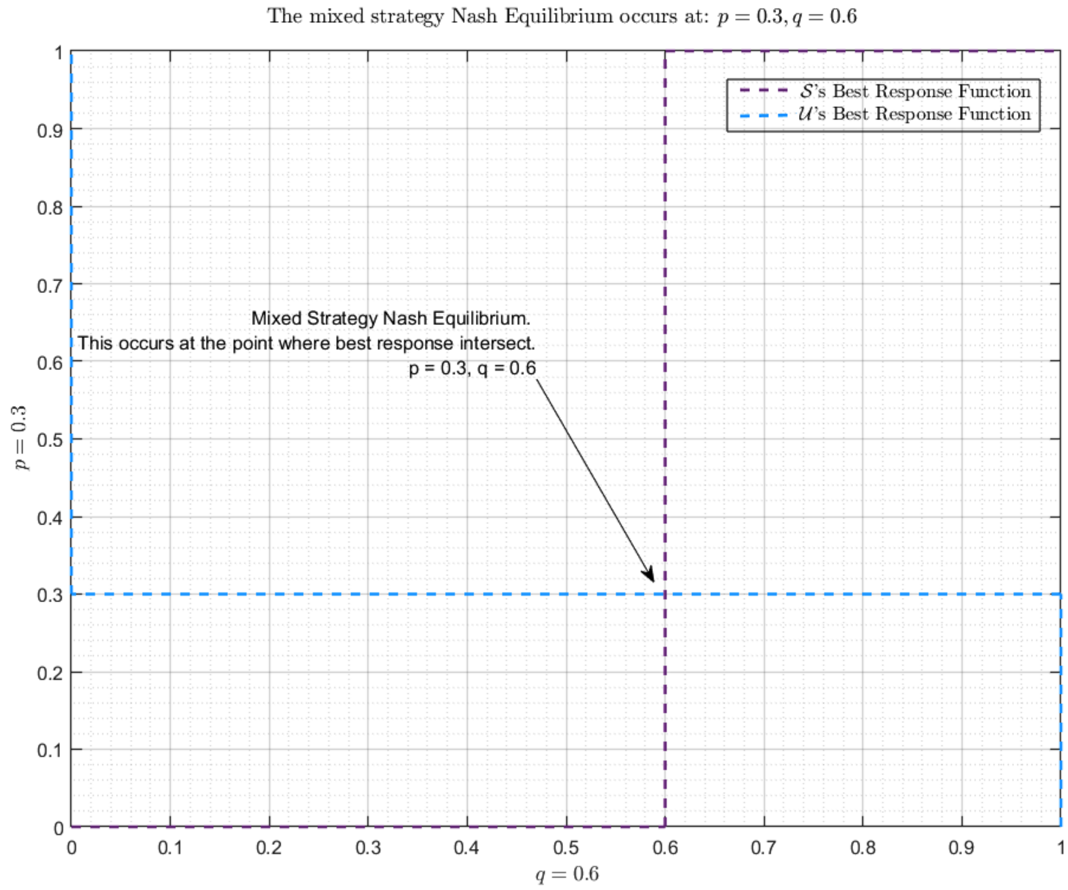


Figure 7.3: The Mixed Strategy Nash Equilibrium Occurs at $p = 0.3, q = 0.6$

An Alternative way to depict both players choice of mixing probability (Recall $p = P(hide)$ by $\mathcal{U}$, $q = P(look)$ by $\mathcal{S}$). This reveals the best strategic response of $q = f(p)$ and $p = g(q)$. The Nash Equilibrium, mixed, is obtained at the point where the best response functions intercept. In our model, the mixed strategy Nash Equilibrium occurs at $p = 0.3, q = 0.6$ as shown in Figure 7.3.

7.6.4 Entropy-Stego Game Analysis

In order to solve the game G_2 and find the Nash Equilibrium, all possible states are examined.

Table 7.8: Matrix for an Entropy-Stego Game $G_2(\cdot,\cdot)$ with $p - mix$ and $q - mix$

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}(q)$	$n^{\mathcal{U}}_{scan}(1-q)$
$h_{entropy}(p)$	$-c_{high}, b_{s-scan}$	$b_{high}, -c_{n-scan}$
$l_{entropy}(1-p)$	$b_{low}, -c_{s-scan}$	$b_{low}, -c_{n-scan}$

Theorem 3. *The entropy stego-game has no pure Nash Equilibrium strategy.*

(a) State 1 $(h_{entropy}, s^{\mathcal{U}}_{scan})$: The existence of pure Nash Equilibrium does not exist in this state. Based on G_2, the strategy for player $\mathcal{U}$ is to hide the secret content using the high-entropy stego approach; for player $\mathcal{S}$, the strategy is to use the sophisticated steganalysis. The components of the payoffs yield no optimal solution.

Proposition 1: If $b_{s-scan} > -c_{high}$ then the game G_2 does not admit a pure Nash Equilibrium strategy profile: $s = (h_{entropy}, s^{\mathcal{U}}_{scan})$ and the payoffs $s_{\mathcal{U}} = -c_{high}$ and $s_{\mathcal{S}} = b_{s-scan}$ are not optimal.

Proof: At first, when observing the strategy profile: $(h_{entropy}, s^{\mathcal{U}}_{scan})$, player $\mathcal{U}$ does not benefit from remaining in that state. Since there is a cost for $\mathcal{U}$ when using the strategy $h_{entropy}$ and a benefit for $\mathcal{S}$ when using $s^{\mathcal{U}}_{scan}$, this state is not suitable as $\mathcal{S}$ will successfully decode and extract the secret content; therefore there is no pure Nash Equilibrium solution.

(b) State 2 $(h_{entropy}, n^{\mathcal{U}}_{scan})$: In this state, the existence of Nash equilibrium does not exist. Player $\mathcal{U}$ plays using the high entropy stego approach, while $\mathcal{S}$ plays with the naive

steganalysis. The resulting strategies are not optimal.

Proposition 2: If $b_{high} > -c_{n-scan}$ then a pure Nash Equilibrum can not be asserted under the strategy profile:$s = (h_{entropy}, n^{\mathcal{U}}_{scan})$ and the payoffs $s_{\mathcal{U}} = b_{high}$ and $s_{\mathcal{S}} = -c_{n-scan}$ are not optimal.

Proof: When observing the strategy profile: $s = (h_{entropy}, n^{\mathcal{U}}_{scan})$. The only player that benefits from this state are $\mathcal{U}$. It is assumed that using naive steganalysis is not robust enough to detect the use of steganography implemented with the high entropy approach; perhaps using the sophisticated steganalysis will be suitable.

(c) State 3 $(l_{entropy}, n^{\mathcal{U}}_{scan})$: The strategy profile in this state does not admit a Nash Equilibrium either. $\mathcal{S}$ plays with the low entropy approach while $\mathcal{U}$ plays with the naive steganalysis approach.

Proposition 3: If $b_{low} > -c_{n-scan}$ then Nash Equilibrium game does not be asserted in this game under the strategy profile used by both players. The payoffs $s_{\mathcal{U}} = b_{low}$ and $s_{\mathcal{S}} = -c_{n-scan}$ are not optimal payoffs.

Proof: The payoff b_{low} is the benefit of using the low-entropy stego approach to transmit the secret message with success is more significant than $-c_{n-scan}$. The strategy profile in this current state benefits only $\mathcal{U}$ and will force $\mathcal{S}$ to change strategy from $n^{\mathcal{U}}_{scan} \rightarrow s^{\mathcal{U}}_{scan}$. It is assumed that using naive-steganalysis detection is not robust in detecting secret messages transmitted with the low entropy approach. Therefore, there is no Nash Equilibrium.

(d) State 4 $(l_{entropy}, s^{\mathcal{U}}_{scan})$: Similar to state 1 and 2 the strategy profile s used by both players are not optimal. $\mathcal{U}$ plays with the low entropy stego approach, while $\mathcal{S}$ plays with

the sophisticated naive steganalysis.

Proposition 4: If $b_{low} > -c_{s-scan}$ then the game does not admit a pure nash equilibrium under the strategy used by both players in state 3.

Proof: The strategy profile used by both players in this current state benefits only $\mathcal{U}$. Sophisticated steganalysis is suitable for analysing channels and covert channels with hidden content. However, it is assumed that the nature of the low entropy stego approach makes it difficult for sophisticated algorithms to detect hidden content. For example, transmitting fake generic messages on a channel looks unsuspicious when monitored by steganalyst.

Theorem 4. *A mixed Nash Equilibrum strategy* $(s^*_{\mathcal{U}}, s^*_{\mathcal{S}})$ *is obtained, where* $p^* = \dfrac{-c_{s-scan} + c_{n-scan}}{b_{s-scan} - c_{s-scan}}$ *and* $q^* = \dfrac{-b_{high} + b_{low}}{-b_{high} + c_{high}}$ *are the probability of hiding and looking respectively.*

The MNE (Mixed Nash Equilibrium) strategy for G_2 is computed and explained below. Let p and q respectively denote the probabilities that $\mathcal{U}$ and $\mathcal{S}$ decides to use the mixed strategies $i \in \{1, 2\}$ so that:

$p = P[(h_{entropy}]$ and consequently, $P[(l_{entropy}] = 1 - p$.

likewise for $\mathcal{S}$,

$q = P[s^{\mathcal{U}}_{scan}]$ and $q = P[n^{\mathcal{U}}_{scan}] = 1 - q$

At first we solve for $\mathcal{U}$'s mixed strategy

$$EU^{s^{\mathcal{U}}_{scan}}_{\mathcal{S},mix} = EU^{n^{\mathcal{U}}_{scan}}_{\mathcal{S},mix}$$

$$EU_{\mathcal{S},mix}^{s_{scan}^{\mathcal{U}}} = f(P_{h_{entropy}})$$

$$EU_{\mathcal{S},mix}^{n_{scan}^{\mathcal{U}}} = f(P_{l_{entropy}})$$

where $f(\cdot)$ is the function of a mixed strategy, $f(P_{h_{entropy}})$ and $f(P_{l_{entropy}})$ are the function of the probabilities that $\mathcal{U}$ will use the high-entropy and low-entropy as strategies.

If player $\mathcal{S}$ plays $s_{scan}^{\mathcal{U}}(q)$ then he is at the mercy of player $\mathcal{U}$'s decision in choosing between $h_{entropy}$ or $l_{entropy}$.

The expected utility EU of $\mathcal{U}$ can be defined as:

$$EU_{\mathcal{S},mix}^{s_{scan}^{\mathcal{U}}} = b_{s-scan} \cdot p + -c_{s-scan} \cdot (1-p)$$

$$EU_{\mathcal{S},mix}^{n_{scan}^{\mathcal{U}}} = -c_{n-scan} \cdot p + -c_{n-scan} \cdot (1-p)$$

since

$$EU_{\mathcal{S},mix}^{s-scan} = EU_{\mathcal{S},mix}^{n-scan}$$

then

$$b_{s-scan} \cdot p + -c_{s-scan} \cdot (1-p) = -c_{n-scan} \cdot p + -c_{n-scan} \cdot (1-p)$$

Correspondingly, solving for $\mathcal{S}$'s mixed strategy,

$$EU_{\mathcal{U},mix}^{h_{entropy}} = EU_{\mathcal{U},mix}^{l_{entropy}}$$

$$EU_{\mathcal{U},mix}^{h_{entropy}} = f(Q_{s-scan})$$

$$EU^{l_{entropy}}_{\mathcal{U},mix} = f(Q_{n-scan})$$

$$EU^{h_{entropy}}_{\mathcal{U},mix} = c_{high} \cdot q + b_{high} \cdot (1-q)$$

$$EU^{l_{entropy}}_{\mathcal{U},mix} = b_{low} \cdot q + b_{low} \cdot (1-q)$$

$$-c_{high} \cdot q + b_{high} \cdot (1-q) = b_{low} \cdot q + b_{low} \cdot (1-q)$$

$$\implies p^* = \frac{c_{s-scan} - c_{n-scan}}{b_{s-scan} + c_{s-scan}}$$

$$\implies q^* = \frac{b_{high} - b_{low}}{b_{high} + c_{high}}$$

7.6.5 Quantitative Example B

Table 7.9: A Numerical Entropy Based Stego-game G_2.

$\mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s - scan\,(q)$	$n - scan\,(1-q)$	
$high - en(p)$	$-30, 80$	$70, -30$	$-30q + 70(1-q)$
$low - en\,(1-p)$	$80, -40$	$80, -30$	$80q + 80(1-q)$
	$80p + -40(1-p)$	$-30p + -30(1-p)$	

In this section, we ascertain the mixed NE solutions of our model G_2 through numerical evaluation that could correlate with a realistic setting. The mixed strategies are established by computing the options between the $p - mix$ and $q - mix$. Using these numerical values, the matrix summary for this scenario is presented in table 7.9.

Row player Optimal choice of p

$\mathcal{U}$ solve for the value of p that equates $\mathcal{S}$ payoff from positioning himself for $s^{\mathcal{U}}_{scan}$ or $n^{\mathcal{U}}_{scan}$. This is presented graphically in Figure 7.4.

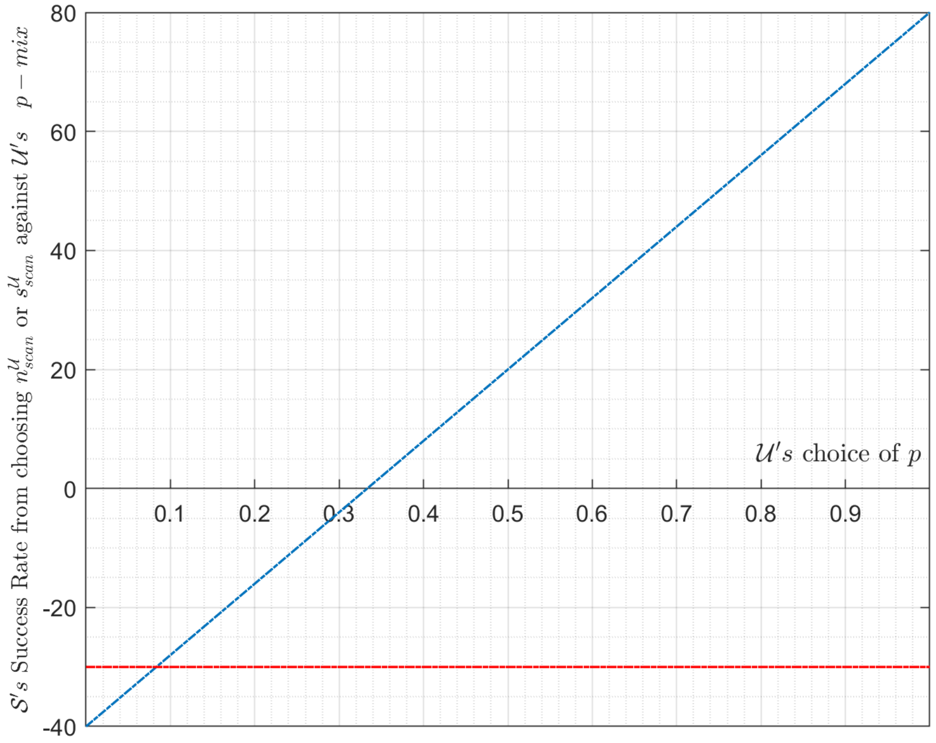


Figure 7.4: $\mathcal{S}$'s Success Rate from choosing $s^{\mathcal{U}}_{scan}$ or $n^{\mathcal{U}}_{scan}$ against $\mathcal{U}$'s p-mixed strategy

$$80p + -40\,(1-p) = -30p + -30\,(1-p)$$

$$: p = \frac{1}{12} \qquad (p = 0.08)$$

If $\mathcal{U}$ plays $h_{entropy}$ with the probability $p = 0.08$ and $l_{entropy}$ with the probability of $1 - p = 0.92$, then $\mathcal{S}$ success rate from

$$s^{\mathcal{U}}_{scan} = 80\,(0.08) + -40\,(0.92) = -30.4\%$$

$$n^{\mathcal{U}}_{scan} = -30\,(0.08) + -30\,(0.92) = -30\%$$

$\mathcal{U}'$s success rate is 100%-$\mathcal{S}$ success rate: $100 - -30.4 = 130.4\%$

$\mathcal{U}'$s success rate is 100%-$\mathcal{S}$ success rate: $100 - -30 = 130\%$

Column Players Optimal Choice of q

$\mathcal{S}$ solve for the value of p that equates $\mathcal{U}$ payoff when positioning the $h_{entropy}$ or $l_{entropy}$ strategy.The column player optimal choice of q is represented in Figure 7.5.

$$-30q + 70\,(1 - q) = 80q + 80\,(1 - q)$$

$$: q = -\frac{1}{10} \quad (q = -0.1)$$

If $\mathcal{S}$ plays $s^{\mathcal{U}}_{scan}$ with the probability $p = -0.1$ and $n^{\mathcal{U}}_{scan}$ with the probability of $1-p = 1.1$, then $\mathcal{U}$ success rate from

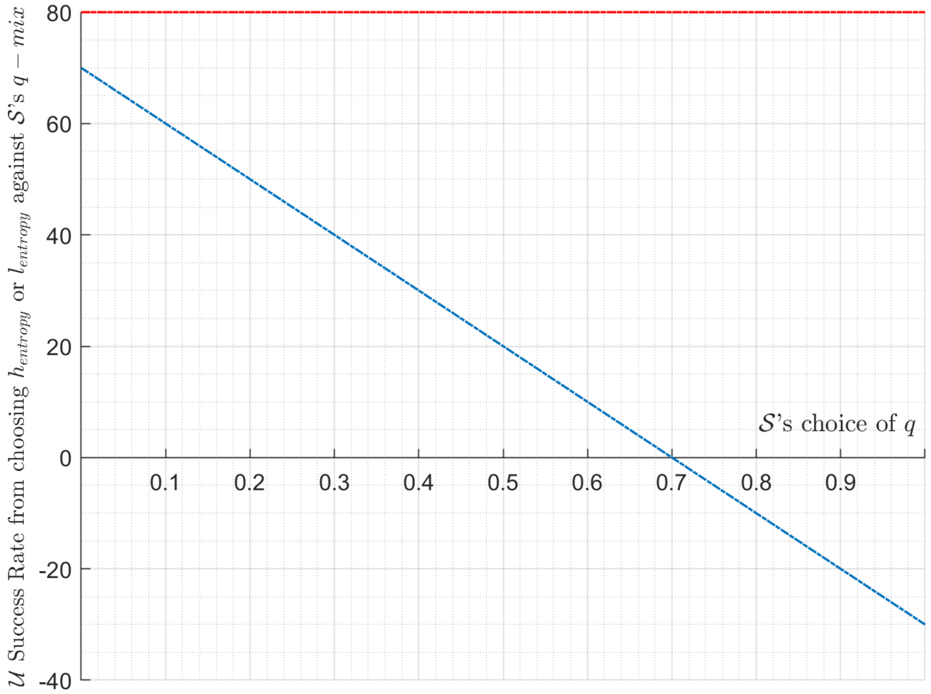


Figure 7.5: $\mathcal{U}$'s Success Rate from choosing $h_{entropy}$ or $l_{entropy}$ against $\mathcal{S}$'s $q - mix$

$$h_{entropy} = -30\,(-0.1) + 70\,(1.1) = 80\%$$

$$l_{entropy} = 80\,(-0.1) + 80\,(1.1) = 80\%$$

$\mathcal{S}'$s success rate is $100\% - \mathcal{U}$ success rate $= 100 - 80 = 20\%$

In our G_2 model, the mixed strategy Nash Equilibrium occurs at $p = 0.08, q = -0.1$.

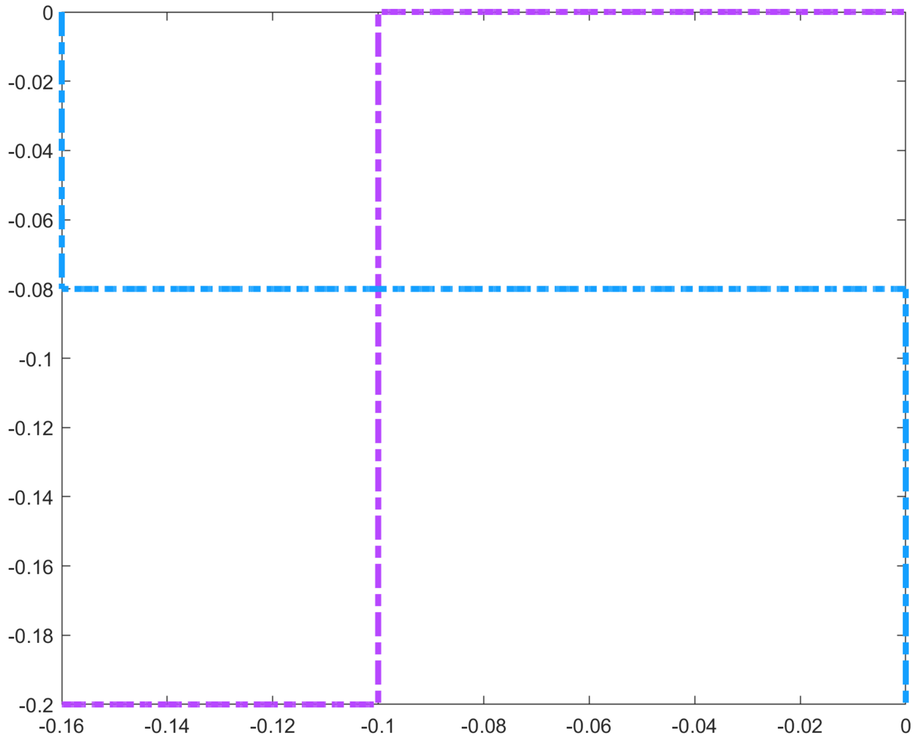


Figure 7.6: The Mixed Strategy Nash Equilibrium occurs at $p = 0.08, q = -0.1$

Table 7.10: Matrix G_3 for $\mathcal{U}$ and $\mathcal{S}$ where $T = 1$

$T = 1, \mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}$	s^{O}_{scan}
$l^{O}_{entropy}$	$-c^{pay}_{\mathcal{U}}, -c^{v}_{scan}$	$-c^{pay}_{\mathcal{U}}, -\infty$
$h^{\mathcal{U}}_{entropy}$	$-c^{hide(v)}_{\mathcal{U}} - c^{v}_{en}, b^{v}_{scan} - c^{v}_{scan}$	$b^{hide}_{\mathcal{U}}, -\infty$

Table 7.11: Matrix G_3 for $\mathcal{U}$ and $\mathcal{S}$ where $T = 0$

$T = 0, \mathcal{U} \downarrow \mathcal{S} \rightarrow$	$s^{\mathcal{U}}_{scan}$	s^{O}_{scan}
$l^{O}_{entropy}$	$-c^{pay}_{\mathcal{U}} - c^{max*}, -c^{v}_{scan}$	$-c^{pay}_{\mathcal{U}} - c^{max*}, b^{v}_{scan} - c^{v}_{scan}$
$h^{\mathcal{U}}_{entropy}$	$-c^{hide(v)}_{\mathcal{U}} - c^{v}_{en}, b^{v}_{scan} - c^{v}_{scan}$	$b^{hide}_{\mathcal{U}}, -c^{v}_{scan}$

7.6.6 Extended Entropy-Stego Game Analysis

This section presents the analysis of the stego game G_3. The establishment of pure Nash Equilibrium is attained for two extreme cases of the complete lack of trust in the OSSP and complete trust in the Online Stego Service. At first, we show that the attainment of Nash Equilibrium cannot be established in G_3 with the T parameter.

(a) State 1 $(l^{O}_{entropy}, s^{\mathcal{U}}_{scan})$: This state clearly does not reveal the establishment of a pure Nash Equilibrium solution.

Proposition 1: If $-c^{pay}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}} > -c^{v}_{scan}$, then the G_3 does not demonstrate a pure Nash Equilibrium under the strategy profile: $s = (l^{O}_{entropy}, s^{\mathcal{U}}_{scan})$ which implies that the payoff $-c^{pay}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}$ and $s_{\mathcal{S}} = -c^{v}_{scan}$ are not optimal strategies.

Proof: On investigating the strategy profile $s = (l^{O}_{entropy}, s^{\mathcal{U}}_{scan})$ only $\mathcal{S}$ benefits from this state due to the lesser cost. $\mathcal{U}$ incurs two costs by trying to hide from the exploitation of steganalysis with the low entropy steganography strategy $l^{O}_{entropy}$. While $\mathcal{U}$ uses the low entropy steganography online through the OSSP, $\mathcal{S}$ scans $\mathcal{U}$ to detect the use of steganography. Since $-c_{\mathcal{U}}^{pay} - c_{\mathcal{U}}^{hide(v)} > -c_{scan}^{v}$ then the current strategy profile is not optimal and a pure Nash Equilibrium cannot be attained.

(b) State 2 $(l_{entropy}^{O}, s_{scan}^{O})$: The existence of pure Nash Equilibrium does not exist. In this state, the strategy for $\mathcal{U}$ and $\mathcal{S}$ is $l_{entropy}^{O}$ and s_{scan}^{O} respectively. The payoff in this state is not optimal.

Proposition 2: If $b_{scan}^{v} - c_{scan}^{v} > -c_{\mathcal{U}}^{pay} - c_{en}^{v}$, then the game $G3$ does not admit a pure Nash Equilibrium solution under the strategy profile: $s = (l_{entropy}^{O}, s_{scan}^{O})$, therefore, the correlated payoff $s_{\mathcal{U}} = -c_{\mathcal{U}}^{pay} - c_{en}^{v}$ and $s_{\mathcal{S}} = b_{scan}^{v} - c_{scan}^{v}$ are not optimal.

Proof: When inspecting $G3$ and observing the strategy profile $s = (l_{entropy}^{O}, s_{scan}^{O})$, it is obvious that only $\mathcal{S}$ benefits from this state despite the cost incurred $(u = b_{scan}^{v} - c_{scan}^{v})$. However, the stego user incurs a greater cost due to the vulnerability exploited by sophisticated steganalysis. Since the payoff $b_{scan}^{v} - c_{scan}^{v} > -c_{\mathcal{U}}^{pay} - c_{en}^{v}$, then pure Nash Equilibrium cannot be established.

(c) State 3 $(h_{entropy}^{\mathcal{U}}, s_{scan}^{O})$: Similarly, to previous states the establishment of pure Nash Equilibrium cannot be ascertained in this state. The strategy for $\mathcal{U}$ is $h_{entropy}^{\mathcal{U}}$ while $\mathcal{S}$ is s_{scan}^{O}.

Proposition 3: If $b_{\mathcal{U}}^{hide} > -c_{scan}^{v}$, then under the strategy profile: $(h_{entropy}^{\mathcal{U}}, s_{scan}^{O})$ the game $G3$ does not establish a pure Nash Equilibrium solution.

Proof: When observing and inspecting this state in $G3$ it can be verified that under the strategy profile $s = (h_{entropy}^{\mathcal{U}}, s_{scan}^{O})$, only the stego user $\mathcal{U}$ benefits in this state while

$\mathcal{U}$ sustains a cost. While $\mathcal{U}$ is responsible for using the high entropy steganography in this state, $\mathcal{U}$ attacks the OSSP. However, this is not optimal for both players as $\mathcal{U}$ benefits from the payoff $s_{\mathcal{U}} = b_{\mathcal{U}}^{hide}$ and this will oblige $\mathcal{S}$ to change strategy.

(d) State 4 $(h_{entropy}^{\mathcal{U}}, s_{scan}^{\mathcal{U}})$: In this state a pure Nash Equilibrium can not be established under the current strategy profile.

Proposition 4: If $b_{scan}^{v} - c_{scan}^{v} > -c_{\mathcal{U}}^{hide(v)} - c_{en}^{v}$, then under the strategy profile: $(h_{entropy}^{\mathcal{U}}, s_{scan}^{\mathcal{U}})$ the game G_3 does not admit a pure Nash Equilibrium solution.

Proof:When observing the strategy profile $s = (h_{entropy}^{\mathcal{U}}, s_{scan}^{\mathcal{U}})$, it is obvious that only $\mathcal{S}$ benefits from this state $(u = b_{scan}^{v} - c_{scan}^{v})$. Although, due to the vulnerability exploited by sophisticated steganalysis, the stego user incurs a greater cost. Since the payoff $b_{scan}^{v} - c_{scan}^{v} > -c_{\mathcal{U}}^{hide(v)} - c_{en}^{v}$, then establishment of a pure Nash Equilibrium is not possible.

Using the T parameter, a pure Nash Equilibrium strategy can be established under the strategy profile: $s = (l_{entropy}^{\mathcal{O}}, s_{scan}^{\mathcal{U}})$.

Theorem 5. *If $T = 1$ and the subsequent circumstances is satisfied:*

$$C_{\mathcal{U}}^{hide(v)} + C_{en}^{v} > C_{\mathcal{U}}^{pay},$$

then the strategy $s = (l_{entropy}^{\mathcal{O}}, s_{scan}^{\mathcal{U}})$ is a pure NE solution for G_3. However, if $T = 0$ and the condition is satisfied:

$$C^{max*} > C_{\mathcal{U}}^{hide(v)} + C_{en}^{v} - C_{\mathcal{U}}^{pay},$$

then the strategy $s = (h_{entropy}^{\mathcal{U}}, s_{scan}^{\mathcal{U}})$ is a pure NE solution for $G3$.

When $T = 1$, the pure NE solution does not seem to be considered desirable for $\mathcal{S}$ as they try to detect the use of steganography while $\mathcal{U}$ is using steganography through the OSSP. In a non-zero-sum game, these circumstances can occur.

Proof: When inspecting Table 7.10 and 7.11 the conditions of a pure NE, the Proof is obtained. It can be demonstrated that their utility function cannot be improved for both players when a different strategy is used. This notion is convincing when presuming that the other player does not change strategy. For the case $T = 1$, it is clear that if $\mathcal{U}$ changes strategies from $l_{entropy}^{O} \rightarrow h_{entropy}^{\mathcal{U}}$, then her utility is reduced. Likewise, If $\mathcal{S}$ changes from $s_{scan}^{\mathcal{U}} \rightarrow s_{scan}^{O}$, their utility will be reduced as well. If the cost of subscribing or purchasing an online stego tool from a completely trusted provider is less expensive than incurring double cost due to steganalysis when the strategy is changed, then the game admits a pure Nash Equilibrium under the strategy profile: $s = (l_{entropy}^{O}, s_{scan}^{\mathcal{U}})$. This condition is true if the OSSP would make steganalysis very challenging and steganography detection unsuccessful.

In the case where $T = 0$, then the strategy $s = (h_{entropy}^{\mathcal{U}}, s_{scan}^{\mathcal{U}})$ is inspected. It considers that changing $h_{entropy}^{\mathcal{U}} \longrightarrow l_{entropy}^{O}$ will reduce $\mathcal{U}'s$ utility. If the OSSP is considered completely untrustworthy and $\mathcal{S}$ successfully detects the use of steganography, then $\mathcal{U}$ will suffer a great cost under the strategy profile $s = (l_{entropy}^{O}, s_{scan}^{\mathcal{U}})$. It will be optimal if $\mathcal{U}$ retain the strategy $h_{entropy}^{\mathcal{U}}$. For $\mathcal{S}$ it is clear that the payoff $b_{scan}^{v} - c_{scan}^{v} > -c_{scan}^{v}$ and if strategy is changed the utility is reduced.

However, depending on the variables in G_3, it is not essential to achieve a pure Nash Equilibrium. A mixed Nash Equilibrium will always exist regardless.

7.7 Summary

In this chapter, we developed a novel theoretical framework for models that applies the concept of game theory to a range of steganographic protocol settings. The game theory models developed are based on two-player non-zero-sum complete information games in strategic standard form. Game theory is used to aid in assessing the risk involved when steganography is used through an Online Stego Service Provider (OSSP). The benefits and costs that arise for both players were modelled. To our knowledge, the models developed in this chapter is the first study that applies a steganographic user and adversarial-centric model in a game-theoretical setting. These models analyse both players' optimal strategies to achieve pure and mixed Nash Equilibrium solutions.

Chapter 8

Conclusion

Tis chapter concludes this thesis by summarising the proposed contributions and security solutions, discussing limitations and drawbacks, and indicating future research questions.

8.1 Thesis Summary

This thesis is motivated by the popularity of mobile banking, which has attracted various privacy and security challenges that directly impact users, banks and payment institutions. In this thesis, a novel steganographic protocol solution is developed to address different privacy and security problems in mobile banking, focusing on SMS banking, and suggest a suitable solution for the challenges discussed above.

The review content chapters of the thesis are Chapters 2, 3 and 4—chapter 2 reviews fundamental and essential security and cryptography concepts, with a focus on steganography. Subsequently, Chapter 3 and 4 discuss various literature bodies relevant to this thesis. The precise areas reviewed are security challenges in short message service (SMS) protocols, followed by security controls focusing on SMS banking transactions. The chapter finishes by reviewing the family of specialised multi-channel Online Social Network (OSN) protocols and security games based on steganography.

Chapters 5, 6 and 7 describe the contributions to knowledge. In particular, as the research in this thesis focuses on steganographic-enhancing technologies for secure SMS mobile banking, a novel secure SMS banking protocol that combines steganography by cover synthesis and steganography by cover modification is developed in Chapter 5. This system is secure against various adversarial entities. Subsequently, Chapter 6 improved this novel approach by using conventional network security protocol techniques for assuring message freshness in distributed authentication protocols. This feature ensures that the protocol can be secure against threats such as the multi-channel replay attack and multi-channel-man-in the middle attack. The enhanced security protocol could be essential for future real-world adaption. The previous contribution in chapter 5 establishes a thorough security analysis of the multi-channel protocol. Chapter 7 of this thesis presents three game-theoretic models used in adversarial decision processing. The game theory models are based on two-player non-zero-sum complete information games in strategic standard form. This framework is then used to evaluate the steganographic protocol of Chapters 5 and 6. A range of use cases is designed using the Matlab scientific tool, simulating these game-theoretical models.

8.2 Discussion

While this thesis has presented novel solutions to mitigate security issues in SMS-based banking using the steganographic multi-channel protocol, some limitations are arising from this contribution. In this section, these aspects are discussed: the potential misuse of the developed protocol in order to exchange confidential messages for purposes of criminal or other illegal activities and the difficulties of it remaining robust concerning multi-channel surveillance.

8.2.1 Multi-Provider Communication Exploit

In this section, we discuss the Short Message Service (SMS) and a simple, confidential messaging exploit, based on sending information through several independent channels, which can be challenging to detect and potentially prevented, expect in circumstances when these channels are monitored simultaneously. The example illustrated in Figure 8.1, shows that in addition to the security issues already outlined in Chapters 5 and 6, there is a danger of illicit use of SMS services which may only be prevented by cooperation between these providers. Let us consider a scenario in which Amara and Ebere are communicating parties who want to exchange confidential messages via SMS, to underpin their criminal or malicious activities. Amara wants to send a secret message S to Ebere using channels C_1, C_2 and C_3, each of which belongs to a different provider. She uses C_1 and C_2 to send "fake" messages S_1 and S_2 to Ebere, and then sends a third message $b = S \oplus S_1 \oplus S_2$ on channel C_3. S_3 has the characteristics of random noise, which could not be mistaken for a true message, but could nevertheless could be embedded as a steganographic payload in an image using LSB

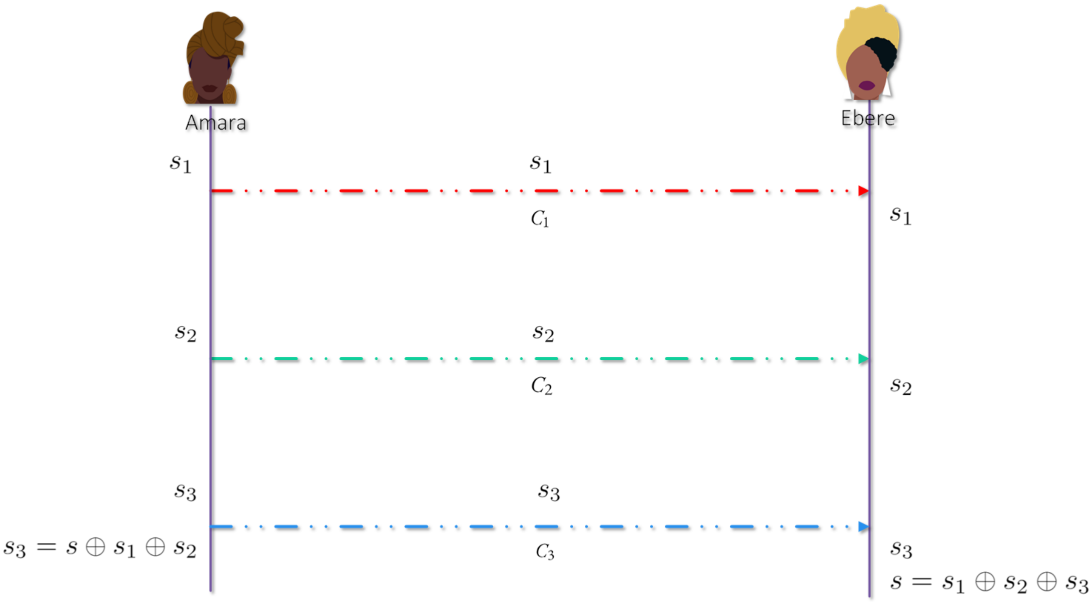


Figure 8.1: Attack using three independent channels to transfer message S

technique to allay suspicion. Bob easily recovers the original message $S = S_1 \oplus S_2 \oplus S_3$ while the channel providers remain unaware that any message has been sent. Even with cooperation between different providers, this attack could prove difficult to combat. It is possible that the pseudo nature of transactions S_1 and S_2 could be detected algorithmically, though Amara and Ebere could also use genuine messages between them for the same purpose. It is also possible that transmission and reception patterns between pairs of users could also reveal the presence of the attack, though this could also be masked by splitting and combining different elements of S_1 and S_2 to be sent at varying times.

Mitigating this form of threat discussed in Section 8.2 is potentially very difficult, as it requires cooperation between providers who are typically competitors and do not willingly share data. The collation and scrutiny of SMS data from independent providers will usually only occur if each provider is required to do so legally (e.g. typically for law enforcement or government security services compliance). Therefore, providing that Amara and Ebere communication activities do not draw the attention of the SMS providers they use, they can assume a reasonable level of confidence in using a multi-provider messaging exploit. Confidence can further be enhanced if Amara and Ebere utilise temporary "burner" mobiles, with pay-as-you-go SIMS, that are discarded after a brief period of use. Further research areas would include the investigation of multi-provider messaging exploit variants and possible strategies for mitigating them.

8.2.2 Traffic Analysis

In Chapter 6, the concept of traffic analysis is discussed. Traffic analysis can assist colluding adversaries to observe if users are communicating a secret message. Threats such as traffic analysis have always been a significant challenge, as explained in [115]. Though a study such as [243] proposed a solution to cope with this threat, they seem challenging to apply in our scenario. Further research will be required to investigate this aspect. In addition, this threat can be addressed through machine learning algorithms and artificial intelligence.

8.3 Further Work

This section will explore some items for further work, by considering two aspects relating to the research developed in this thesis: the suitability of the multi-channel protocol for real-world implementations resulting in a user-friendly product, and the future role of multi-channel protocols as mature, standardised controls in network security.

8.3.1 Usability

As explained in Chapter 5, users require a dual SIM phone (or alternatively, two mobile devices) in order for the multi-channel protocol to be implemented. Only this type of phone enables users to operate different mobile phone networks on one unit. Furthermore, the protocol requires a side-channel, the architecture suggested in the thesis was the use of a cybercafe. An open question is whether the approach could be improved, in order to yield a more user-friendly approach, suitable as a real-world mobile security architecture, deployable for large-scale implementations and usage. The main issue is the elimination of the side-channel, although, from an information-theoretical point of view, this seems difficult.

8.3.2 Multi-Channel Security Protocols

Chapters 5 and 6 of this thesis proposed a Multi-Channel Security Protocol for SMS mobile banking. As explained in these chapters, subscribers of this system require a dual SIM phone to use the multi-channel protocol successfully. This type of phone enables users to operate different mobile phone networks on one unit. Alternatively, two mobile phones can be used by subscribers. Furthermore, the protocol requires an additional channel; the architecture suggested in the thesis was the use of a cybercafe. An open question is whether the approach could be improved to yield a more user-friendly approach, suitable as real-world mobile security architecture, deployable for large-scale implementations and usage. The main issue is the elimination of the side-channel, although this seems challenging from an information-theoretical point of view. Otherwise, the consideration of using a single SIM phone could yield a more user-friendly system. The additional channel that adds a layer of security to the protocol can be replaced with a shared secret key k though this will require the bank and subscribers to keep the key secure. This approach is illustrated in the figure 8.2.

$$\begin{tikzcd}
Amara & & & Bank \\
\{m, m_1, k\} & & & k \\
& {} \arrow[r, "m_1", "C_1"'] & {} & \\
b = m \oplus m_1 \oplus k & & & \\
m_2 = E(b) & & & \\
& {} \arrow[r, "m_2", "C_2"'] & {} & \\
& & & b = D(m_2) \\
& & & m = b \oplus m_1 \oplus k
\end{tikzcd}$$

Figure 8.2: A Multi-Channel Steganographic Network Protocol Trace (b)

Preferably another approach can also be used instead. This approach will require the use of a security token. This token is a secure portable device that provides electronic authentication for users by storing some personal information. The usage of this security token requires that legitimate powers insert the device into a system to grant access to a network service. The service that is responsible for issuing security tokens is Security Token Service (STS) [14] [237]. Security tokens are of various kinds, including hardware tokens that contain USB Tokens that can be inserted into USB ports and wireless Bluetooth tokens or even programmable electronic key fobs, which can be activated remotely. However, tokens linked to computers and networks could present a severe security issue. Disconnected hardware tokens are not physically nor logically linked to any computer or network in any way; they do not require a particular input device, though instead, they have a built-in LCD screen that displays the generated authenticated data. The user manually inputs the generated data through a keypad or keyboard. Various hardware tokens contain an internal clock that combines a unique device identifier, password, fingerprint reading or input PIN to generate a code; the code lasts for 30 seconds. To increase the protocol's security described in Chapters 5 and 6 of this thesis, a hardware security token can be used to complete transactions on the bank website. Preferably, it can be combined so that a particular hardware token could be used to input $b = m \oplus m_1, \oplus m_2$ which generates an authentication code. Such an approach could improve security and prevent attacks such as coordinated attacks on all three channels; further studies are required for investigation.

Security hardware tokens are not without vulnerabilities, as with any computing system. If the device is stolen, stolen by a criminal or not in possession of the legitimate owner, then it is problematic. Besides, these devices present an increased level of security for the user's and are not functional without the services with which they are associated; therefore, it is necessary to keep them securely. Suppose an adversary wants to compromise a system that uses a hardware token. In that case, the adversary will need to steal a hardware token and compromise the infrastructure that was synchronized with the information output from the device or extract some vital information.

A central theme of this thesis was the concept of a security protocol, that uses n channels where, in contrary to most current protocol standards, $n > 2$, referred to as multi-channel protocol. It would be interesting to further investigate the use of multi-channel protocols in other settings, and to study the resulting advantages. It could be postulated that in the near future, multi-channel protocols might become mainstream, and might be adapted in major security standards for the web or mobile environments. In subsection 8.3.2 the potential use of the protocol in a system such as the block-chain is briefly discussed.

8.3.3 Trustless Secure Systems

The banks offer various mobile banking services which can be classified into models: mobile service provider-led, Third-Party Service Provider Model, and bank-led model. In this thesis, the Bank-Centric Model was mainly considered with a focus on SMS banking. The bank is considered a trusted entity that facilitates the transaction process leaving the transport and network functionalities to the mobile operators as shown in figures 5.10 and 5.11 of the multichannel steganographic protocol. In contrary to the proposed solutions described in this thesis, it would be interesting to research and evaluate the use of multi-channel protocols in block-chain applications and the resulting advantages. For instance, publishing the transactions m_1, m_2 and m_3 on the blockchain would increase security through immutability and privacy. The blockchain is a peer to peer public ledger that can perform transactions (structured into a linked list of blocks) without the need for a trusted or central authority. Besides decentralization, the blockchain has various benefits such as transparency [36].

8.3.4 Game Theoretical Models

In Chapter 7 of this thesis, three-game theoretical models were used to evaluate the protocol developed in Chapters 5 and 6. The game models present a robust security decision framework for using the multichannel steganographic protocol, though the scenario used to present the security practicalities of the approach is an email-based scenario. The scenario demonstrates that the protocol can be easily deployed and adopted in a different domain apart from SMS banking.

Game 1 presents a simple steganographic game where the steganographer and the adversaries use two strategies: $s_i = (hide, \neg hide)$ for $\mathcal{U}$ and $s_i = (look, \neg look)$ for $\mathcal{S}$, though G_1 does not model a realistic setting as in some situations adversarial entities would want to search and extract the hidden message. The extraction of secret messages with the use of $s^{\mathcal{U}}_{scan}$ strategy was modelled in game 2; besides, games 2 and 3 are considered more realistic models, though these games can be further improved. When adversarial entities look for ways to compromise a computing system or network, they are assumed to use multiple strategies. Since adversaries use multiple strategies, network security administrators should also employ a similar approach. The game models in Chapter 7 are limited to only two strategies that limit the protocol's evaluation results. Introducing more strategies will aid in capturing more risks and further predicting the behaviour of adversarial entities. The third game introduces a vital component known as the Online Stego Service provider, introducing an interesting Nash equilibrium outcome. The Online Stego Service provider is a T parameter that represents the level of trust $\mathcal{U}$ has in the steganographic service. Besides, it will be interesting to model the strategies and behaviour of the OSSP by introducing OSSP as a third player. These improvements would provide a more interesting Nash equilibrium outcome.

On the other hand, the G_3 can be extended to G_4 and applied in an SMS mobile banking setting, where the bank $\mathcal{B}$ can also be modelled as a third player.Solving a three-player game G_4 in table 8.1 might be challenging; however, such a game will be considered more realistic and suitable for a comprehensive analysis. The player strategies and utility function is described in following subsection.

Table 8.1: Matrix for an Extended Entropy-Stego Game G_4 for $\mathcal{U}, \mathcal{S}$ and $\mathcal{B}$

Player $\mathcal{B}$ plays $l^{defend}_{entropy}$		$\mathcal{S} \rightarrow$	
	$l^{defend}_{entropy}$ $h^{defend}_{entropy}$	$s^{\mathcal{U}}_{scan}$	$s^{\mathcal{B}}_{scan}$
$\mathcal{U} \downarrow$	$l^{B}_{entropy}$	$-c^{pay*}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}, - c^{v}_{scan},$ $b^{defend}_{controls} - c^{defend}_{controls}$	$-c^{pay*}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}, - c^{v}_{scan},$ $b^{defend}_{controls} - c^{defend}_{controls}$
	$h^{B}_{entropy}$	$-c^{pay}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}, - c^{v}_{scan},$ $b^{defend}_{controls} - c^{defend}_{controls}$	$-c^{pay}_{\mathcal{U}} - c^{hide(v)}_{\mathcal{U}}, b^{v}_{scan} - c^{v}_{scan},$ $b^{under(v)}_{controls} - c^{att(v)}_{controls}$

Player Strategies

Consequently, it is assumed that the bank in table 8.1 can be regarded to be a mutual team player of $\mathcal{U}$ since the bank is trusted according to Chapter 5, section 5.6. As both $\mathcal{U}$ and $\mathcal{B}$ are team players then their strategies could be linked. If $\mathcal{U}$ plays $l^{\mathcal{B}}_{entropy}$ then $\mathcal{B}$ will automatically choose $l^{defend}_{entropy}$ as strategy. If $\mathcal{U}$ choose $h^{\mathcal{B}}_{entropy}$ then $\mathcal{B}$ will choose strategy $h^{defend}_{entropy}$. The notations $l^{defend}_{entropy}$ and $h^{defend}_{entropy}$ are appropriate defensive strategies $\mathcal{B}$ will use for protection.

The strategies are $s_i = (s^{\mathcal{U}}_{scan}, s^{\mathcal{B}}_{scan})$ for $\mathcal{S}$, where the notation $s^{\mathcal{U}}_{scan}$ is the strategy that enables the adversary to use sophisticated steganalysis directly on $\mathcal{U}$ or even performing a man-in-the-middle attack or related attacks. The strategy $s^{\mathcal{B}}_{scan}$ enables the adversary to use sophisticated steganalysis while $\mathcal{U}$ is using steganography to transmit banking instruction to the bank through the different mobile network providers.

The stego user's strategies are $s_i = (l^{\mathcal{B}}_{entropy}, h^{\mathcal{B}}_{entropy})$. The strategy $l^{\mathcal{B}}_{entropy}$ enables the stego user to use the low entropy steganography to transmit banking instruction to $\mathcal{B}$ through the different mobile network providers. The notation $h^{\mathcal{B}}_{entropy}$ represents $\mathcal{U}$'s strategy to use high entropy steganography to transmit banking instruction to $\mathcal{B}$.

Utility Functions

For the payoff functions of this game, the notation $b^{defend}_{controls}$ is the benefit of securing bank servers while $\mathcal{S}$ attempts to compromise the steganographic system. On the other hand, $c^{defend}_{controls}$ is the cost of defending the bank. In other words, this cost function is the time, computing power and essential resources used to secure the system from steganalysis attacks. The notation $b^{under(v)}_{controls}$ is the benefits of understanding how the system vulnerability was exploited and penetrated, which leads to developing new controls, upgrading and patching systems. The notation $c^{att(v)}_{controls}$ is the cost sustained when the system is penetrated by $\mathcal{S}$ which will lead $\mathcal{B}$ to compensate $\mathcal{U}$ for losses.

For $\mathcal{U}$ the utility function $u_i = (-c^{pay}_{\mathcal{U}}, -c^{pay*}_{\mathcal{U}})$ are slightly different from those presented in Chapter 7, subsection 7.4.5. The notation $-c^{pay*}_{\mathcal{U}}$ is the cost of subscribing for or buying mobile phone airtime for the transmitting banking instructions, while $-c^{pay}_{\mathcal{U}}$ is the cost of subscribing or buying internet cybercafe time.

In G_3, the naive steganalysis strategy was removed since adversaries in the real world would not be willing to compromise systems using naive approaches; perhaps capturing all these strategies in a single game would also make an interesting outcome. Modelling a game where a strategy such as an "Advanced Persistent Threat" refers to well-organized, malicious adversarial entities who launch stealthy attacks against specific computer systems would also contribute to the protocol evaluation. Such an attack is long-lasting and challenging to expose and often use very advanced system penetration techniques. Finally, using Bayesian and stochastic game-theoretical approaches would provide an insightful protocol analysis.

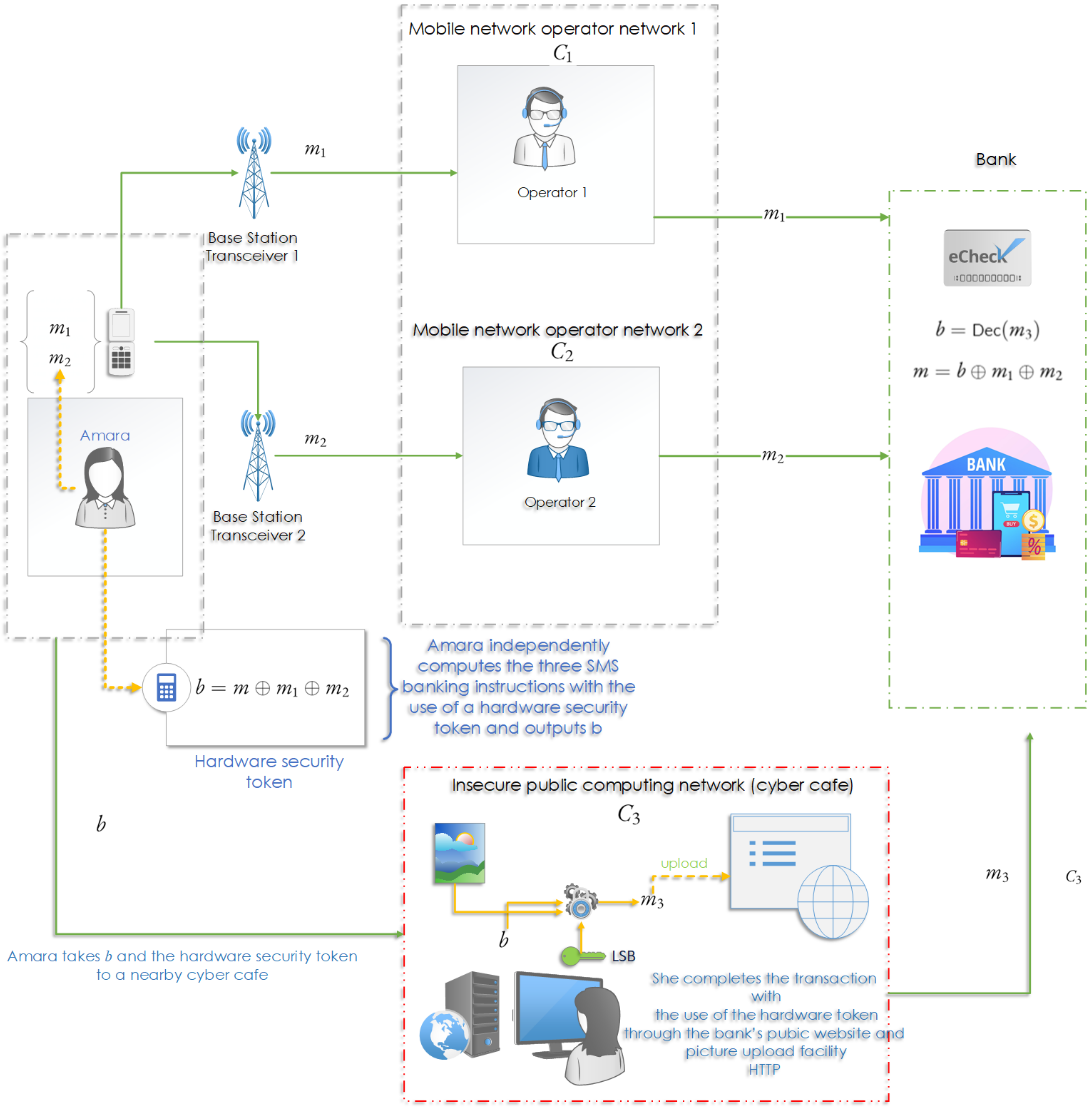

Mobile network operator network 1
C_1
Operator 1
m_1
Base Station Transceiver 1
m_1
Bank
eCheck
$b = \text{Dec}(m_3)$
$m = b \oplus m_1 \oplus m_2$
BANK
m_1
m_2
Mobile network operator network 2
C_2
Operator 2
Amara
m_2
Base Station Transceiver 2
m_2
$b = m \oplus m_1 \oplus m_2$
Amara independently computes the three SMS banking instructions with the use of a hardware security token and outputs b
Hardware security token
b
Insecure public computing network (cyber cafe)
C_3
upload
m_3
b
LSB
m_3
C_3
Amara takes b and the hardware security token to a nearby cyber cafe
She completes the transaction with
the use of the hardware token
through the bank's pubic website and
picture upload facility
HTTP

Figure 8.3: System Protocol Overview with hardware Token

References

[1] Access. USSD Banking, 2021.

[2] Adewoye, J. Impact of mobile banking on service delivery in the Nigerian commercial banks. *International Review of Management and Business Research 2*, 2 (2013), 333–344.

[3] Agoyi, M., and Seral, D. SMS security: An asymmetric encryption approach. In *Proceedings - 6th International Conference on Wireless and Mobile Communications, ICWMC 2010* (Valencia, 2010), IEEE, pp. 448–452.

[4] Agwu, E. M., and Carter, A.-L. Mobile Phone Banking In Nigeria: Benefits, Problems and Prospects. *International Journal of Business and Commerce 3*, 6 (2014), 50–70.

[5] Alam, S., Zakariya, S. M., and Rafiq, M. Q. Analysis of modified lsb approaches of hiding information in digital images. In *Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013* (Mathura, India, 2013), IEEE, pp. 280–285.

[6] Alam, S. B., Sakib, M. N., Rafi Sazzad, A. B. M., Shahnaz, C., and Fattah, S. A. Digital security algorithm for GSM incorporated virtual e-banking protocol using watermarking technique. In *2010 IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2010* (Luxor, Egypt,, dec 2011), IEEE, pp. 420–423.

[7] Albanese, M., Battista, E., and Jajodia, S. A deception based approach for defeating OS and service fingerprinting. In *2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015* (2015), IEEE, pp. 317–325.

[8] Almeshekah, Mohammed H and Spafford, E. H. Cyber Security Deception. In *Cyber deception* (2016), Springer, pp. 23–50.

[9] Alpcan, T., and Basar, T. An Intrusion Detection Game with Limited Observations. In *12th Int. Symp. on Dynamic Games and Applications* (Sophia Antipolis, France, 2006), vol. 26.

[10] Alpcan, T., and Başar, T. A game theoretic analysis of intrusion detection in access control systems. *Proceedings of the IEEE Conference on Decision and Control 2* (2004), 1568–1573.

[11] Alpcan, Tansu and Basar, T. *Network Security: A Decision and Game-Theoretic Approach*, 1 ed. Cambridge University Press, 2010.

[12] and others Nash, J. F. Equilibrium points in n-person games. *Proc. Natl. Acad. Sci. 36*, 1 (1950), 48–49.

[13] Anderson, R. E., Brunette, W., Johnson, E., Lustig, C., Poon, A., Putnam, C., Salihbaeva, O., Kolko, B. E., and Borriello, G. Experiences with a transportation information system that uses only GPS and SMS. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development - ICTD '10* (London, dec 2010), ACM, pp. 1–10.

[14] Andress, J. Identification and Authentication. In *The Basics of Information Security*. 2014, ch. 2, pp. 23–38.

[15] Arrow, K and Honkapohja, S. What is game theory trying to accomplish? In *Front. Econ. Oxford Basil Blackwell* (1985), pp. 5–46.

[16] Azimi, N. A., and Welch, H. G. The Effectiveness of Cost-Effectiveness Analysis in Containing Costs. *Journal of General Internal Medicine 13*, 10 (1998), 664–669.

[17] Bakerf, T., Baker, T., Gill, J., and Solovay, R. Relativizations of the $\mathcal{P} =?\mathcal{NP}$ Question. *SIAM J. Comput. 4*, 4 (1975), 431—-442.

[18] Baldwin, R. W., and Chang, C. V. Locking the e-safe. *IEEE spectrum 34*, 2 (1997), 40–46.

[19] Balfanz, D., Smetters, D. K., Stewart, P., Wong, H. C., Balfanz, D., Smetters, D. K., Stewart, P., and Wong, H. C. Talking To Strangers : Authentication in Ad-Hoc Wireless Networks Talking To Strangers : Authentication in Ad-Hoc Wireless Networks. In *NDSS* (2002), Citeseer.

[20] Bankole, F. O., Bankole, O. O., and Brown, I. Mobile Banking Adoption in Nigeria. *The Electronic Journal of Information Systems in Developing Countries 47*, 1 (2011), 1–23.

[21] Bankole;, F. O. B. O. B. I. T. J. B. Mobile Banking Adoption in Nigeria. *The Electronic Journal on Information Systems in Developing Countries 47*, 2 (2011), 1–23.

[22] Bao, T., Shoshitaishvili, Y., Wang, R., and Brumley, D. How Shall We Play a Game ? A Game-theoretical Model for Cyber-warfare Games. In *2017 IEEE 30th Comput. Secur. Found. Symp.* (Santa Barbara, California, USA, 2017), IEEE, pp. 7–21.

[23] Barnes, S. J., and Corbitt, B. Mobile banking: concept and potential. *International Journal of Mobile Communications 1*, 3 (2003), 273–288.

[24] Bayar, B., and Stamm, M. C. A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. In *Proc. 4th ACM Work. Inf. Hiding Multimed. Secur. - IH and MMSec '16* (2016), ACM, pp. 5–10.

[25] Bayram, S., Dirik, A. E., Sencar, H. T., and Memon, N. An ensemble of classifiers approach to steganalysis. In *Proc. - Int. Conf. Pattern Recognit.* (2010), pp. 4376–4379.

[26] Beato, Filipe and De Cristofaro, Emiliano and Rasmussen, K. B. Undetectable Communication : The Online Social Networks Case. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on* (Toronto, ON, Canada, 2014), IEEE, pp. 19—-26.

[27] Bellare, M., Boldyreva, A., Desai, A., and Pointcheval, D. Key-Privacy in Public-Key Encryption. In *Adv. Cryptol. - ASIACRYPT 2001, 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur. Gold Coast, Aust. December 9-13, 2001, Proc.* (2001), vol. 2248, Springer, Berlin, Heidelberg, pp. 566–582.

[28] Bellare, M., and Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conf. Comput. Commun. Secur.* (1993), no. November 1993, ACM, pp. 62–73.

[29] Bellia, P. Designing Surveillance Law. *Arizona State Law Journal 43*, 293 (2011).

[30] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., and Shamir, A. Key Recovery Attacks of Practical Complexity on {AES}-256 Variants with up to 10 Rounds. In *"Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (French Riviera, 2010), no. October 2000, Springer, Berlin, Heidelberg, pp. 299–319.

[31] Biryukov, Alex and Shamir, Adi and Wagner, D. Real Time Cryptanalysis of A5/1 on a PC. In *International Workshop on Fast Software Encryption* (2000), Springer, pp. 1–18.

[32] Black, C., and Ryan Gallagher. Swiss tech company boss accused of selling mobile network access for spying, 2021.

[33] Bogdan. How to build a PoC for business idea, 2019.

[34] Bojjagani, S., and Sastry, V. N. SSMBP: A secure SMS-based mobile banking protocol with formal verification. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015* (Abu Dhabi, United Arab Emirates, 2015), IEEE, pp. 252–259.

[35] Bojjagani, S., and Sastry, V. N. A secure end-to-end SMS-based mobile banking protocol. *Int. J. Commun. Syst. 30*, 15 (2017), 1–19.

[36] Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications 168*, June 2020 (2021), 114384.

[37] Branton, P. K. Document summarization using noun and sentence ranking, 2015.

[38] Brown, J., Shipman, B., and Vetter, R. SMS: The Short Message Service. *Computer 40*, 12 (dec 2007), 106–110.

[39] Bt Abd Rahman, N. A., Shajaratuddur Bt Harun, K., and Bt Yusof, Y. SMS banking transaction as an alternative for information, transfer and payment at merchant shops in Malaysia. In *3rd International Conference on Information Technology and e-Services, ICITeS 2013* (2013).

[40] Cachin, C. An Information-Theoretic Model for Steganography. In *Int. Work. Inf. Hiding* (1998), vol. 72, Springer, pp. 306– 318.

[41] Cancelli, G., and Barni, M. MPSteg-color: A new steganographic technique for color images. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2007), vol. 4567 LNCS, Springer Berlin Heidelberg, pp. 1–15.

[42] Chandramouli, Rajarathnam and Memon, N. Analysis of LSB based image steganography techniques Chandramouli. In *Analysis of LSB based image steganography techniques* (Thessaloniki, Greece, Greece, 2001), vol. 3, IEEE, pp. 1019–1022.

[43] Changescyclic, C., Dynamic, S., and Environments, L. An Image Steganography Technique using X-Box Mapping. In *Adv. Eng. Sci. Manag. (ICAESM), 2012 Int. Conf.* (Nagapattinam, Tamil Nadu, 2012), IEEE, pp. 709–713.

[44] Chikomo, K., Chong, M. K., Arnab, A., and Hutchison, A. Security of mobile banking. *University of Cape Town, South Africa, Tech. Rep., Nov 1* (2006), 1–10.

[45] Cho, E. M., and Koshiba, T. Secure SMS transmission based on verifiable hash convergent group signcryption. In *Proceedings - 18th IEEE International Conference on Mobile Data Management, MDM 2017* (Daejeon, jun 2017), IEEE, pp. 332–335.

[46] Clarke, C., Pfluegel, E., and Tsaptsinos, D. Enhanced Virtual Private Social Networks: Implementing user content confidentiality. In *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013* (London, UK, 2013), IEEE, pp. 306–312.

[47] Clarke, Charles A and Pfluegel, Eckhard and Tsaptsinos, D. Implementing Multi-channel Overlay Protocols : An Approach to Ad-hoc Message Authentication in Online Social Networks. In *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on* (London, UK, 2015), IEEE, pp. 1–6.

[48] Croft, N. J., and Olivier, M. S. A silent SMS denial of service (DoS) attack. *Inf. Comput. Secur. Archit. Res. Gr. South Africa 29* (2007).

[49] Dahiya, A., and Gupta, B. B. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Generation Computer Systems 117* (2021), 193–204.

[50] Daniel. Full List of Data Plans and Prices in Nigeria, 2020.

[51] David D. Kirkpatrick, and Azam Ahmed. Hacking a Prince, an Emir and a Journalist to Impress a Client. Tech. rep., 2018.

[52] De Cristofaro, E., Soriente, C., Tsudik, G., and Williams, A. Hummingbird: Privacy at the time of Twitter. In *Proceedings - IEEE Symposium on Security and Privacy* (San Francisco, CA, 2012), no. January 2011, IEEE, pp. 285–299.

[53] De Santis, A., Castiglione, A., Cattaneo, G., Cembalo, M., Petagna, F., and Petrillo, U. F. An extensible framework for efficient secure SMS. In *CISIS 2010 - The 4th International Conference on Complex, Intelligent and Software Intensive Systems* (Krakow, 2010), IEEE, pp. 843–850.

[54] Densmore, M. Experiences with bulk SMS for health financing in Uganda. In *Proceedings of the 2012 ACM annual conference extended abstracts on Human Factors in Computing Systems Extended Abstracts - CHI EA '12* (Austin, Texas, may 2012), ACM, pp. 383–398.

[55] Department of Justice. FAQ - Lawful Access – Consultation Document - Summary of Submissions to the Lawful Access Consultation - Lawful Access FAQ, 2005.

[56] DeRenzi, B., Findlater, L., Payne, J., Birnbaum, B., Mangilima, J., Parikh, T., Borriello, G., and Lesh, N. Improving community health worker performance through automated sms. In *Proceedings of the Fifth International Conference on Information and Communication Technologies and Development* (2012), ACM, pp. 25–34.

[57] Derks, D., Bos, A. E. R., and von Grumbkow, J. Emoticons and Online. *Soc. Sci. Comput. Rev. 26*, 3 (2007), 379—-388.

[58] Desoky, A. *Noiseless Steganography: The Key to Covert Communications*. Auerbach Publications, Boca Raton, 2012.

[59] Dey, S. K., Choudhary, P., and Gunter, F. A Detailed View on Spying Mobrob – Innovative Mobile Number Tracking System. In *2017 International Conference on Distributed Computing and Internet Technology (ICDCIT),* (Bhubaneswar, Odisha, India, 2017), Researchgate, pp. 1–5.

[60] Díaz, C., Seys, S., Claessens, J., and Preneel, B. Towards Measuring Anonymity. In *Int. Work. Priv. Enhancing Technol.* (2002), Springer, pp. 54–68.

[61] Diffie, W., and Landau, S. Communications surveillance: Privacy and security at risk. *Communications of the ACM 52*, 11 (2009), 42–47.

[62] Ding, Z., Chen, C., Cui, M., Bi, W., Chen, Y., and Li, F. Dynamic game-based defensive primary frequency control system considering intelligent attackers. *Reliability Engineering and System Safety 216*, September (2021), 107966.

[63] Eckhard Pfluegel, Joakim G. Randulff, Charles A. Clarke, Dimitris Tsaptsinos, J. O. Building Secure ICT through Virtual Private Social Networks: A Multi-Channel Mobile Instant Messaging Approach. In *9th CMI Conference on Smart Living, Cyber Security and Privacy* (Copenhagen, nov 2016).

[64] Economy. Access Bank Transfer Code and how to use it.

[65] Electronic Frontier Foundation. The Problem with Mobile Phones | Surveillance Self-Defense, 2015.

[66] Elkhodr, M., Shahrestani, S., and Kourouche, K. A proposal to improve the security of mobile banking applications. In *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on* (Bangkok, 2012), IEEE, pp. 260–265.

[67] Engel, T. SS7: Locate. Track. Manipulate., 2014.

[68] Faniran, A. O., and Odumeru, J. A. Acceptance of Mobile Banking in Nigeria : A Modified TAM Approach. In *Int. Conf. eBusiness, eCommerce, eManagement, eLearning eGovernance 2015 [IC5E 2015]* (2015), vol. 1, pp. 39–49.

[69] Findlay, P., and McKinlay, A. Surveillance, electronic communications technologies and regulation. *Industrial Relations Journal 34*, 4 (2003), 305–318.

[70] First Bank Nigeria. Quick Banking with FirstBank USSD Code *894#, 2021.

[71] Flaherty, A. The price of surveillance: US gov't pays to snoop, 2013.

[72] Franz, Elke and Pfitzmann, A. Steganography Secure against Cover-Stego-Attacks. In *Int. Work. Inf. Hiding* (1999), Springer, pp. 29–46.

[73] Fridrich, J. *Steganography in Digital Media: : Principles, Algorithms, and Applications*, 1 ed. Cambridge University Press, Cambridge, 2009.

[74] Fuchs, C. Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance. *Information Communication and Society 16*, 8 (2013), 1328–1359.

[75] Gedkhaw, E., Soodtoetong, N., and Ketcham, M. The Performance of Cover Image Steganography for Hidden Information within Image File using Least Significant bit algorithm. In *ISCIT 2018 - 18th International Symposium on Communication and Information Technology* (2018), IEEE, pp. 504–508.

[76] Gehrmann, C., Mitchell, C. J., and Nyberg, K. Manual authentication for wireless devices. *RSA Cryptobytes Cryptobytes 7*, 1 (2004), 29–37.

[77] Gligoric, N., Dimcic, T., Drajic, D., Krco, S., and Chu, N. Application-layer security mechanism for M2M communication over SMS. In *2012 20th Telecommun. Forum, TELFOR 2012 - Proc.* (Belgrade, 2012), vol. 7, IEEE, pp. 5–8.

[78] Green, N., and Smith, S. 'A spy in your pocket'? The regulation of mobile data in the UK. *Surveillance and Society 1*, 4 (2003), 573–587.

[79] (GTB), G. T. B. GTBank's 737# Features Mobile Banking Made Easy, 2017.

[80] Gupta, J. A Review on Steganography and Cryptography. In *2015 Int. Conf. Adv. Comput. Eng. Appl.* (2015), vol. 1, pp. 1–4.

[81] Gupta, S., and Jain, R. An innovative method of Text Steganography. In *Proc. 2015 3rd Int. Conf. Image Inf. Process. ICIIP 2015* (Waknaghat, 2016), IEEE, pp. 60–64.

[82] Hamandi, Khodor and Elhajj, Imad H and Chehab, Ali and Kayssi, A. Android SMS Botnet: A New Perspective. In *Proceedings of the 10th ACM international symposium on Mobility management and wireless access* (Paphos, oct 2012), ACM, pp. 125–129.

[83] Hamdan, A. M., and Hamarsheh, A. AH4S: an algorithm of text in text steganography using the structure of omega network. *Secur. Commun. Networks 9*, 18 (2017), 6004–6016.

[84] Hamza, Y. A. Highly secure image steganography approach using arnold's cat map and maximum image entropy. In *ACM International Conference Proceeding Series* (2019), ACM, pp. 134–138.

[85] Hankerson, D. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, 2004.

[86] Hannak, A., Soeller, G., Lazer, D., Mislove, A., and Wilson, C. Measuring price discrimination and steering on E-commerce web sites. In *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC* (2014), pp. 305–318.

[87] Harb, H., Farahat, H., and Ezz, M. SecureSMSPay: Secure SMS mobile payment model. In *2nd International Conference on Anti-counterfeiting, Security and Identification, ASID 2008* (Guiyang, China, 2008), IEEE, pp. 11–17.

[88] Hashemi, M. R., and Soroush, E. A secure m-payment protocol for mobile devices. *Canadian Conference on Electrical and Computer Engineering*, May (2007), 294–297.

[89] Hassan Shirali-Shahreza, M., and Mohammad Shirali-Shahreza. Text Steganography in chat. In *2007 3rd IEEE/IFIP Int. Conf. Cent. Asia Internet* (Tashkent, 2007), IEEE, pp. 1–5.

[90] Hassinen, M. Java based Public Key Infrastructure for SMS Messaging. In *2006 2nd Int. Conf. Inf. Commun. Technol.* (Damascus, 2006), IEEE, pp. 88–93.

[91] Holtmanns, S., and Oliver, I. Sms and one-time-password interception in lte networks. In *Communications (ICC), 2017 IEEE International Conference on* (2017), IEEE, pp. 1–6.

[92] Hopper, N. On Steganographic Chosen Covertext Security. In *International Colloquium on Automata, Languages, and Programming* (2005), vol. 3580, Springer, pp. 311–323.

[93] Hopper, N., von Ahn, L., and Langford, J. Provably secure steganography. *IEEE Transactions on Computers 58*, 5 (2009), 662–676.

[94] Hopper, N. J., Langford, J., and Ahn, L. V. Provably secure steganography. In *Annu. Int. Cryptol. Conf.* (2002), Springer, pp. 77—-92.

[95] Hopper, N. J., Langford, J., and von Ahn, L. Provably Secure Steganography. *IEEE Trans. Comput. 58*, 5 (2009), 662 – 676.

[96] Hosein, G., and Palow, C. W. Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques.

[97] Hua, J., and Sakurai, K. A sms-based mobile botnet using flooding algorithm. In *IFIP Int. Work. Inf. Secur. Theory Pract.* (2011), Springer, pp. 264–279.

[98] Internet Banking. Union bank, 2021.

[99] Ion, I., Beato, F., Capkun, S., Preneel, B., and Langheinrich, M. For some eyes only: Protecting online information sharing. In *CODASPY 2013 - Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy* (2013), pp. 1–12.

[100] Iranmanesh, V., Jing Wei, H., Lee Dao-Ming, S., and Arigbabu, O. A. On using emoticons and lingoes for hiding data in SMS. In *2nd Int. Symp. Technol. Manag. Emerg. Technol. ISTMET 2015 - Proceeding* (2015), IEEE, pp. 103–107.

[101] Isaac, J. T., and Carabobo, U. D. Secure Mobile Payment Systems. *IT Professional 16*, 3 (jun 2014), 36–43.

[102] Jain, A., and Gupta, I. S. A JPEG compression resistant steganography scheme for raster graphics images. In *IEEE Region 10 Annual International Conference, Proceedings/TENCON* (2007), IEEE, pp. 1–4.

[103] James Robinson, William Cole, Jack Maidment, D. P. E. f. M. Privacy campaigners slam secret 'Snooper's Charter' surveillance trial as Home Office teams up with two internet firms to test how to track the browsing history of every person in the country, 2021.

[104] Jamil, M. S., and Mousumi, F. A. Short messaging service (SMS) based m-banking system in context of Bangladesh. In *Proceedings of 11th International Conference on Computer and Information Technology, ICCIT 2008* (Khulna, dec 2008), IEEE, pp. 599–604.

[105] Jenna McLaughlin. South African Spy Company Used by Gadaffi Touts its NSA-Like Capabilities, oct 2016.

[106] Joseph, P., and Vishnukumar, S. A study on steganographic techniques. In *Glob. Conf. Commun. Technol. GCCT 2015* (2015), no. Gcct, pp. 206–210.

[107] Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I., and Manifavas, C. Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAs. In *Proceedings - 22nd International Conference on Field Programmable Logic and Applications, FPL 2012* (Oslo, aug 2012), IEEE, pp. 747–753.

[108] Katz, J. Bridging Game Theory and Cryptography: Recent Results and Future Directions. In *Proceeding Theory Cryptogr. Conf. (TCC)* (2008), vol. 4948, Springer Berlin Heidelberg, pp. 251–272.

[109] Katzenbeisser, S., and Petitcolas, F. A. P. Defining security in steganographic systems. In *Proc. SPIE 4675, Secur. Watermarking Multimed. Contents IV, 50* (2002), vol. 4675, International Society for Optics and Photonics, pp. 50–56.

[110] Khiabani, Y. S., Wei, S., Yuan, J., and Wang, J. Enhancement of secrecy of block ciphered systems by deliberate noise. *IEEE Transactions on Information Forensics and Security 7*, 5 (2012), 1604–1613.

[111] Khozooyi, N., Tahajod, M., and Khozooyi, P. Security in mobile governmental transactions. In *2009 International Conference on Computer and Electrical Engineering, ICCEE 2009* (2009), vol. 2, IEEE, pp. 168–172.

[112] Kim, C. H. Improved differential fault analysis on AES key schedule. *IEEE Transactions on Information Forensics and Security 7*, 1 (2012), 41–50.

[113] Kim, E. K., McDaniel, P., and La Porta, T. A detection mechanism for SMS flooding attacks in cellular networks. In *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.* (2013), Springer, pp. 76–93.

[114] Kisore, N. R., and Sagi, S. A secure SMS protocol for implementing digital cash system. In *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015* (2015), pp. 1883–1892.

[115] Kohls, K. S., and Poepper, C. POSTER: Traffic Analysis Attacks in Anonymity Networks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (Abu Dhabi, apr 2017), ACM, pp. 917–919.

[116] Krishna, G. M. Design and implementation of Short Message Service (SMS) based blood bank. In *Inventive Computation Technologies (ICICT), International Conference on* (Coimbatore, aug 2016), IEEE, pp. 2–5.

[117] Kumar, M., and Singh, G. Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach. *International Journal of Computer Applications 171*, 8 (2017), 12–15.

[118] Kumar, S. S., and Sylish, S. V. Image steganography in high entropy regions using a key & modified LSB for improved security. In *Proceedings of the International Conference on Computing Methodologies and Communication, ICCMC 2017* (2018), vol. 2018-Janua, IEEE, pp. 1104–1108.

[119] Kungpisdan, S., Srinivasan, B. and Le, P. A Secure Account-Based Mobile Payment Protocol. In *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on* (2004), IEEE, pp. 35–39.

[120] Laber, J., Troubh, J., Redel, V., Oakes, J., Lipman, E., Baldwin, J., Frost, R., Ginsberg, A., Hughes, L., Miller, A., O'neill, E., Sontag, S., and Steinbeck, J. Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. Tech. Rep. 212, PEN American Center, New York, 2013.

[121] Lam, Kwok-Yan and Gollmann, D. Freshness assurance of authentication protocols. In *ESORICS* (1992), vol. 92, Springer, pp. 261—-272.

[122] Lee, M. Y., Iranmanesh, V., and Quiroz, J. C. A New Approach to SMS Steganography using Mathematical Equations. In *International Conference on Computer Applications and Technology, ICCAT 2015* (2016), pp. 1–6.

[123] Lee, Huei, Yu Zhang, K. L. C. An Investigation of Initial Trust in Mobile Banking. *Int. J. Acad. Res. Bus. Soc. Sci. 3*, 9 (2013), 22–46.

[124] Level, T., and Bamford, B. J. The NSA Is Building the Country' s Biggest Spy Center (Watch What You Say). *Wired*, Avril (2012), 1–15.

[125] Li, M., Koutsopoulos, I., and Poovendran, R. Optimal jamming attack strategies and network defense policies in wireless sensor networks. *IEEE Transactions on Mobile Computing 9*, 8 (2010), 1119–1133.

[126] Li, P., Liu, Y., Xin, H., and Jiang, X. A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant under Cyber-Attacks. *IEEE Transactions on Industrial Informatics 14*, 10 (2018), 4343–4352.

[127] Li, Tai-ching; Hang, Huy; Faloutsos, Michalis; Efstathopoulos, P. TrackAdvisor: Taking back browsing privacy from Third-Party Trackers. In *International Conference on Passive and Active Network Measurement* (2015), Springer, pp. 1–12.

[128] Liang, X., and Xiao, Y. Game theory for network security. *IEEE Communications Surveys and Tutorials 15*, 1 (2013), 472–486.

[129] Lisoněk, D., and Drahanský, M. SMS Encryption for mobile communication. In *Proc. - 2008 Int. Conf. Secur. Technol. SecTech 2008* (Hainan Island, 2008), IEEE, pp. 198–201.

[130] Liu, F., Gao, H., and Wei, Z. Research on the game of network security attack-defense confrontation through the optimal defense strategy. *Security and Privacy 4*, 1 (2021), 1–9.

[131] Liyun Li, Husrev Taha Sencar, N. M. A cost-effective decision tree based approach to steganalysis. In *Media Watermarking, Secur. Forensics 2013* (2013), vol. 8665, spiedigitallibrary, p. 86650P.

[132] Lucas, M., and Borisov, N. FlyByNight: Mitigating the Privacy Risks of Social Networking. In *Proceedings of the Seventh ACM Workshop on Privacy in the Electronic Society* (2008), ACM, pp. 1–8.

[133] Madsen, W. FBI's communications surveillance capabilities widen. *Computer Fraud & Security 2000*, 10 (2000), 16–17.

[134] Maghrabi, L., and Pfluegel, E. Moving assets to the cloud: A game theoretic approach based on trust. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015* (2015), IEEE, pp. 1–5.

[135] Malone, D., and Sullivan, W. Guesswork is not a substitute for Entropy. In *Proceedings of the Information Technology and Telecommunications Conference* (2005).

[136] Manshaei, Mohammad Hossein and Zhu, Quanyan and Alpcan, Tansu and Basar, Tamer and Hubaux, J.-P. Game Theory Meets Network Security and Privacy. *ACM Comput. Surv. 45*, 3 (2013), 1–45.

[137] Massey, J. L. Guessing and Entropy. In *IEEE International Symposium on Information Theory* (1994), IEEE.

[138] Mathkour, H., Al-Sadoon, B., and Touir, A. A New Image Steganography Technique. In *Wirel. Commun. Netw. Mob. Comput. 2008. WiCOM'08. 4th Int. Conf.* (Dalian, 2008), IEEE, pp. 1–4.

[139] Mayer, J. R., and Mitchell, J. C. Third-party web tracking: Policy and technology. In *Proceedings - IEEE Symposium on Security and Privacy* (2012), IEEE, pp. 413–427.

[140] Me, G., Strangio, M. A., and Schuster, A. Mobile local macropayments: Security and prototyping. *IEEE Pervasive Computing 5*, 4 (2006), 94–100.

[141] Memon, N. A Unified Steganalysis Framework for office Scientific Research. Tech. Rep. April, Polytechnic University of NYU, Brooklyn, NY, 2013.

[142] Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. *Handbook of applied cryptography*. CRC Press-Taylor and Francis, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL, 1997.

[143] Mikians, J., Gyarmati, L., Erramilli, V., and Laoutaris, N. Detecting price and search discrimination on the Internet. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks, HotNets-11* (2012), no. July, pp. 79–84.

[144] Mikians, J., Gyarmati, L., Erramilli, V., and Laoutaris, N. Crowd-assisted search for price discrimination in E-commerce: First results. In *CoNEXT 2013 - Proceedings of the 2013 ACM International Conference on Emerging Networking Experiments and Technologies* (2013), pp. 1–6.

[145] Mittelholzer, T. *An information-theoretic approach to steganography and watermarking*. Springer, 1999.

[146] Murdoch, J. Security Measurement. Tech. Rep. November, Computer Science Department, University of York, YORK YO10 5DD UK, 2006.

[147] Murynets, I., and Piqueras Jover, R. Crime scene investigation. In *Proceedings of the 2012 ACM conference on Internet measurement conference - IMC* (Boston, nov 2012), ACM, pp. 441–452.

[148] Nagarhalli, T. P. A New Approach to SMS Text Steganography Using Emoticons. *Int. J. Comput. Appl. (0975 – 8887) 975* (2014), 0975–8887.

[149] Needham, R. M., and Schroeder, M. D. Using encryption for authentication in large networks of computers. *Communications of the ACM 21*, 12 (1978), 993–999.

[150] Nehra, A., Meena, R., Sohu, D., and Rishi, O. P. A Robust Approach to Prevent Software Piracy. In *Engineering and Systems (SCES), 2012 Students Conference on* (Allahabad, Uttar Pradesh, mar 2012), IEEE, pp. 16–18.

[151] New York Times. 4 cellphone carriers may face $200M in fines for selling location data | Honolulu Star-Advertiser, feb 2020.

[152] Newman, L. H. 5G Is Here—and Still Vulnerable to Stingray Surveillance | WIRED, 2019.

[153] Nichal, A. Steganography for JPEG2000 Baseline System. Tech. Rep. January 2013, 2017.

[154] Nissar, A., and Mir, A. H. Classification of steganalysis techniques: A study. *Digit. Signal Process. A Rev. J. 20*, 6 (2010), 1758–1770.

[155] Odumeru, J. A. Going Cashless : Adoption of Mobile Banking in Nigeria. *Arab. J. Bus. Manag. Rev. 1*, 2 (2013), 9–17.

[156] Osborne, M. J., and Rubinstein, A. *A Course in Game Theory.*, first edit ed. MIT press, 1994.

[157] Otway, D., and Rees, O. Efficient and timely mutual authentication. *ACM SIGOPS Operating Systems Review 21*, 1 (1987), 8–10.

[158] Oyindamola Olofinlua. How mobile internet killed off Nigeria's cyber cafes, 2015.

[159] Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., and Smeraldi, F. Cybersecurity Games and Investments: A Decision Support Approach. In *Int. Conf. Decis. Game Theory Secur.* (2014), Springer, Cham, pp. 266–286.

[160] Park, K., Ma, G. I., Yi, J. H., Cho, Y., Cho, S., and Park, S. Smartphone remote lock and wipe system with integrity checking of SMS notification. In *Digest of Technical Papers - IEEE International Conference on Consumer Electronics* (Las Vegas, NV, jan 2011), IEEE, pp. 263–264.

[161] Paul Masurel. Of generating random text using a Markov model, 2013.

[162] Pawar, P. Y., and Gawande, S. H. M-Commerce Security Using Random LSB Steganography and Cryptography. *Int. J. Mach. Learn. Comput. 2*, 4 (2013), 427–430.

[163] Pell, Stephanie K and Soghoian, C. Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy. *Harv. JL & Tech 28*, 1 (2014), 2014.

[164] Pereira, G. C., Santos, M. A., De Oliveira, B. T., Simplicio, M. A., Barreto, P. S., Margi, C. B., and Ruggiero, W. V. SMSCrypto: A lightweight cryptographic framework for secure SMS transmission. *J. Syst. Softw. 86*, 3 (2013), 698–706.

[165] Perlroth, N. How Spy Tech Firms Let Governments See Everything on a Smartphone. *New York Times, September 2*, A1 (2016), 2–5.

[166] Peter Wayner. *Disappearing cryptography: information hiding: steganography and watermarking.*, 3rd ed ed. Morgan Kaufmann Publishers, Amsterdam, 2009.

[167] Petrovic, S., and Fuster-Sabater, A. Cryptanalysis of the a5/2 Algorithm. In *IACR Cryptology ePrint Archive* (2000), pp. 1–7.

[168] Petrowski, K., Kharrazi, M., Sencar, H. T., and Memon, N. PSteg: Steganographic embedding through patching. In *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.* (2005), vol. 2, IEEE, pp. ii—-537.

[169] Pfitzmann, A., and Köhntopp, M. Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology BT - UbiComp 2002: Ubiquitous Computing. *UbiComp 2002 Ubiquitous Comput. 2009*, Chapter 1 (2001), 1–9.

[170] Pfluegel, Eckhard and Clarke, Charles and Randulff, Joakim and Tsaptsinos, Dimitris and Orwell, J. A secure channel using social messaging for distributed low-entropy steganography. In *Cybersecurity and Privacy - Bridging the Gap*, K. E. Khajuria, Samant , Sørensen, Lene and Skouby, Ed. River Publishers Series in Communications, 2017.

[171] Pibre, L., Jérôme, P., Ienco, D., and Chaumont, M. Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source-mismatch. *Electron. Imaging 2016*, 8 (2016), 1–11.

[172] Pliam, J. O. Guesswork and Variation Distance as Measures of Cipher Security. In *International Workshop on Selected Areas in Cryptography* (1999), Springer, pp. 62–77.

[173] Pottathil, A., and Ornatowski, C. Digital Communications Surveillance : a challenge for Rhetoric Studies. *African Yearbook of Rhetoric 3*, 1 (2012), 13–22.

[174] Prevelakis, V., and Spinellis, D. The Athens affair. *IEEE Spectrum 44*, 7 (2007), 26–33.

[175] Qian, Yinlong and Dong, Jing and Wang, Wei and Tan, T. Deep learning for steganalysis via convolutional neural networks. In *Media Watermarking, Secur. Forensics 2015* (San Francisco, California, 2015), vol. 9409, spiedigitallibrary, p. 94090J.

[176] Qiang Guo ; Dawei Sun ; Guiran Chang ; Lina Sun ; Xingwei Wang. Modeling and Evaluation of Trust in Cloud Computing Environments. In *2011 3rd International Conference on Advanced Computer Control (ICACC 2011)* (Harbin, China, 2011), no. Icacc, IEEE, pp. 112–116.

[177] Qiao, X., Ji, G., and Zheng, H. A New Method of Steganalysis Based on Image Entropy. In *Advanced Intelligent Computing Theories and Applications. With Aspects of Contemporary Intelligent Computing Techniques* (2007), pp. 810–815.

[178] Rafat, K. F. Enhanced text steganography in SMS. In *2009 2nd Int. Conf. Comput. Control Commun. IC4 2009* (Karachi, 2009), IEEE, pp. 1–6.

[179] Rainer Böhme. *Advanced Statistical Steganalysis*. Springer Science & Business Media, 2010.

[180] Rajyaguru, M. H. CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys. *Int. J. Emerg. Technol. Adv. Eng. 2*, 10 (2012), 329–332.

[181] Ramachandran, K., and Stefanova, Z. Dynamic Game Theories in Cyber Security. In *Proceedings of Dynamic Systems and Applications (2016)* (sep 2016), vol. 7, Dynamic Publishers, Inc.

[182] Rao, S. P., Holtmanns, S., Oliver, I., and Aura, T. Unblocking stolen mobile devices using SS7-MAP vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access. In *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015* (2015), vol. 1, pp. 1171–1176.

[183] Raphael, A. J., and Sundaram, V. Cryptography and steganography – A survey. *Int. J. Comput. Technol. Appl. 2*, 3 (2011), 626–630.

[184] Rathi, S., and Wang, Z. Fast EBCOT encoder architecture for JPEG 2000. In *IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation* (2007), IEEE, pp. 595–599.

[185] Raymond, J.-F. Traffic analysis: Protocols, attacks, design issues, and open problems. In *Designing Privacy Enhancing Technologies* (2001), vol. 2009, Springer, pp. 10—-29.

[186] Regan, L. Electronic communications surveillance. *Monthly Review 66*, 3 (2014), 32–42.

[187] Rico-Larmer, S. M. Cover Text Steganography: N-gram and Entropy- based Approach. In *2016 KSU Conf. Cybersecurity Educ. Res. Pract.* (2016), pp. 1–8.

[188] Roesner, F., Kohno, T., and Wetherall, D. Detecting and defending against third-party tracking on the web. In *Proceedings of NSDI 2012: 9th USENIX Symposium on Networked Systems Design and Implementation* (2012), no. Nsdi, pp. 155–168.

[189] Roque, J. J., and Minguet, J. M. SLSB: Improving the Steganographic Algorithm LSB. In *Proc. 7th Int. Work. Secur. Inf. Syst.* (2009), IEEE, pp. 57–66.

[190] Ryan Gallagher. How Governments and Telecom Companies Work Together on Surveillance Laws, 2012.

[191] Sakib, M. N., Sazzad, a. R., Alam, S. B., Shahnaz, C., and Fattah, S. A. Security Enhancement Protocol in SMS-Banking using Digital Watermarking Technique. In *2010 Fourth UKSim European Symposium on Computer Modeling and Simulation* (Pisa, Italy, nov 2010), IEEE, pp. 170–173.

[192] Sanders, Gillian D and Maciejewski, Matthew L and Basu, A. Overview of Cost-Effectiveness Analysis. *JAMA - Journal of the American Medical Association 321*, 14 (2019), 1400—-1401.

[193] Satyanarayanan, M. Integrating security in a large distributed system. *ACM Transactions on Computer Systems 7*, 3 (1989), 247–280.

[194] Saxena, A., Das, M. L., and Gupta, A. MMPS: A versatile mobile-to-mobile payment system. In *4th Annu. Int. Conf. Mob. Business, ICMB 2005* (2005), no. 1, IEEE, pp. 400–405.

[195] Saxena, N., and Chaudhari, N. S. A secure approach for SMS in GSM network. In *Proc. CUBE Int. Inf. Technol. Conf.* (Pune, 2012), ACM, p. 59.

[196] Saxena, N., and Chaudhari, N. S. EasySMS: A protocol for end-to-end secure transmission of SMS. *IEEE Transactions on Information Forensics and Security 9*, 7 (2014), 1157–1168.

[197] Saxena, N., Shen, H., Komninos, N., Choo, K. K. R., and Chaudhari, N. S. BVPSMS: A Batch Verification Protocol for End-to-End Secure SMS for Mobile Users. *IEEE Trans. Dependable Secur. Comput.*, 99 (2018).

[198] Saxena, Neetesh and Chaudhari, N. S. A Secure Digital Signature Approach for SMS Security. *Int. J. Comput. Appl. 4*, 1 (2011), 98–102.

[199] Schlenker, A., Thakoor, O., Xu, H., Tran-Thanh, L., Fang, F., Vayanos, P., Tambe, M., and Vorobeychik, Y. Deceiving cyber adversaries: A game theoretic approach. In *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS* (2018), vol. 2, pp. 892–900.

[200] Serjantov, A., and Danezis, G. Towards an Information Theoretic Metric for Anonymity. In *Int. Work. Priv. Enhancing Technol.* (2002), Springer, pp. 41–53.

[201] Shahreza, M. S. M-quiz by sms. In *Sixth IEEE International Conference on Advanced Learning Technologies (ICALT'06)* (2006), IEEE, pp. 726–729.

[202] Shahreza, S. Stealth steganography in SMS. In *2006 IFIP Int. Conf. Wirel. Opt. Commun. Networks* (Bangalore, 2006), IEEE, pp. 5 pp.–5.

[203] Shamir, A. How to share a secret. *Commun. ACM 11*, 22 (1979), 612—-613.

[204] Shannon, C. E., and Weaver, W. The mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review 5*, 1 (2001), 3–55.

[205] Sharma, P., and Corresponding, B. Issues & Challenges i n Mobile Banking In India : A Customers ' Perspective. *Research Journal of Finance and Accounting 2*, 2 (2011), 112–120.

[206] Shih, F. Y. *Digital Watermarking and Steganography*, 1 ed. CRC Press-Taylor and Francis, Boca Raton, Fl, 2007.

[207] Shirali-Shahreza, M. Improving mobile banking security using steganography. In *Proceedings - International Conference on Information Technology-New Generations, ITNG 2007* (Las Vegas, NV, USA, 2007), IEEE, pp. 885–887.

[208] Shirali-Shahreza, M., and Shirali-Shahreza, M. H. Text steganography in SMS. In *2007 Int. Conf. Converg. Inf. Technol. ICCIT 2007* (Gyeongju, 2007), IEEE, pp. 2260–2265.

[209] Shirali-Shahreza, M. H., and Shirali-Shahreza, M. Steganography in SMS by sudoku puzzle. In *AICCSA 08 - 6th IEEE/ACS Int. Conf. Comput. Syst. Appl.* (2008), IEEE, pp. 844–847.

[210] Shondeep, L., Energy, C., Energy, C., and Cited, R. Secure communication method and apparatus, 1995.

[211] Solanki, K., Sarkar, A., and Manjunath, B. S. YASS: Yet another steganographic scheme that resists blind steganalysis. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 4567 LNCS*, May 2014 (2007), 16–31.

[212] Song, X., Jiang, W., Liu, X., Lu, H., Tian, Z., and Du, X. A Survey of Game Theory as Applied to Social Networks. *Tsinghua Science and Technology 25*, 6 (2020), 734–742.

[213] Soni, P. M-payment between banks using SMS. In *Proceedings of the IEEE* (Kherva, Gujarat, 2010), vol. 98, IEEE, pp. 903–905.

[214] Soram, R. Mobile SMS Banking Security Using Elliptic Curve Cryptosystem. *International Journal of Computer Science and Network Security 9*, 6 (2009), 30–38.

[215] Stallings, W. *Cryptography and network security principles and practice*, 7 ed. Pearson, 2017.

[216] Stanbic IBTC Bank. USSD Banking - *909#, 2021.

[217] Standard, I., and Activities, I. S. *8802-11, Second edition: 2005/Amendment 6 2006: IEEE STD 802.11i-2004 - ISO/IEC International Standard - Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11:*, vol. 2006. 2006.

[218] Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, N. L., and Safi, M. Revealed: leak uncovers global abuse of cyber-surveillance weapon, 2021.

[219] Stevens, M., Bursztein, E., Karpman, P., Albertini, A., and Markov, Y. The first collision for full SHA-1. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2017), vol. 10401 LNCS, pp. 570–596.

[220] Stinson, D. R. *Cryptography: theory and practice*, third edit ed. CRC Press-Taylor & Francis, 2005.

[221] Stuti Goel, S. G. A Review of Comparison Techniques of Image Steganography. *IOSR Journal of Electrical and Electronics Engineering 6*, 1 (2013), 41–48.

[222] Su, P. C., and Kuo, C. C. Steganography in JPEG2000 compressed images. *IEEE Transactions on Consumer Electronics 49*, 4 (2003), 824–832.

[223] Taleby Ahvanooey, M., Li, Q., Hou, J., Dana Mazraeh, H., and Zhang, J. AITSteg: An innovative text steganography technique for hidden transmission of text message via social media. *IEEE Access 6* (2018), 65981–65995.

[224] Thomas, M., and Panchami, V. An encryption protocol for end-to-end secure transmission of SMS. In *IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2015* (2015), IEEE, pp. 1–6.

[225] Tiwari, R., and Buse, S. The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Secotr. Tech. rep., 2007.

[226] Tom, L. Game-theoretic approach towards network security: A review. In *IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2015* (2015), IEEE, pp. 1–4.

[227] Toorani, M., and Shirazi, A. A. B. SSMS - A secure SMS messaging protocol for the m-payment systems. In *Proceedings - IEEE Symposium on Computers and Communications* (Tehran, Iran, 2008), IEEE, pp. 700–705.

[228] Traynor, P., Enck, W., McDaniel, P., and La Porta, T. Mitigating attacks on open functionality in SMS-capable cellular networks. *IEEE/ACM Transactions on Networking 17*, 1 (feb 2009), 40–53.

[229] Tu, G.-H., Li, C.-Y., Peng, C., Li, Y., and Lu, S. New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks. In *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16* (Vienna, 2016), ACM, pp. 1118–1130.

[230] Uba internet Banking. *919# Funds Transfer.

[231] Valentino-DeVries, J. FBI's 'Stingray' Cellphone Tracker Stirs a Fight Over Search Warrants, Fourth Amendment - WSJ, 2011.

[232] Valor, A. L., Apsay, M. R. B., Acebo, J. R. M., Aguilar, A., Onquit, C. J. B., and Chua, M. G. Heartsaver: A heart rate monitoring system with sms notification. In *Systems, Process and Control (ICSPC), 2016 IEEE Conference on* (dec 2016), IEEE, pp. 1–6.

[233] Wang, D., Zhang, X., Ming, J., Chen, T., Wang, C., and Niu, W. Resetting Your Password Is Vulnerable: A Security Study of Common SMS-Based Authentication in IoT Device. *Wirel. Commun. Mob. Comput. 2018* (2018), 1–16.

[234] Wang, Huaiqing and Wang, S. Cyber Warfare: Steganography vs. Steganalysis. *Commun. ACM 47*, 10 (2004), 76–82.

[235] Wang, Xiaoyun and Yin, Yiqun Lisa and Yu, H. Finding collisions in the full SHA-1. In *Annual international cryptology conference* (2005), Springer Berlin Heidelberg, pp. 17–36.

[236] Wei, H., Chunhe, X., Haiquan, W., Cheng, Z., and Yi, J. A game theoretical attack-defense model oriented to network security risk assessment. In *Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008* (2008), vol. 3, pp. 498–504.

[237] West, M. *Preventing System Intrusions*, second edition ed. Elsevier Inc., 2013.

[238] Westfeld, A. F5 — A Steganographic Algorithm High Capacity Despite Better Steganalysis. In *4th International Workshop in Information Hiding* (2001), Springer-Verlag, pp. 289–302.

[239] Westfeld, A., and Pfitzmann, A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned. In *International Workshop on Information Hiding* (1999), Springer, pp. 1–16.

[240] WikiLeaks. Spy Files, 2017.

[241] Wong, K. C. A preliminary assessment of the Hong Kong interception of communications and surveillance ordinance. *Commonwealth Law Bulletin 34*, 3 (2008), 607–621.

[242] Woodhams, S. Spyware: An Unregulated and Escalating Threat to Independent Media. Tech. Rep. August, 2021.

[243] Wright, C. V., Coull, S. E., Monrose, F., and Hill, C. Traffic Morphing : An Efficient Defense Against Statistical Traffic Analysis. In *Proceedings of the 16th Network and Distributed Security Symposium* (2009), vol. 9, pp. 375–382.

[244] Wu, M., Zhu, Z., and Jin, S. Detection of hiding in the LSB of DCT coefficients. *Lecture Notes in Computer Science 3644*, PART I (2005), 291–300.

[245] Yu, H.-C., Hsi, K.-H., and Kuo, P.-J. Electronic payment systems: an analysis and comparison of types. *Technology in Society 24*, 3 (aug 2002), 331–347.

[246] Yun Q., S., Chen, C., and Chen Wen. A Markow process based approach for effectively attacking JPEG stegnography. In *Int. Work. Inf. Hiding* (2006), Springer, pp. 249–264.

[247] Zeng, Y., Shin, K., and Hu, X. Design of SMS commanded-and-controlled and P2P-structured mobile botnets. In *WISEC '12 Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks* (Tucson, Arizona, apr 2012), no. February, ACM, pp. 137–148.

[248] Zhu, Q., and Rass, S. Game theory meets network security a tutorial. In *Proceedings of the ACM Conference on Computer and Communications Security* (2018), pp. 2163–2165.

[249] Zirikovic., Z. secretwit - twitter client that hides messages in tweets, 2011.

[250] Zöllner, Jan and Federrath, Hannes and Klimant, Herbert and Pfitzmann, Andreas and Piotraschke, Rudi and Westfeld, Andreas and Wicke, Guntram and Wolf, G. Modelling the security of steganographic Systems. In *Int. Work. Inf. Hiding* (1998), Springer-Verlag Berlin Heidelberg, pp. 344—-354.