KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY,

KUMASI, GHANA

ENHANCING DATA SECURITY USING VIDEO STEGANOGRAPHY, RSA AND HUFFMAN CODE ALGORITHMS WITH LSB INSERTION

by

Richard Apau (BSc. Computer Science)

A Thesis submitted to the Department of Computer Science,

College of Science

in partial fulfilment of the requirements for the degree of

MASTER OF PHILOSOPHY (COMPUTER SCIENCE)

September, 2016

DECLARATION

I hereby declare that this submission is my own work towards the MPhil degree and that , to the best of my knowledge, it contains no material previously published by another person, nor material which has been accepted for the award of any other degree of the University, except where due acknowledgement has been made in the text.

Richard Apau (PG 2573214)	……	……..
Student Name & ID	Signature	Date

Certified by:

Dr. J. B. Hayfron-Acquah	……	……
Supervisor Name	Signature	Date

Certified by:

Dr. J. B. Hayfron-Acquah	……	……
Head of Department Name	Signature	Date

ABSTRACT

Security (i.e. Confidentiality, Integrity, Authentication, Non-Repudiation, and Availability) in the field of data communication have remained a subject matter of discussion over the years. The internet as well as computer technology have made significant strive in data communication existence. Transferring data securely and safely amidst vulnerabilities of computer networks remain a source of worry to many in the field of data communication. Without security there is no need for data communication. The main objective of this study was to ensure security of data transmitted over the internet. The study proposed a novel approach of data security using video steganography, Huffman Code compression and asymmetric cryptography. In the proposed system, messages are encrypted with RSA and encrypted messages are compressed using Huffman code algorithm. The compressed encrypted messages are hidden using Least Significant Bit (LSB) algorithms. This research brings to light the concept of effectively combining steganography, compression and asymmetric cryptographic algorithm. The preference of RSA over any other cryptographic algorithm is due to its ability to provide better security for large file size thereby reducing computational complexity. The use LSB for video embedding is also good for larger file sizes due to its low computational complexity. Huffman code compression is a lossless compression algorithm which allows reduction in size of data without loss of data. From the results obtained in this research, it was observed that when video steganography is combined with Huffman code compression and asymmetric cryptography, a higher level of security, robustness and capacity are achieved. The

distortion experienced in this study is negligible; therefore the study achieved increased security by the high PSNR values and low

MSE and BER values

Table of Contents

LIST OF TABLES

LIST OF FIGURES

DEDICATION

This study is dedicated first and foremost to the Almighty God for whose strength, goodness and mercies that this thesis was completed successfully. Secondly, the entire work is dedicated to Miss Catherine Frema Bamfo, whose motherly love, care, guidance and advice saw the timely completion of this thesis.

ACKNOWLEDGEMENTS

My foremost appreciation goes to the Almighty God, the creator of Heaven and Earth for the knowledge bestowed upon me and the grace to finish this this work. I am thankful to my supervisor Dr. J. B. Hayfron-Acquah for his guidance, contributions, encouragement and fatherly love shown me throughout this research.

Special Appreciation goes to Miss Mercy Serwaa for her tremendous and caring love Miss Catherine Frema Bamfo for her motherly love and her support in diverse ways.

I am forever grateful to my beloved cousin, Mr Benjamin Simpri Yaw Amoako, whose toils, love and mentorship have brought me this far. I am also indebted to Miss Victoria Asiedua my elder sister who has also contributed immensely towards my success and to all my siblings for their support in diverse ways. May God bless them all.

Again, thankful to Mr Emmanuel Ofori Oppong, Lecturer, KNUST for his guidance and advice throughout the start of the programme, my beloved and dear friend Miss Henrietta Obaabeng Dompreh, for her advice and encouragement throughtout the start of the programme.

Finally, I am appreciative of Kofi Asamoah Boadu who assisted me in my programming and codes when I had challenges.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

A good research requires a proper elaboration of the subject matter under investigation or study. This chapter has an essential and paramount role of meeting such aims and objectives. This chapter begins by elaborating on the background of the study, and then discusses the statement of the problem under investigation; this is followed by the purpose of the study. The justification underpinning the investigation is also considered after the purpose in this chapter. This is immediately followed by the main and specific objectives behind the research, the research questions are therefore outlined, followed by the scope of the study. Finally, the chapter ends by discussing the organisation of the entire research.

1.1 Background of the study

The privacy and security in the field of data communication have remained a subject matter of discussion over the years. The internet as well as computer technology have made significant strive in data communication existence (Ramalingam, 2011). This breakthrough that has existed in data communication has paved a new way for the implementation of steganography in order to ensure that, data is transferred securely. Transferring data securely and safely amidst vulnerabilities of computer networks remain a source of worry to many in the field of data communication. Whereas some have opted for steganography, others prefer cryptography as a way of securing data that is transmitted over the computer networks. According to Wajgade and Kumar (2013),

the effect of combining steganography and cryptography is more beneficial in terms of obtaining the security and privacy of data. Various approaches and techniques of data security and information have been implemented by researchers to achieve secret communication.

In today's digital world, steganography is one of the most safest forms of data communication (Dengre et al , 2013**).** Prabakaran and Bhavani (2012), defines steganography as "the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message". This basically involves the use of appropriate multimedia carriers such as image, audio and video files in communicating the secret data. Steganography can be grouped into five main types (Dengre et al, 2013). This grouping is primarily based on the nature of cover object used. In modern approach, image stenography, audio steganography, protocol steganography, video steganography and watermarking have widely been used. Video steganography, which is generally the collection of images and sounds, is the most preferred type. This preference is comparatively so because, large amount of data can be hidden inside a video. Distortion in the video is mostly unobserved by humans due to the moving stream of sounds and images. Due to the techniques of steganalysis tools, that have the capacity of detecting hidden messages in covert media (Budhia et al., 2006), cryptography has been employed as another means of securing data transmission.

Cryptography until recent times was referred to be encryption. Though the two words have been used interchangeably in the past, they are not the same. Cryptography can simply be defined as the process of data storing and transmitting in a particular way such that, those whom the message is intended for can read and process it. Many until modern times believed that steganography is an alternative to cryptography. According

to Ramalingam (2011), steganography is rather the dark cousin of cryptography and not an alternate. Whereas steganography provides secrecy cryptography is intended to provide privacy. The very essence of steganography is to hide or mask the existence of the message while cryptography concerns itself with the masking of the content of a message. The seemly exploitation of steganalysis which detect the presence of hidden message in covert media (Das et al., 2011), made the combined effect of steganography and cryptography crucial. There are many areas of study in the field of cryptography. The chief among them are symmetric key cryptography, asymmetric key cryptography, cryptanalysis and cryptosystems. Primarily, cryptography is divided into two main types. The two known types are; symmetric key cryptography popularly referred to as secret key cryptography and asymmetric key cryptography also known as public key cryptography. Kessler (2015) contend that, cryptography can be classified into three types based on the number of keys used. The three classifications according to the keys are: private key which uses only one key for encrypting and decrypting, public key which uses two keys, one for encrypting and another for decrypting, and hash functions that irreversibly encrypts information using mathematical transformation. Dengre et. al. (2013) revealed that, cryptography employs the techniques of encryption. Encryption is the method of encoding messages to ensure that only authorised persons can have access and read.

Examples of encryption algorithms in symmetric key cryptography are DES, AES and Triple DES. In this algorithm, only one private key is used for the encrypting and the decrypting of the message by both the sender and receiver. The vulnerabilities and the weaknesses associated with the symmetric key cryptography necessitated the development of public-key cryptography called asymmetric cryptographic algorithm in 1976 by Whitfield Diffie and Martin Hellman.

Asymmetric cryptographic algorithm was developed to add more security features to the symmetric key cryptography. It must however be indicated that, it is not a replacement to secret-key cryptography. Asymmetric cryptographic algorithm can be described as the most revolutionary new concept in the field of cryptography. The asymmetric cryptography has the comparative advantage of increased security and convenience. The provision of digital signature as a method for authentication is another major advantage in asymmetric cryptography. The encryption algorithms such as; Diffie-Hellman, RSA, Cramer-Shoup cryptosystem, ElGamal encryption and Elliptic Curve Cryptosystem (ECC) are used in asymmetric cryptographic algorithm (Wander et al., 2005). Somani et al. (2010) opined that, implementation of digital signature with RSA algorithm ensures data security. Hence, the use of RSA algorithm is very critical in helping to increase security and privacy of data.

Against this backdrop, it has become important therefore to design a system that has the capacity and the capability of ensuring the security and privacy of data. Although a number of studies have been done on video steganography, many focused on the use of symmetric cryptographic algorithm. Few others also used asymmetric cryptographic algorithm, those done in the area of asymmetric cryptographic algorithm places little or no emphasis on the use of RSA encryption, compression algorithms and LSB insertion. This study is therefore designed to enhance video steganography using RSA encryption algorithm and Huffman code compression with LSB insertion.

1.2 Statement of the problem

The high increased in internet penetration has led to many computer related crimes. Privacy and secrecy of data still remain a major challenge in today's technological world. Though stringent measures have been put in place to ensure the security and privacy of data transmitted over the computer networks, hackers and eavesdroppers also continue to device a more sophisticated and complex way of accessing such information. Steganography which was introduced to conceal the existence of message from hackers and attackers has also been exposed to attacks. Steganalysis has been identified as one major tool that is used by eavesdroppers and hackers to detect and extract hidden information in a covert media. Whereas passive steganalysis is design to detect and identify the algorithm used, active steganalysis has the capacity to detect and extract the hidden message depending on the strength of the algorithm used.

To this end, cryptography was introduced to make data communication more secure and safer. Most systems that have been designed to enhance steganography are based on symmetric-key or private-key cryptography. However, the vulnerabilities associated with the private key cryptography have also been exploited significantly by attackers and hackers. In symmetric key cryptography, a private key is transmitted either manually or through a communication channel. This key can be intercepted by an enemy in the transmission process. Authentication in secret-key cryptography is still a challenge. This normally requires sharing of some secret information or third party. These weaknesses if not address would go a long way to affect the integrity of data transmitted over the computer networks or internet. Therefore, the problem this research seeks to address is how a system using RSA and Huffman algorithm with LSB can be designed to solve the vulnerabilities identified in the existing systems.

1.3 Justification of the study

Stenographic programs are there in abundance. A few of such programs are splendid in every respect. Unfortunately, majority of the existing programs lack usable interfaces or has many bugs or lacks the ability to run on other operating systems. The shortcomings associated with the existing systems and the weaknesses identified in the private-key cryptography would greatly be taken into account. The operability over multiple operating systems and the ability of the proposed application to run on a different hardware platform would not be an issue. This is convincingly so, because the application would be written in java high portability and high operability. An object oriented program like java will help achieve. For encryption, the most appropriate remedy is to combine secret key and public key system. The combination would help get the security advantage of asymmetric cryptographic algorithm and the speed advantage of symmetric cryptography or private-key systems. Asymmetric cryptographic algorithm provides a method for digital signature or envelop that explores the combined effects of public and private key systems. In order that, the challenges and the vulnerabilities pertaining to steganography is curtailed, RSA encryption algorithm combined with Huffman code algorithm is used to provide the needed security, privacy, capacity and robustness. In an environment where security and privacy is of utmost important, it is always necessary to use hard to break algorithm. The mathematical factorizations associated with the RSA encryption always make it difficult to break. The study is therefore justified on the use of asymmetric cryptographic algorithm, RSA encryption algorithm to be precise, to enhance video steganography. This will result in a method that is capable of ensuring that data is transferred over the internet safely and securely without interception by eavesdroppers or distortion of the content.

1.4 Motivation of the study

The discussion of steganography has gained prominence in recent times. Intelligence agencies, IT companies, IT experts and the media have brought the discussion into the limelight. The groundlaying principle underpinning the concept of steganography is imperceptibility. This basically means that the message hidden in the covert media should not be detectable by the human eyes. Over time, this fundamental requirement of steganographic programs has been broken. Cryptography was therefore envisaged to be another method of security provision. The combined effects of steganography and cryptography have been taunted as positive innovation in the field of data communication. Stringent and stiff measures have over the years been introduced to mitigate the attacks by hackers. Researchers, computer science experts, IT experts and other renowned individuals have proposed several approaches in ensuring secure and secret data communication. Notwithstanding the scholarly works that have already been done, there still exist challenges. At all times we must strive to ensure the integrity, secrecy and privacy of data. Against the backdrop of security threats posed by hackers and eavesdroppers in the process of data transmission, I am therefore motivated to provide solution that has the tendency to resolving the existing threats.

1.5 Research objectives

Based on the above problem statement, parameters must be identified to tackle the problem. It is therefore imperative to assess the objectives of the research that seek to

provide solutions to the identified problem. Hence the main objective of the study is to ensure the secrecy, privacy, authenticity, integrity and the non-repudiation of data that is transmitted over the internet. The specific objectives are:

- To provide a high security system that makes it difficult for eavesdroppers to detect hidden message.
- To provide efficient and effective method of concealing the existence of data from hackers and attackers.
- To provide a good, robust and high embedding capacity system of sending data securely and safely to its intended destination.
- To develop a method of platform –independent that ensures portability and consistency.

1.6 Research questions

In order that the objectives stated are achieved, questions targeted at obtaining the desire solutions must be asked. The questions to be asked in this research include:

- Will the proposed method provide a high security system that makes it difficult for eavesdroppers to detect hidden message?
- How can the proposed system provide effective and efficient method of hiding data from hackers and attackers?
- To what extent can the system ensure that larger data is sent securely and safely to its intended destination?
- What can be done to ensure that the proposed system is platform-independent for high consistency and high portability?

1.7 Scope of the study

Steganographic algorithms are many. The classification is done based on the covert media used. The proposed steganographic algorithm used in this research is video steganography. Hence, the method cannot be applied to any other steganographic algorithm but for video steganography. Again, cryptography likewise is in groups. In cryptographic algorithm, the classification is based on the number of keys used. The proposed cryptographic algorithm used in this research is the asymmetric cryptographic algorithm also known as public-key cryptography. Though there are numerous asymmetric cryptographic algorithms, the specific algorithm implemented in this research is the RSA encryption algorithm. To ensure the portability and operability of the proposed method, the code for the system is written in Java. Therefore, any platform that is not compatible with java object oriented programming language cannot run the system.

1.8 Organisation of the study

The outline of this study is divided into five chapters. Chapter One introduces the study with a general introduction and background information on steganography and cryptography; a description of the research problem, justification for the study,

motivation as well as study objectives. The research questions and the scope are described here, the chapter ends with the organisation of the study. Chapter Two presents the literature review of the study while Chapter Three describes the research methodology. The focus of the fourth chapter is on the empirical results obtained and the discussions of these results. The final chapter provides concluding discussions and recommendations. Further, recommendations for further academic research are provided in the final chapter.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

Technology as a product of knowledge has vulnerabilities so that its development is continuously undertaken. Researching steganography and cryptography relates to the perception of secrecy and privacy. This Chapter aims to review the literature to identify gaps. It starts by discussing the overview of data communication followed by the elaboration of steganography and cryptography in general, involving their definitions and concept as well as types of steganography and cryptography. Since this study uses video steganography, exhibiting a picture of video steganography basics is appropriate. This chapter also introduces us to the researches that have been done on video steganography. The chapter discusses research on video steganography using LSB insertion algorithm, follow by research on DCT based video steganography. The Chapter again introduces us to research on combine use of video steganography and symmetric key cryptosystems and finally ends by discussing related work on video steganography using asymmetric cryptographic algorithms.

2.1 Overview Of Data Communication

Before computer networks were based on telecommunication systems, communication between the machines was done by people wearing instructions from one computer to another, and most of the social aspects of the Internet that we know it began in this way (Dhupar, n.d). Data communication begun as far back as 1834 when the first Morse Code Telegraph system was invented (Morse and Veil, 1834). Data communication is therefore the exchange of digital information or transmission of digital data over computer networks or through the internet medium (Schwartz, 2010). There has been exponential advancement in data communication over the past years.

According to Li et al. (2010) increased in data access poses data security and privacy risks. Data tampering, Falsification of user identities, eavesdropping and data theft, unauthorized access and password related threats are some of the security risks that have been encountered during data communication (Oracle, 2002). Though researchers in the field of data communication continue to devise more sophisticated system of sending data securely and safely over the internet medium, attackers also continue to penetrate in a more intelligent manner. The quest to completely overcome the attacks on data communication necessitated the development of steganography and cryptography.

2.2 Definitions and Concepts of Steganography and Cryptography

2.2.1 Steganography

The rapid growth of the internet coupled with the explosive increased in data communication has triggered the need for secure data communication methods. The word "Steganography" is derived from the Greek words "Stegano" or "Stegos" meaning covered or hidden and "Graphia" or "Graptos" meaning writing (Odeh and Elleithy, 2012). In steganography, the data to be transferred is hidden or embedded in another object (Dengre et al., 2013). This is to ensure that the middle attacker cannot get hold of the message. However, an authorised person can read the content of the message (Odeh and Elleithy, 2012). According to Ramalingam (2011), steganography is the science of conveying messages in a secret way so that only the intended receiver knows the existence of the message. Xu et al. (2006) opined that steganography is a contemporary approach of covert communication whose primary objective is to convey data secretly by concealing the very existence of the data. Patidar and Patidar (2015)

argued that steganography must necessarily prevent the reading of the content of the embedded message by third party. For steganography to provide the needed security and concealment from eavesdroppers and attackers, it must be based on appropriate techniques (Sumathi et al.,2014). Cover Generation methods, Statistical Techniques, Distortion Techniques, Spread Spectrum Techniques, Transform Domain techniques, Substitution and Insertion are some of the steganographic techniques used to modify the covert media (Mathe et al., 2012). The component of steganographic process are shown in fig 2.1

Figure 2.1: Components of Steganographic process.
Source: Odeh and Elleithy, 2012.

Mazumder and Hemachandran (2013) also provided a detailed generic description of the process that takes place in steganography. Fig2.2 shows a detailed description of the process of steganography.

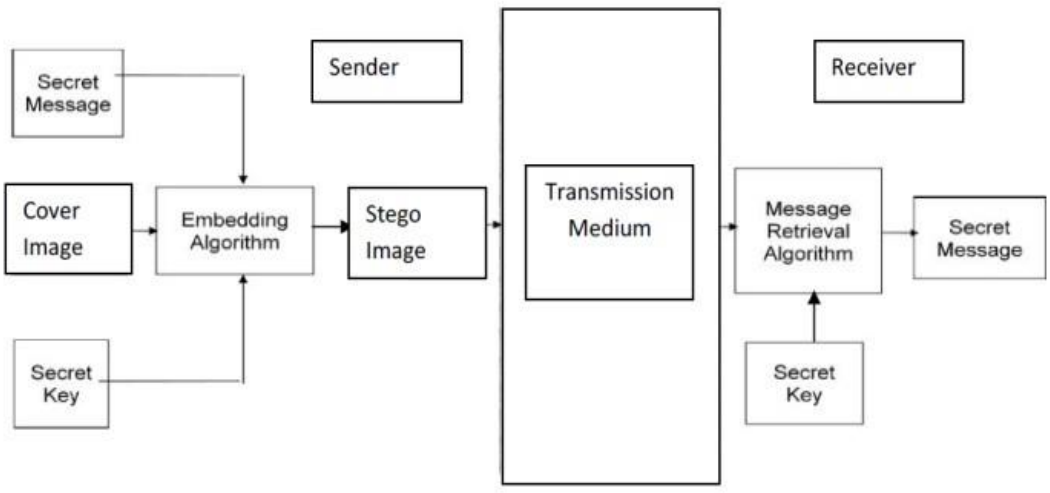

Figure 2.2: Detailed process of steganography. Source: Mazumder and Hemachandran, 2013.

Fundamentally, the role of steganography is to conceal or hide data from an attacker, eavesdropper or hackers. This aspect of steganography has been exploited greatly by attackers through the use of steganalysis (Tyagi et al., 2010). Steganalysis is therefore an application designed to expose confidential information embedded or hidden in a covert media (Gupta et al., 2012). According to Tyagi et al. (2010), the main purpose of steganalysis is to detect and extract information hidden in innocuous cover objects. Steganalysis can be passive in which only the presence of the hidden message or the steganographic algorithm is detected or active where additional features of the hidden message can be detected and extracted (Budhia et al., 2006).

2.2.2 Steganographic Types

Various forms of steganography have been proposed by researchers in the field of data communication. The types of steganography are classified according to the cover object used (Wajgade and Kumar, 2013). Rana et al. (2012) argued that there four types of steganography depending on the covert media as text, image/audio,video and protocol. Though the headers of TCP/IP packets were recognised as capable of hiding information hence the protocol steganography, image and audio were put in the same category. Khot and Patil (2015) opined the four type cover objects mainly in used as text, image, audio and video. They however failed to recognise the ability of TCP/IP header file to contain a message. Wajgade and Kumar (2013.) also opined the four types of steganography as image, audio, video network/protocol. They however failed to provide the ability of text to also hide information, hence text steganography was ignored. Al-Othmani et al. (2012), however proposed five types of steganography which is adopted in this study as text, image, audio, video and network/protocol.

One other techniques similar to steganography is watermarking. According to Umamaheswari (2010) watermarking which basically embeds information into a digital multimedia and later extracted. The main purpose of watermarking is copyright and digital content protection while steganography concerns itself with sending information securely (Cox et al., 2007).

Text as a cover media is one of the oldest used in steganography. In the olden days, letters, books and telegrams were used to hide secret messages within their text. According to Hariri et al. (2011) text steganography is the process of changing the text formatting or changing certain characteristics of the textual features. Wajgade and Kumar (2013) referred to network steganography as the use of network protocol to send hidden data. Recently, the demand for network steganography has increased due to the complexity of communication protocols(Lubacz et al., 2012). Audio steganography is a technique employed in transmitting secret or hidden information by modifying an audio signal in a manner that is imperceptible (Balgurgi and Jagtap,
2012). According to Djebbar et al. (2012), Least Significant Bits (LSB), Parity Coding, Phase Coding, Spread Spectrum and Echo Hiding are most widely used methods in audio steganography. The use of image as a cover object to hide information is called image steganography (Hussain and Hussain, 2013). In general, the approaches used to hide information in image are pixel intensities. According to Shelke et al. (2014) images are one of the most popular carrier file or cover objects used in steganography. Tiwari et al. (2014) asserted that digital images are attractive for steganographic systems due to their degree of redundancy in the presentation and preservative systems in our everyday life. According to Eltyeb and Elgabar (2013) different image file formats such as JPEG, GIF, TIFF, BMP and PNG can be implemented in image steganography. Video steganography is the technique of embedding a message in a carrying video file

(Prabakaran and Bhavani, 2012). The capacity for video to contain large amount of data (Xu et al.2006.) makes it the most appropriate data hiding technique. Video files are composition of images and sounds or series of frames. Swathi and Jilani (2012) argued that video steganography is suitable and the most appropriate due to its size and memory requirements. Various video file formats exist but the most popular and widely used video file formats are MPEG and AVI (Rhoads, 2007). To further strengthen data communication security, cryptography was introduced.

2.2.3 Cryptography

Cryptography until recent times was referred to be encryption (Al-Vahed and Sahhavi, 2011). Cryptography can simply be defined as the process of data storing and transmitting in a particular way such that, those whom the message is intended for can read and process it (Kundalakesi et al., 2015). Cryptographic technique plays an essential role in protecting data communication (Raghu, et al., 2012), and also ensures that only intended recipient receives the message (Venkateswaralu et al., 2012). According to Kundalakesi et al.(2015) cryptography is very important in data communication especially when the data is being transferred over an untrusted medium particularly the internet.

Cryptography is directly connected to cryptology and cryptanalysis (Furht et al., 2005). The Encyclopeadia Britannica (n.d), referred to cryptology as " science concerned with data communication and storage in secure and usually secret form ".Cryptanalysis is the technique of studying ciphertext in order to reveal the protected data (Katz and Lindell, 2014). Cryptanalysis is a counter measure against cryptography whose targeted objective is to reveal the algorithm that is used to encrypt the message.

In modern computer world, cryptography is associated with encryption which is the process of scrambling plaintext, which is an ordinary text into a ciphertext (Natarajan et al., 2011). Encryption is the most secured way to achieve data security in cryptography. The process of converting the ciphertext into plaintext at the recipient side is called decryption. Joselin et al. (2015) opined that for encryption to be made possible, it must do so through the use of keys.

2.2.4 Types of Cryptographic Algorithms

Garg and Yadav (2014) classified cryptographic algorithm into two types based on the number of keys: asymmetric and symmetric. Al-Vahed and Sahhavi (2011) also consented to the two types of cryptographic algorithms as asymmetric and symmetric. However, Kundalakesi et al.(2015) contended that based on the number of keys used , cryptographic algorithm are classified into three types, namely asymmetric, symmetric and cryptographic hash function. The fig 2.3 shows the three types of cryptographic algorithms.

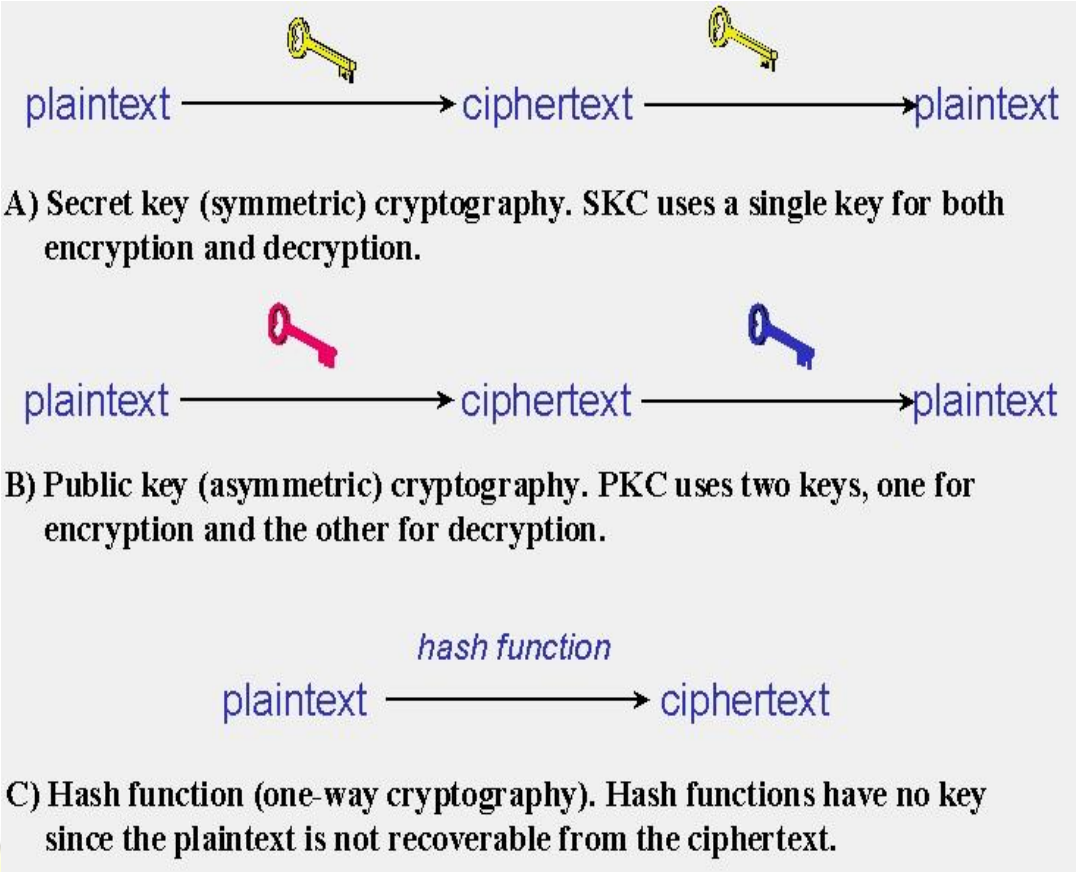

Figure 2.3: Depiction Of The Three Classification Of Cryptographic Algorithms

A cryptographic hash function irreversibly encrypts information using mathematical transformation. According to Panford et al. (2015) Cryptographic Hash Functions (CHFs) accept variable length of messages and transform them into fixed length hash codes called digests. Cryptographic hash functions are necessary tool of cryptography and exhibit a rudimentary task in effective and secure data processing (Gauravaram and Knudsen, 2010). In symmetric key cryptography, the key used to encrypt the message by the sender is also used to decrypt the message by the receiver (Al-Vahed and Sahhavi, 2011). Elminaam et al. (2010) categorised symmetric key cryptography into two types, block cipher and stream cipher. Asymmetric cryptographic algorithm uses two keys, a public key used for encryption and private key used for

decryption (Salomaa, 2013). According to Vahedi et al. (2013) the public key used for the encryption can be transmitted over an untrusted network like internet.

2.2.5 Steganography and Cryptography

Many until modern times believed that steganography is an alternative to cryptography. According to Ramalingam (2011), steganography is rather the dark cousin of cryptography and not an alternate. Whereas steganography provides secrecy cryptography is intended to provide privacy. The very essence of steganography is to hide or mask the existence of the message while cryptography concerns itself with the masking of the content of a message. The seemly exploitation of steganalysis which detect the presence of hidden message in covert media (Das et al., 2011), made the combined effect of steganography and cryptography crucial. Whereas steganography can use cryptography, cryptography cannot use steganography (Kaur and Singh, 2015.)

2.3 Video Steganography Basics

The main objective of securely hiding data in video is to achieve better confidentiality and data recovery (Shraddha et al., 2014). Using video stream to hide data should remain undetected by the human eye. If a steganographic algorithm based on video is detected then it is invalid. For the purpose of concealing message in video two video steganographic algorithms; Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) have been proposed (Bodhak and Gunjal, 2012). In Least

Significant Bit (LSB) algorithm, the least significant bits of the carrier file's individual pixels are modified, hence the hidden data is encoded (Neeta et al., 2006). Bodhak and Gunjal (2012) explained that Discrete Cosine Transform (DCT) transforms the image component of the video from spatial domain to frequency domain. Singh (2014) opined that most of data hiding techniques in video are based on Least Significant Bits Algorithm. This is primarily so due to its low computational complexity (Singh, 2014). Wajgade and Kumar (2013) explained that Least Significant Bits when used in video replaces the last digit of the carrier file. Video steganography that is used to hide data should be robust against attacks, as such any algorithm used to hide data in video must conform to this basic requirement (Wajgade and Kumar, 2013).

Bhaumik et al. (2009) asserted that for data hiding techniques in video to be useful it must be evaluated on certain important characteristics namely; imperceptibility, capacity, robustness s and security. However, Elbayoumy et al. (2014) contended that data hiding techniques in video be evaluated on requirements of perceptibility, capacity, robustness to attacks and tamper resistance. When the video with embedded data and the video without data are noticeably identical, we say it is imperceptible (Bhaumik et al., 2009). Capacity is the amount of data that can be hidden in the video whereas robustness talks about the ability of video steganography to resist destruction and changes when subjected to manipulations. The overall purpose of steganography is to provide security. Security which is refers to the inability of hidden data to be accessed by unauthorised person (Sherly and Amritha,
2010) as a requirement evaluation in video data hiding may not be accurate.

By far, video steganography hiding technique is the best since it overcame the

capacity problem of image steganography and alteration problem of text steganography . Using video as a cover object didn't overcome the capacity problem only, but it also enhanced the security of the embedded data (Basheer and Safiya, 2014).

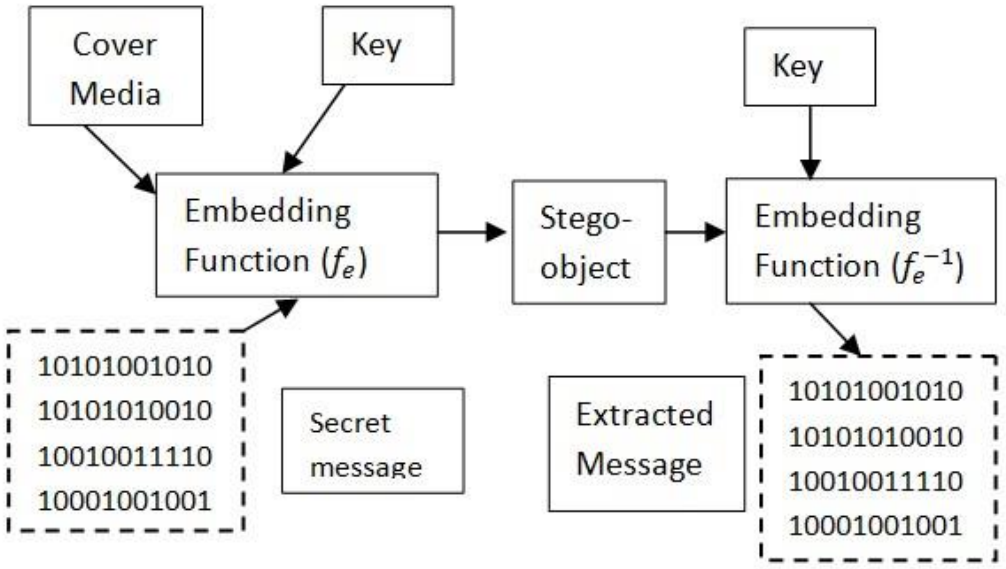

Figure 2.4: A Block Diagram of Data Hiding.

Source: Elbayoumy et al., 2014.

2.4 Research On Video Steganography Using LSB

The use of Least Significant Bit (LSB) for video embedding is widely used due to the easiness associated with its use. It is also good for larger file size.

Bhaumik et al. (2009) proposed a method of data hiding in video using LSB. In their approach, a high resolution AVI video file was streamed to get images and AVI video frames. A single bit plane LSB replacement algorithm was used to embed the message into the AVI video frame. The method was successful but found to fall short of some video quality metrics. The use of single bit plane LSB replacement makes the proposed system prone to detection by eavedroppers . Ker (2007) opined that least

significant bit involving multiple bit planes is less to detect than single bit plane. No quality check was also done to compare the original video to the stego video.

Malde and Admuthe (2013) however proposed a method of data hiding in video of motion vectors. In this approach, a video file was framed to get motion vectors, the magnitude of the motion vector was calculated to select the video stream with larger magnitude. A stream with larger magnitude limits distortion during embedding. The secret message was then embedded using the multiple bit LSB replacement. A PSNR comparison was made which showed negligible changes in the original and the stego video. The method however was limited to only compressed video. Video steganography is divided into types namely embedding data into uncompressed video which is later compressed and directly embedding data in a compressed video (Chae and Manjunath, 2000).

Elbayoumy et al (2014) proposed a technique for data hiding in video which is relevant to this study. A least significant bit (LSB) embedding algorithm was used to hide the data into the images of a video file. Because video is a composition of images, the system was successful in applying it to different image file format. Another security measure was introduced to check the noise level cause by the embedding algorithm. A hash code application was used to check whether the image has been modified or not. A PSNR quality metric was applied which showed an improvement in video quality. One major disadvantage identified in this approach was that, it was susceptible to the human eye due to the use of spatial domain technique in hiding the data.

Singh (2014) also proposed a novel Least Significant Bit insertion method for video steganography. The LSB video file was changed with the information bits. LSB substitution was used to hide the information in specific frame of the video and specific

position of the frame. The system is user friendly and simple. However, the author failed to perform quality metric check such as PSNR to check the quality of the original video to the stego video. The payload capacity of the systems is also low.

Basheer and Safiya (2014) proposed a novel approach of hiding data in video that had the capacity of improving the security performance of LSB substitution algorithm. The method first breaks the video files into frames .A perceptual distortion model specifically, just noticeable distortion (JND) is applied to the compressed video for quality improvement. A mapping function based on human visual sensitivity was also applied on the LSB to change the gray level value of each pixel. The system was very portable and platform independent since java was used in the development of application. The approach however was not subjected to objective quality measure. The most appropriate quality metric is PSNR not the human visual sensitivity.

2.5 Embedding Data In Video Steganography Using DCT

Discrete Cosine Transformation (DCT) based video steganography begun many years ago as one of the most robust data embedding technique in digital images. Though LSB has become the most widely used video steganography embedding technique, DCT still remain in use.

Chae and Manjunath (1999) proposed a system of data hiding in MPEG video file format using block of DCT. In this approach, an input video file was first streamed into host frames and signature image. The host frame was then transformed to the DCT domain using 8*8 block size. The 8*8 block size host frame was then analysed to check the content of the texture and the texture block factor was also calculated. The computation of the texture factor helps to appropriately scale the signature coefficient

using the signature quantization matrix. Upon estimation of the signature codes using the total scale factor, the signature codes and the original DCT coefficient were then combine to form the fused blocks of DCT coefficients. The fused blocks of DCT coefficients was therefore inversely transformed to form the embedded frame. The system was robust at the time due to the results as shown by the PSNR output. A large amount of data was embedded. However, in contemporary video quality metric measurement, the system cannot provide the necessary robustness needed to secure data transfer. Current video quality metrics ranges averagely from 30dB to 50dB on the PSNR scale, however the system recorded 19.4dB after the MPEG coding from the embedded frame.

The choice of which embedding technique to use in a video steganography is a daunting task. This is pretty so because each of LSB and DCT has its own advantages and disadvantages. LSB has the capacity to allow a larger amount of data to be embedded whereas DCT ensures less and unnoticeable distortion with small file size.

Walia et al. (2010) proposed a system that compared the performance of LSB based video steganography and DCT based video steganograpgy. In this method, a data was first embedded in a video file using LSB replacement algorithm, the same file size was embedded using DCT frequency domain. The results as shown by the PSNR indicated high quality with the DCT frequency domain. Walia et al (2010) therefore recommended the use of DCT rather than LSB due to the security of DCT for smaller file size. In a sharp contradiction, a system proposed by Ahmed (2014) showed otherwise. Ahmed (2014) proposed a system of comparing data hiding techniques in video file. Experimental results from the system showed that 75% of the hidden

message using LSB showed higher PSNR values than the one using DCT. The file size embedded in Ahmed (2014) was larger than Walia et al. (2010).

Bodhak and Gunjal (2012) proposed a system of improving the protection of video steganography based on DCT and LSB embedding algorithms. In their approach, an AVI video file was converted into frames and images. Randomly selected images were then broken into 8*8 block pixels. 128 were then subtracted from each block of pixels from left to right in a top- bottom manner. DCT frequency domain algorithm was applied to the block pixels and the block pixels were subsequently compressed through the process of quantization. The LSB of each discrete cosine (DC) was computed and each bit was then replaced with a secret message. This approach is completely opposite to the one proposed by Khosla and Kaur (2014). The system behaved as expected as all expected results matched actual results as shown in the system's testing phase. This system is comparatively better since some form of encryption idea was introduced. The message to be hidden was first converted to bytes to obtain some secret key. However, this method of encryption was not strong enough to prevent eavesdropping.

Bodhak and Gunjal (2013) proposed an improved video steganography performance using DCT. In this method, a new encoding technique called Class Dependent Coding Scheme (CDCS) was applied to the DCT frequency domain to enhance payload capacity. An AVI video file formart was input to extract the video frames. The image frames were randomly selected to embed the secrete file. The DCT embedding technique was applied to the 8*8 image frame and the data was embedded using quantization modulation to obtain the DCT coefficients of the block frames. The video was finally reconstructed from the frame containing the secret data to get the stego video file to send. The system was an improvement of the one proposed by Chae

and Manjunath (1999). The system was robust and platform independent since an object oriented programming language, Java was used. The only problem identified with this system was the fact that the secret data embedded was not encrypted.

Khosla and Kaur (2014) proposed a system of securing data using watermarking and steganography. In their approach, DCT and LSB were combined in the embedding process. A video file was first converted to frames and images, and frames were randomly selected to act as covert media. Password was added graphically, to make it more secured. The secret messages were then hidden inside the randomly selected image to get the binary data in which the LSB replacement algorithm is applied. The DCT domain frequency is then applied on the LSB binary data to be transmitted over the internet. The system was robust against attacks and more secured. However, the proposed system was not platform independent since the implementation was done in MATHLAB.

Over the years, several steganographic algorithms have been proposed. Different methods of video steganography have also been implemented in the past. Majority of these systems have suffered some attacks. Das et al. (2011) opined that steganographic attacks comprises of detecting, extracting and destroying the hidden data within the covert media. Visual attacks and statistical attacks (Bateman and Schaathun, 2008) are the two widely known attacks against steganography. Pevný and Fridrich (2008) developed a steganalysis application that was successful in detecting a message embedded in image based on DCT. Statistical video steganalysis proposed by Bhudia et al. (2006) also successfully detected and extracted a data hidden in video whose algorithm was based on LSB. Because of the fear of terrorists using steganography to

communicate over the internet, Qi (2013) came out with a steganalysis called the active warden approach that was capable of detecting embedded messages in image and video.

In order to mitigate the attacks against steganography, many researchers have proposed systems that combine steganography and cryptography for optimal security and secure data transmission.

2.6 Video Steganography Based On Symmetric Key Cryptosystem

Symmetric cryptographic algorithm also known as symmetric-key cryptography was the only known cryptography until 1976 (Diffie and Hellman, 1976**)**. Symmetric key cryptography is the use of only one key known as single key or secret key or private key for both encryption and decryption. DES and AES are the most popular private key algorithms.

Taqa et al. (2009) proposed a system for video steganography using LSB substitution algorithm with AES data encryption technique. In their approach, a video file was converted into images and frames, the data to be embedded was first encrypted using the AES encryption scheme. The AES encrypted file is then embedded in a randomly selected frames using LSB insertion algorithm. At the receiver's side, the encrypted file was first extracted from the video and the private key used for the encryption was used to decrypt the file. This approach however failed to compress the file encrypted. No quality metric measure was also performed to check the robustness of the system.

Sarmah and Bajpai (2010) also proposed video steganography application using DCT embedding technique with AES cryptographic algorithm. In this method, a video

file was embedded with a secret data encrypted using AES encryption scheme. The encrypted file was first compressed using Huffman compression algorithm. The compressed encrypted file was then embedded in the 8*8 block pixels of the frames using DCT. Though DCT does not support large file size, the compression allowed a substantial amount of file to be embedded. No comparison of the original video and the stego video was also done to check for distortion in the video quality.

Wajgade and Kumar (2013) in their quest to further strengthen AES encryption algorithm proposed an enhanced video steganography application. In this method, the video was embedded with an encrypted file using AES. A secured hashed algorithm (SHA-1) was then applied to the encrypted file to make it restricted so that when the file is identified it cannot be altered without a key. LSB replacement algorithm was finally applied to embed the encrypted data into the video. This system provided much security to the data that was transmitted. However, the payload capacity was low since the file was not compressed. Again the videos were not check for noticeable distortion.

Reddy et al. (2013) however proposed a similar video steganography approach but with different encryption scheme. Their novel approach was aimed at hiding encrypted data into image, audio and video using steganography. The file to be hidden was encrypted using DES encryption and the encrypted file was embedded with LSB replacement algorithm. No compression was done and no quality of video check was also carried out. The DES encryption security is also poor since it was broken long ago (Zande, 2001).

Dengre et al (2013) proposed an improved version of video steganography by introducing the techniques of watermarking and multiple symmetric key encryptions. In their proposed system, AVI video was input to extract the frames and images. The

audio file to be embedded using LSB was encrypted with DES, triple DES, RC2 and Rijndael algorithm. The results showed that triple DES and RC 2 generated the highest number of binary bits, hence triple DES and RC2 were used for the encryption. Watermarks were then added to the frames of images in the audio file and were then inserted into the AVI video to obtain the stego video. This approach is more complex and an improvement of earlier versions. However the system works with uncompressed video files only.

Gupta and Chaturvedi (2014) haven identified the weaknesses of the existing system proposed a better approach. Most of the issues raised in the previous systems were addressed in this method. An AVI video was converted into images and frames. An AES encrypted file was embedded in a randomly selected frame using LSB replacement algorithm. The MSE of the stego video was computed to the check the PSNR of the original and stego video. The MATHLAB displayed computed PSNR showed that there were no noticeable variations or distortion in the two videos. The approach however did not apply compression but it was the most robust as compared with earlier proposed system.

Historically, several symmetric key cryptographic based video steganography exist. Those reviewed in this study are selected few. However, not a single of the proposed system was able to address the fundamental challenges associated with symmetric key cryptography. The secure way of transmitting the private key over the untrusted internet medium for encryption and the inability of symmetric key to provide digital signature facilitated the systems such as the one proposed in this study.

2.7 Video Steganography Using Asymmetric Cryptographic Algorithm

In order that the key distribution problem in symmetric key is curtailed, public key or asymmetric key cryptography was proposed (Diffie and Hellman, 1976). Asymmetric cryptographic algorithm uses two keys, a public key used for encryption and private key used for decryption (Salomaa, 2013). The most well regarded asymmetric cryptographic algorithms are Rivest Shamir and Adleman(RSA) algorithm, ElGamal, Digital Signature Algorithm (DSA), Diffie-Hellmann (D-H) and Elliptic Curve Cryptography (ECC) (Laskov, 2015).

Tyagi et al. (2010) proposed a novel system of securing a larger file size for data integrity and authenticity using LSB insertion algorithm with RSA encryption algorithm. In this method, a video file was embedded with a secret file encrypted with RSA encryption algorithm. RSA encryption makes the security of the system hard to tamper with. The approach was successful in embedding a considerable size of file into the video. However, the file was not compressed hence the payload capacity was low. No PSNR quality measure was also performed to check the distortion caused by the embedded file; therefore the system could not be concluded to be robust. For steganographic system to be deemed effective and efficient, capacity, robustness and security must be evaluated. The researcher failed to all of this important exercise.

Jain (2012) proposed public key steganography using LSB with Deffie-Hellman key exchange protocol. A shared stego-key was found between two communicating people through the application of Deffie-Hellman algorithm. This system is not efficient in that, Deffie-Hellman does not encrypt the file. A different encryption standard needed to be performed before the key is exchanged through Deffie-Hellman key exchange protocol. Authentication could not also be achieved in this application since Deffie-

Hellman does not provide that function. The embedded file was not compressed and evaluation to determine the security, capacity and the robustness of the application was completely ignored.

Deshmukh and Rahangdale (2014) also proposed a data hiding technique in video steganography using LSB replacement algorithm and hash function. An AVI video file was selected and converted into images and frames. The file to be hidden was then inserted into the frames using LSB insertion algorithm. Hash code which provides password to hide data was used to find the position to allow the LSB insertion to take place by splitting the secret text into 3bits, 3bits, 2bits for red, green and blue pixel stego frames respectively. The other frames in addition to the stego frames were combined to get the stego video. This system was able to embed a sizeable amount of data without causing any distortion as showed in the experimental results. The system however was not secured since the embedded file was not encrypted. Encryption is one of the most important consideration in steganographic applications since it provides security.

Mohanta (2014) proposed a secure video steganography using Elliptic Curve Cryptography and LSB insertion algorithm. The author first encrypted a secret message with the ECC algorithm. The encrypted file is then inserted into an image using LSB. The image is subsequently embedded in the cover video using the same LSB technique. MSE was calculated to determine the PSNR. The PSNR results showed that the system was robust. However, the hybrid approach of inserting the text in an image before finally embedding in the cover video increased the computation overheads and slow down the system. ECC encryption is however less secured as compared to RSA (Singh et al., 2014). The encrypted file and the image containing the encrypted data were all

not compressed. This system can be inferred to achieve only one consideration of steganographic applications, thus robustness. However, security and capacity are very important and it should have equally been considered.

Shukla and Singh (2014) proposed a secured data communication application based on RSA encryption with LSB insertion. A raw data was embedded in an AVI video file after performing RSA encryption. This system was secured because of the use of RSA encryption. RSA algorithm is the most secured public key cryptography. The system was not robust as the histogram showed a noticeable distortion after embedding 96bits of file in the frame. The payload capacity of the system is very low as no compression algorithm was performed on the data. No MSE and PSNR computations were done to verify the distortion in the original and the stego videos. Though no compression was carried out, the researcher also failed to prove how robust and secure the system was without the necessary quality metrics.

Kumar et al. (2014) also proposed a similar system that showed not much different to the one proposed by Shukla and Singh (2014). The same method was adopted with no new parameter or new technique. The system was however a little improvement over the one proposed by Shukla and Singh (2014). The payload capacity of the system is as well very low as no compression algorithm was performed on the data. No MSE and PSNR computations were done to verify the distortion in the original and the stego videos.

Kaur and Singh (2015) however proposed an improved version of the system proposed by Mohanta (2014). In this approach, an image to be transmitted was first encrypted with ECC encryption algorithm and inserted into the cover video using LSB insertion. Huffman compression was applied on the hidden image for bandwidth

optimisation. The system was very robust with high embedding capacity as showed by the PSNR experimental results. The problem identified in this system is the fact that ECC cannot be used efficiently for larger data size as compared to RSA. To some extent, the researcher considered almost all the important considerations in steganographic applications. However security, capacity and robustness are considered trinity in steganography. The use of ECC instead of RSA makes the system exposed to security threats when a larger file is to be sent. Perhaps this is the most recent and closely related work in existence

Kour and Kaur (2015) proposed a data hiding system that is applicable in images and videos. DSA was combined with multiple LSB for the steganography. The carrier file file being video or image is selected, and then the raw data to be hidden is also selected with the implementation of the DSA to generate the key. Multiple LSB is performed on the data and embedded in the carrier file to get the stego video which is finally sent to the receiver. This system resulted in the provision of data integrity and authentication. However, since the DSA does not encrypt the data it is still prone to attacks. MSE and PSNR calculations were also not done and no data compression algorithm was employed. Encryption is one of the most important consideration in steganographic applications since it provides security.

Vegh and Miclea (2015) proposed a system for ensuring security in physical cyber system using LSB for the steganography and ElGamal for cryptography in addition to digital signature. Elgamal has the disadvantage of doubling the ciphertext of the plaintext and not efficient for larger file size as compared to RSA encryption algorithm.

Sameerunnisa et al. (2015) however proposed a system that seems to be an improvement of earlier proposed systems. The system utilised RSA encryption to

provide security for video steganography. A video file is first broken into images and frames. Frames are randomly selected to embed the data using Hash-LSB insertion algorithm. RSA computation is performed to generate the keys needed for encryption. SHA-1 technique is applied on the RSA encrypted file before the steganographic process is activated. The only feature added to the earlier proposed system is the application of SHA-1 on the RSA encrypted file. The embedding capacity of the system was not computed. Again, it was observed that the system could not take large amount of data since no standard compression algorithm was employed. No video quality metric measurement was also carried out to check the extent of distortion. Computation of MSE and PSNR of the original and stego video are necessary to ensure the robustness and the security of the proposed system.

Various forms of video steganography are in place. Majority of them have been reviewed in this study. Upon careful completion of the review of the existing literature, it is accurate to say that a lot of gaps exist in development of secure video steganography for data communication. Most of the existing systems lack good user interface and not platform independent. The method proposed is this study is carried out with aim of embedding a message or secret file in a video as cover using the appropriate techniques. The most important stimulation for this study is to increase the payload capacity of the embedded data robustness and security through the use of PSNR and MSE. After the review of the existing system, the main contribution of this study is to offer a new path on how to improve the steganographic systems that are currently in existence. The comparative advantages with respect to this study are more security, more flexibility, more invisibility, high robustness and larger payload embedding capacity. The flaws and the weaknesses identified in the existing system would be taken into consideration

in order to design a system that is highly secured, robust, and efficient and with high embedding or payload capacity.

2.8 Least Significant Bit (LSB)

For the purpose of concealing message in video two video steganographic algorithms; Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) have been proposed (Bodhak and Gunjal, 2012). In Least Significant Bit (LSB) algorithm, the least significant bits of the carrier file's individual pixels are modified, hence the hidden data is encoded .Ahmed (2014) proposed a system of comparing data hiding techniques in video file. Experimental results from the system showed that 75% of the hidden message using LSB showed higher PSNR values than the one using DCT.

2.9 Huffman Code Compression Algorithm

In order that, the application is able to embed a larger amount of data, a compression technique was used. There are many compression techniques available for use. The technique used in this study was the Huffman code compression. The Huffman algorithm is easy to implement and produces lossless compression. Huffman compression belongs into a family of algorithms with a variable codeword length. The basic idea behind the algorithm is to build the tree bottom-up whose leaves are labelled with the weights.

For example. Let us consider this ASCII fixed length code.

A 000 B 001 C 010 D 011 E 100 F 101 G 110 H 111 .With this code, the message **BACADAEAFABBAAAGAH** is encoded as the string of 54 bits as

00100001000001100010000010100000100100000000110000111.

Now let us consider the variable length code below:
A 0 B 100 C 1010 D 1011 E 1100 F 1101 G 1110 H 1111, with this code, the same message as above is encoded as the string of 42 bits.
100010100101101100011010100100000111001111. In comparison, 20% of space is saved.

2.10 RSA Algorithm

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

The key generation involves obtaining two keys, private and public keys. This is generated through the factoring problem of RSA. A key distribution involves the sending of the public key through a communication medium normally the internet by a recipient of a message to the sender of a message. The process by which the sender converts a message into a binary bit using the public key is called encryption. At the recipient end, the message is reconverted from binary bit to the original text using the private key. Such process of decrypting the message using the private key is called decryption.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

Research Methodology comprises of major aspects of the research that deals with strategy and procedure adopted for the study. In this chapter, the model proposed for the study is discussed. This basically concerns itself with the steps that were followed for the development of the proposed work. The proposed model is followed by the proposed work, which is divided into three parts: cryptography, compression and steganography. The research strategy and procedure including data collection method and instrumentation is discussed. The chapter ends by elaborating on criteria used for evaluating the performance of the proposed system as well as the parameters used for the performance evaluation.

3.1 Proposed Model

The proposed model makes use of covert media, specifically video as a carrier for the secret data. The data to be sent secretly over the communication channel is the input secret file. At the destination, the legitimate recipient has to undergo some required steps to process the message so as to reveal the data; else the very existence of the secret file is indiscernible. The proposed technique fundamentally ensures that quality information is hidden to differentiate this system from a typical data hiding application currently in existence. This is so, due to the larger payloads capacity that this system is significantly required to provide.

There are three main phases that composed of the proposed model. The first is the encryption phase that converts the message to be sent into binary data to get the secret file. Compression is applied as a second phase to reduce the size of the encrypted file in order to accommodate larger payloads. The third phase is the embedding technique which deals with the process of hiding the encrypted file into the cover video. Fig. 3.1 depicts the proposed model.

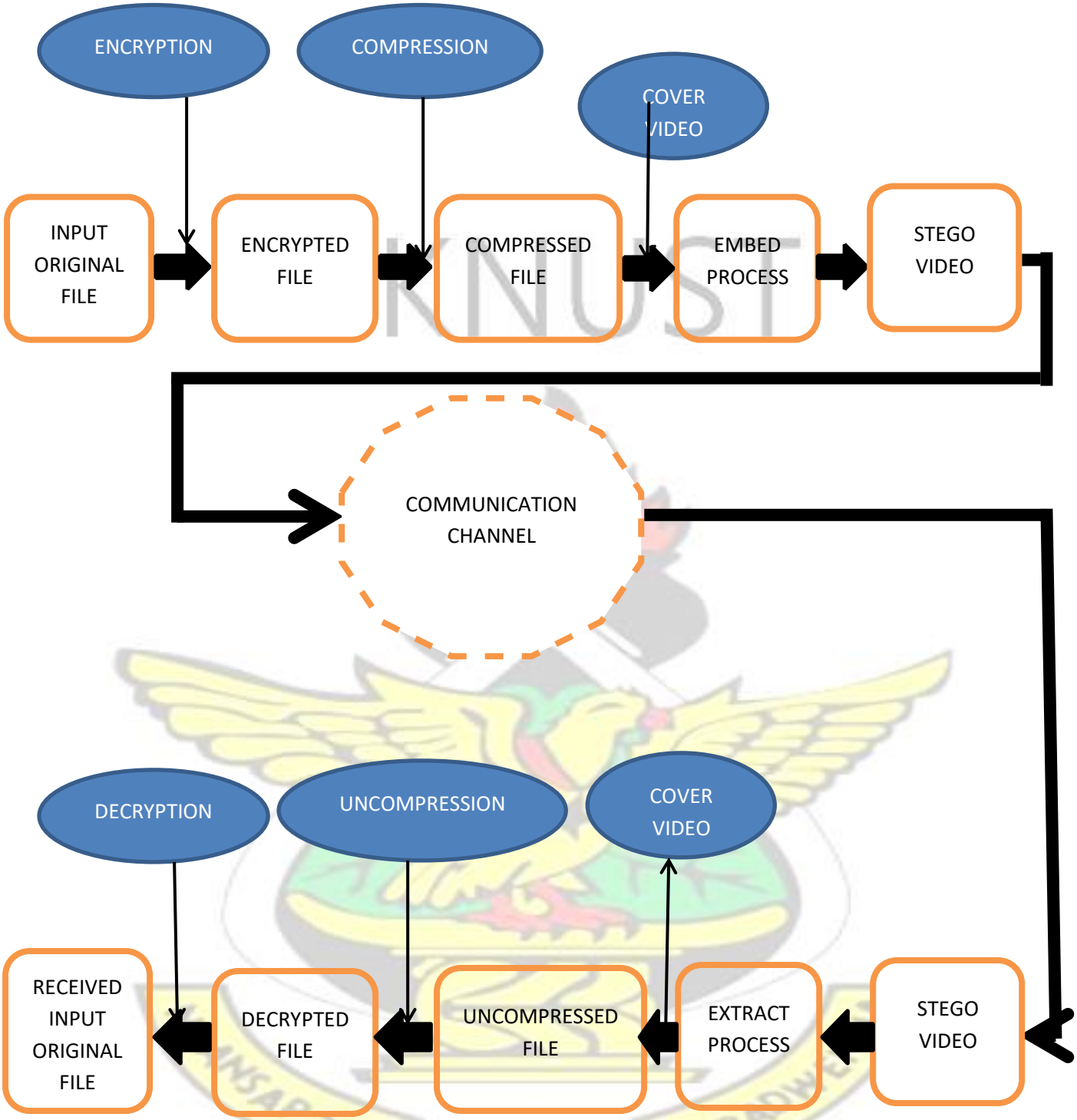

Figure 3.1: The Proposed Model

The entire process of the proposed model is composed of ten main consecutive steps: The first step is the encryption phase in which a standard encryption algorithm is employed to convert the secret message into an encrypted file normally in the form of binary data for utmost security. In the second step, the encrypted file is compressed

using a lossless data compression algorithm in order that a large amount of the file would be embedded and also to ensure bandwidth optimisation during the transmission process. The third step is a process in which the video is converted into frames for the techniques of embedding to be made possible. The fourth step is the application of the embedding technique to hide the compressed encrypted file into the appropriate selected frames. The fifth step is the reconstruction of the converted frames to obtain the stego video. In the sixth step, the stego video is sent over the communication channel, normally untrusted medium like the internet to the intended recipient. At the destination, the intended recipient undergoes the seventh process in which the cover video or the stego video is separated again into frames in order to get the frames holding the compressed encrypted secret file. In the eighth step secret file is extracted from the holding frames. In the ninth step the secret file is uncompressed to get the encrypted file, whereas the tenth step decrypts the encrypted file using the intended receiver's private key through a process called decryption to obtain the input original file. The proposed model however is not concerned about securing the communication channel

3.2 The Proposed System

The proposed system is basically divided into three main categories.

3.2.1 Cryptography

Before embedding a message into a video, the message is first encrypted using RSA encryption algorithm. The algorithm first generates two keys, public and private

keys for encryption and decryption respectively. Then, encrypted message is hidden using steganography.

3.2.2 Video Steganography

Video files are composition of images and sounds or series of frames. Least Significant Bit (LSB) technique is used to embed message into video. In this procedure, a video is separated into frames and the appropriate frame is determined and selected based on the histogram values of the frames. The message is therefore embedded using the LSB method. This procedure ensures double security based on the assumption that, if an unauthorised individual extracts the message from the video, the message cannot be read. This is mainly due to the encryption of the message with the receiver's public key using RSA algorithm.

3.2.3 Data Compression

Before the encrypted message is hidden or embedded, data compression technique is applied to reduce the size. Huffman code compression was used in this application. Huffman code is a lossless compression scheme in that no data is lost after compression. It is the compressed encrypted file that is embedded into the video using LSB insertion.

3.3 Research Strategy and Procedure

The strategy which was adopted and appropriate to implement this empirical study is experimental research. Experimental research has the objective of evaluating and testing existing system or new system with the expectation of how the said system

works or behaves. This is an important element of engineering and scientific process. Therefore, if the experiment is properly and well executed, the outcome would solve the identified problem. The procedure followed in this study was the development of Test Suite using JAVA SDK and NetBeans IDE in a lab to conduct the study on a computer system.

3.6 Criteria and Parameters For Performance Evaluation.

Steganographic applications are evaluated on some basic views. The criteria upon which the performance of such applications is evaluated are Security, Robustness and Capacity. These performance evaluation criteria are independent of each other. Fig 3.2 illustrates the three performance evaluation criteria.

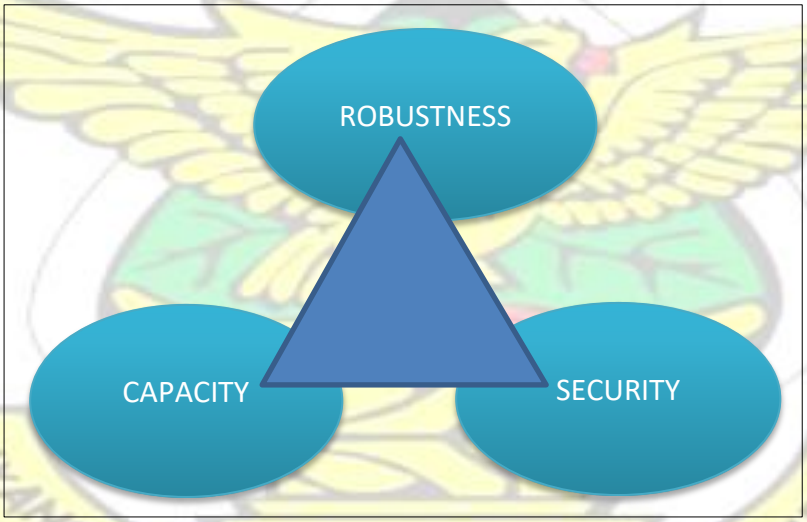

Figure 3.2: Criteria For Performance Evaluation

3.6.1 Robustness

Robustness of the steganographic application is the ability of the system to withstand various attacks and manipulation. It clearly demonstrates the quality of the system developed. In this regard, the quality of the original video is compared with the quality of the stego video. The Parameter used to demonstrate the robustness performance of

the application is Peak-Signal-to-Noise-Ratio (PSNR). PSNR is a video quality measure by comparing the original video to the stego video. The unit of measurement of PSNR is decibels (dB). The higher the PSNR value, the quality the video . PSNR is calculated using:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\ &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE) \end{aligned}$$

where MAX_I is the maximum possible pixel value of the image. $MAX_I = 2^B-1$, B is the bits per sample. So if the image is represented using 8 bits per sample, $MAX_I = 2^8-1$= 256-1 =255, therefore PSNR can be rewritten as **PSNR = 20. Log $_{10}$(255) - 10. Log $_{10}$(MSE).**

MSE is the Mean Square Error which is the measure to determine the distortion between the original and the stego video. MSE is calculated using:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

where M and N are the Height and Width of the video respectively.

3.6.2 Capacity

Capacity which is mostly referred as embedding capacity or payload capacity is the amount of data that can be embedded or hidden in a cover object without the quality of the video deteriorating statistically or without causing statistically significant modification. Capacity is expressed in terms of bits per pixel whereas the maximum hiding capacity is expressed in term of percentage.

$$Capacity = \frac{number\ of\ bits\ used\ to\ hide\ data}{total\ number\ of\ bits\ in\ image} \times 100\%$$

3.6.3 Security

Security is the ability of an unauthorised person or a third party to discover or detect a hidden information or message in a video. This criterion is purely demonstrated by the embedding algorithm and the encryption algorithm used. In this case, the RSA and LSB algorithm should be able to make it difficult for a third party to detect the hidden information.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.0 Introduction

This chapter gives elaboration on the most important aspect of the study. This comprises of implementation of methodology and results obtained. The results show the user interface design of the various phases of the system. The chapter ends by

discussing the analysis of the proposed system with respect to the performance parameters.

4.1 Implementation of Proposed Model/System

The system was implemented using JAVA SDK and NETBEANS IDE as the development tools**.** The version of Java used to develop the application is the Standard Edition (SE). The Java platform, Standard Edition allows you to develop and deploy java applications on desktops and servers. One major objective of this research is to develop a method of platform –independent that ensures portability and consistency. The application is designed to provide good and friendly user interface. The tool used to design the interface is Java FX. Java FX which consists of graphics and media allows you to design and deploy rich user interface client applications that work consistently over a wide range of platforms. The environment in which the code developed in Java SE was run is NetBeans IDE. The NetBeans IDE provides a faster and smarter way to code and supports the JDK, Java SE and Java FX.

4.1.1 Home Page

Fig. 4.1 shows the home screen when the application is run. The home page shows the various processes that have to be followed to encrypt, compressed, embed and send over the internet to the intended recipient. The inverse of the process is also shown.

Figure 4.1: Home Page

4.1.2 Security Menu

The security menu consists of the encrypt and the decrypt pages. This is where the entire security of the system resides. The algorithm implemented to encrypt and decrypt the message is the RSA algorithm. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. In order to encrypt the messages, two keys must be generated. The public key and private key are generated for encryption and decryption respectively. Fig. 4.2 illustrates the working example of how the keys are calculated and fig. 4.3 shows the algorithm for key generation.

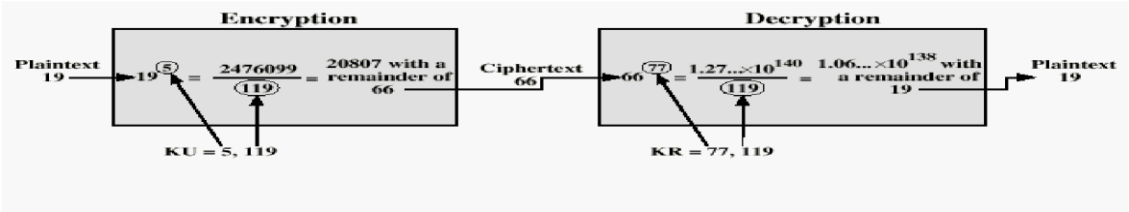

Figure 4.2: How the public key and private keys are generated

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Figure 4.3: RSA Key Generation Algorithm

When a user generate the keys, a file is then chosen to encrypt. In fig 4.6 , when a user click the encrypt button, the user is prompted to enter the public key e, the another prompt pops up for public key n to be entered. At the recipient end, the values in d and n is entered as private keys to decrypt the message. Fig 4.4 and fig 4.5 show the encryption and decryption pages.

Figure 4.4: Encryption Page

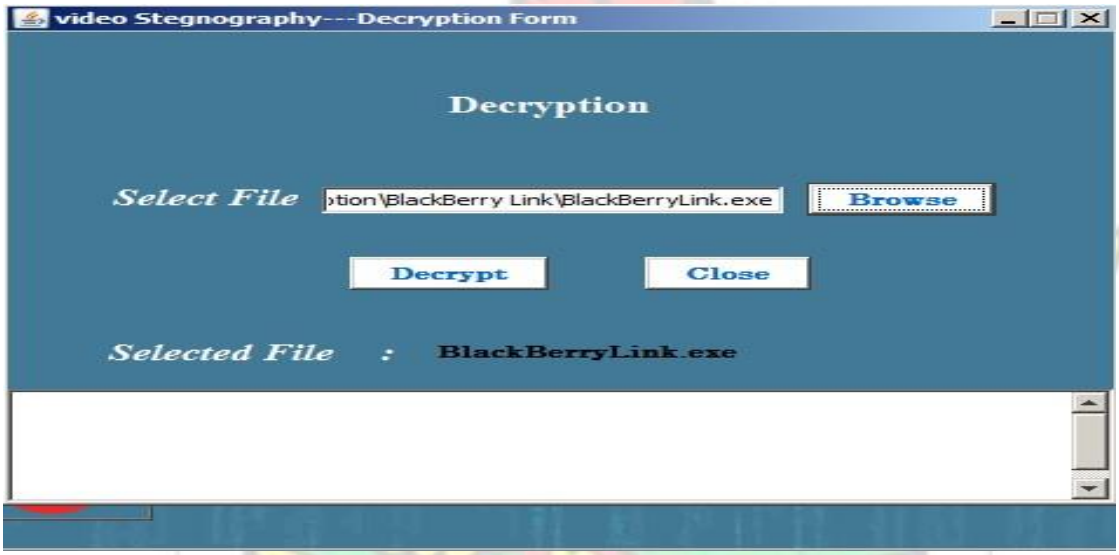

Figure 4.5: Decryption Page

4.1.3 Compression Menu

After encryption is completed, compression is applied**.** In order that, the application is able to embed a larger amount of data, a compression technique was used. . The technique used in this study was the Huffman code compression. The Huffman algorithm is easy to implement and produces lossless compression. When this compression is applied on text, it increases the volume of text to be hidden indirectly.

Huffman compression belongs into a family of algorithms with a variable codeword length. The basic idea behind the algorithm is to build the tree bottom-up whose leaves are labelled with the weights.

At the compression page, an encrypted file is browsed through and chosen from the computer or the location where it is saved. The compress button is pressed to start the process of compression. As soon as the compression is completed, a folder named "Stegan File " is automatically generated at the computer's documents folder containing the compressed file. The path showing the file location is displayed on the interface for easy location. At the recipient end, the compressed file is uncompressed before the process of decryption is applied. When the file is uncompressed, the path showing the location of the umpressed file is created on the uncompressed page. The fig. 4.6 and fig. 4.7 show the compression and decompression pages respectively.

Figure 4.6: File Compression Page

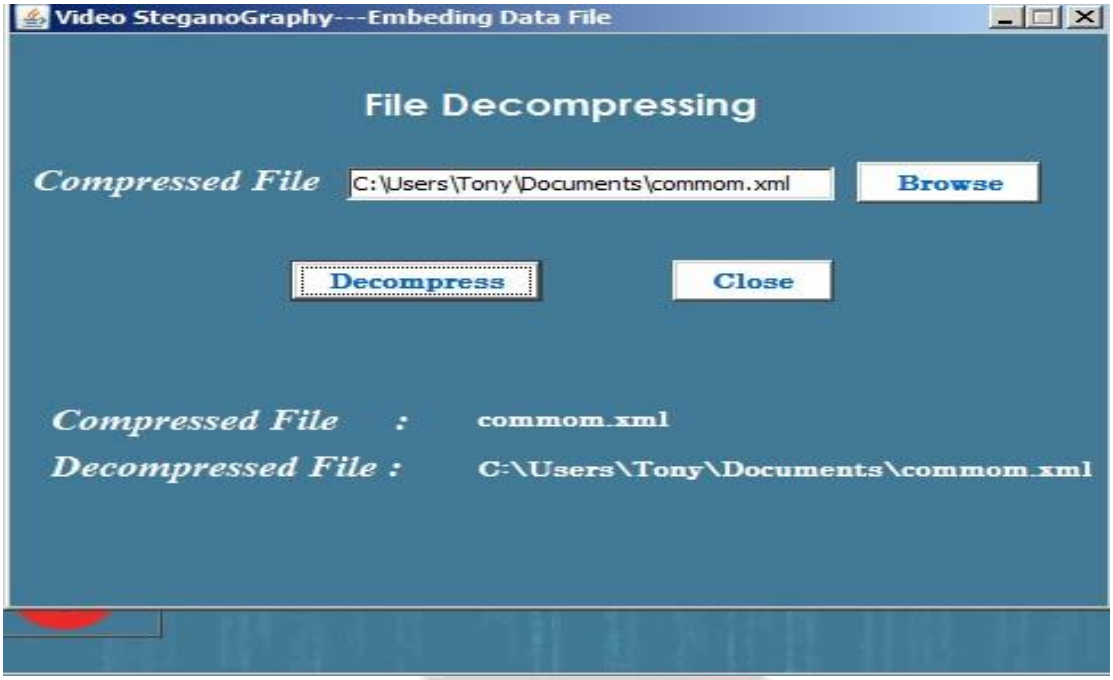

Figure 4.7: Decompression page

4.1.4 Steg Utility Menu

The actual process of video steganography takes place. The steg utility menu consist of the enbed and the de-embed pages. This process was implemented using LSB. The LSB based Steganography was, used to embed the secret data in to the least significant bits of the pixel values in a cover image. LSB is the lowest bit in a series of numbers in binary. Fig. 4.8 and fig. 4.9 show the embed and the de-embed pages respectively.

Figure 4.8: Embedding Page

Figure 4.9: De-embedding Page

The process of embedding requires the compressed encrypted file to be chosen from its location. The cover video in which the file is to be embedded is also chosen. This application works with a wide range of video file extensions including the two most popular video file extensions, AVI and MPEG-4 (MP4). When the compressed encrypted file is completely embedded, a folder named “Stegan file ” is created on the desktop. At the recipient end, the de-embed separate the file from the video and put the file as the same location of the video. The embed process produces the stego video. Fig 4.10 and fig 4.11 show the original and stego videos respectively.

Figure 4.10: Original video

Figure 4.11: Stego Video

4.1.5 Send File Menu

The resultant stego video is transmitted through a communication channel to the intended recipient. The video can be sent through either e-mail address or IP address. When sending through e-mail, the simple mail transport protocol must be configured. However, a recipient of a message through the IP address must be located within the same network as the sender. Fig 4.12, fig 4.13 and fig 4.14 show the e-mail, SMTP setting and the IP address pages respectively.

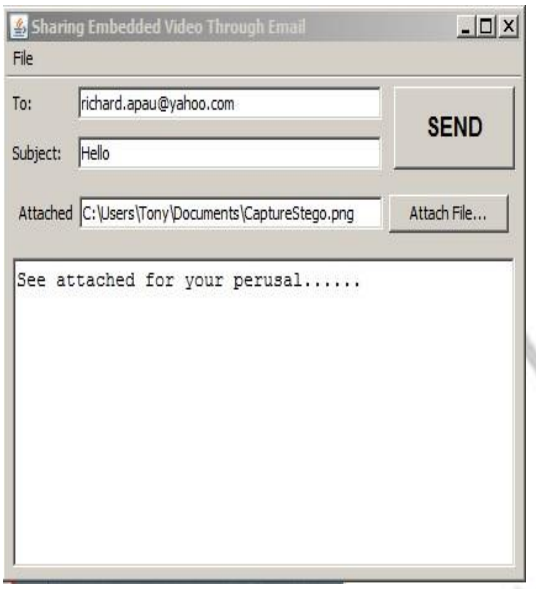

Figure 4.12: E-mail Page

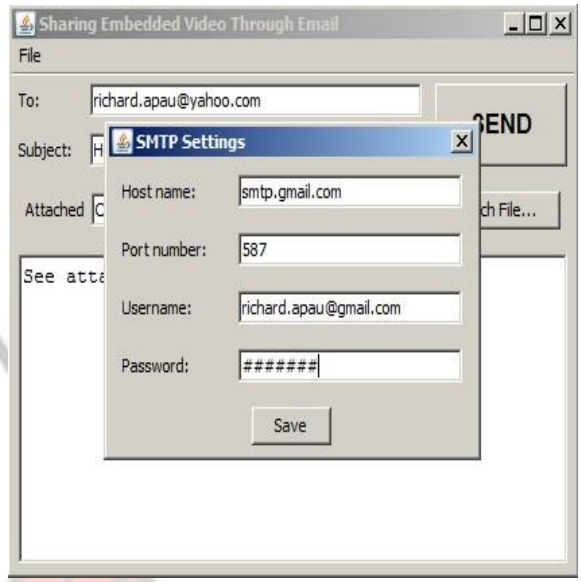

Figure 4.13: SMTP Setting

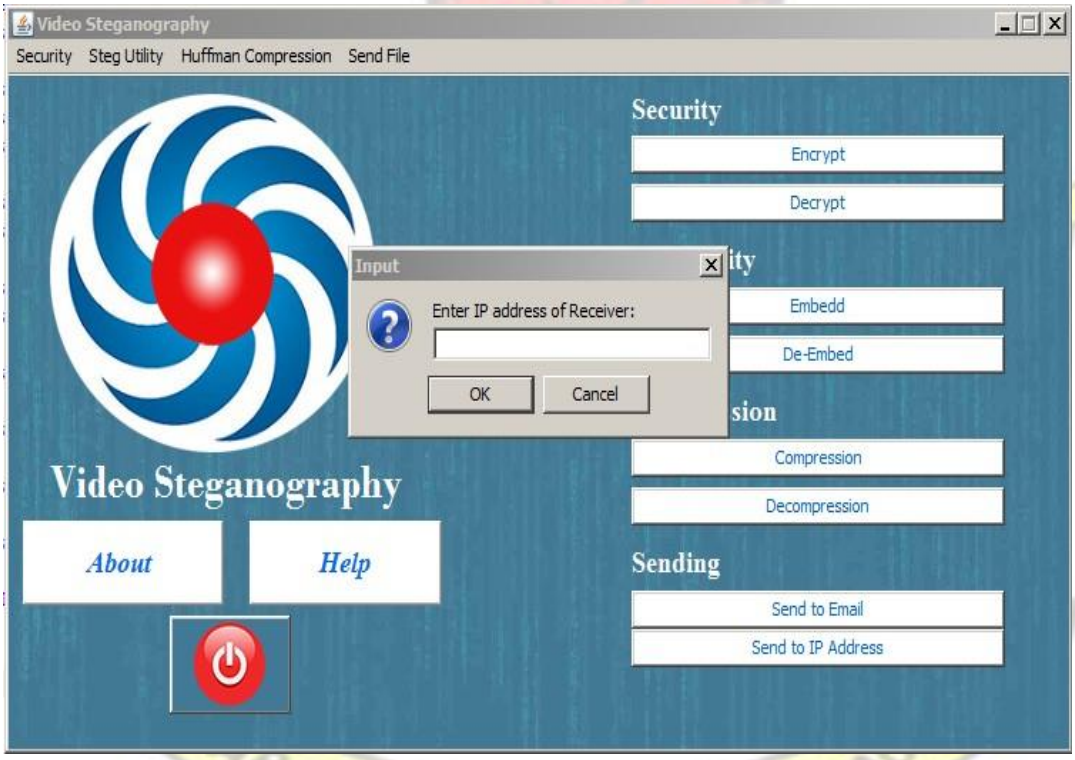

Figure 4.14: IP Address Page

4.2 Results and Analysis of Proposed Model/System

Steganographic applications are mainly evaluated on embedding capacity and imperceptibility. Imperceptibility is the inability of an intruder to detect and read a message embedded in a video. In these results, the stego video was implemented in a MATLAB software to generate the properties of the stego video. The application has been applied on a wide range of files, including images, database files, word files, pdf file and many more. In order to ensure that, the file transferred reach its destination unaltered, a bit error rate (BER) analysis was performed using the proposed model. The results were compared to a previous work (Kaur and Singh, 2015) and the proposed system proved far better. The table 4.1 shows the BER results for different file sizes.

Table 4.1: Table showing BER Results

File Size (byte) proposed work	**File Size(byte) prevous work**	**Proposed Work**	**Previous Work**
1,785	1,710	0.0190	0.0194
26, 700	26, 265	0.0182	0.0185
53, 980	52,044	0.0194	0.0195

The results in table 4.1 show that, the proposed system adopted in this research performed better as compared to a previous work. The previous work used Elliptic Curve Cryptography and Huffman code compression with LSB insertion algorithm whiles the proposed work used RSA algorithm and Huffman code compression with LSB algorithm. Fig 4.15 shows the graph representation of the proposed work and the previous work conducted.

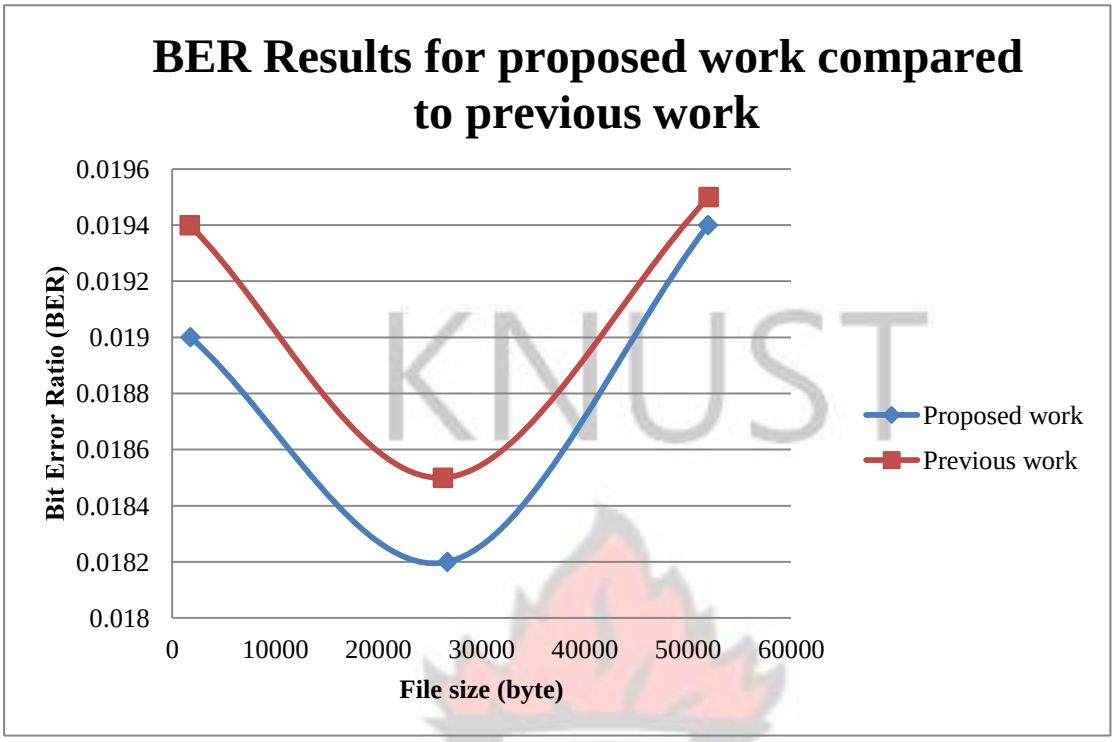

Figure 4.17: BER results of proposed work and previous work

The GRAPH results in fig 4.15 shows that the system performed better in terms of the number of bit errors recorded. From table 4.1, it can be observed that the file sizes embedded in the proposed work were at all times bigger than the previous work, yet the performance in terms of BER was still better in the proposed work than the previous work.

The technique proposed in this study was analysed on seven different cover videos. The videos are SITI.mp4, SOC 360.mp4, SOC 366.mp4, GEOG 366.mp4, Man.avi, Saddest.avi, and Youtube.avi . These seven cover videos were analysed with a common text file. The resultant invisibility of the hidden file is shown by comparing the stego video with the cover video. There was virtually no loss in quality and also the presence of a hidden message in the video was proven to be undetected.

Table 4.2 and Table 4.3 show the results obtained from the video properties.

Table 4.2: Video Properties

Video File	Resolution (W*H)	Number of Frames	Total Bit Rate (kbps)	Length(seconds)	Size(MB)
SITI.mp4	640*360	40	954	711	81
SOC 360.mp4	1280*720	45	909	1168	126
SOC 366.mp4	720*360	44	751	1203	108
CSM366.mp4	540*297	39	1215	990	143
Man.avi	720*480	57	1806	532	48.2
Saddest.avi	426*240	38	379	319	61.4
Youtube.avi	426*212	32	369	822	99.1

Table 4.3: Results Obtained

Video File	Number of Frames	Number of characters in text file	Embedding Capacity	PSNR	MSE
SITI.mp4	40	1,200	856360	60.3565	0.0599
SOC 360.mp4	45	1,200	998576	63.3886	0.0298
SOC 366.mp4	44	1,200	902600	62.0030	0.0410
CSM366.mp4	39	1,200	699400	59.6923	0.0698
Man.avi	57	1,200	987580	66.1997	0.0156
Saddest.avi	38	1,200	504780	58.5932	0.0899
Youtube.avi	32	1,200	412560	58.1351	0.0999

From the results in table 4.3, it can be observed that when RSA algorithm is combined with Huffman code using LSB insertion algorithm in video steganography

by employing JAVA as the tool for steganography, the PSNR values are high. It also gives high embedding capacity without the video losing it quality. The high embedding capacity explains the reasons behind the low MSE and the high PSNR values. From the results, it can be realised the proposed system works better than previous works conducted as its average embedding capacity of 765979 is far higher than that of (Kaur and Singh, 2015) which was 230400, and also that of (Deshmukh and Rahangdale, 2014) which was 497670. Furthermore, the PSNR average value of 61 is an indication that, the proposed system is good. Again, Kaur and Singh (2015) recorded average PSNR of 52 whiles Deshmukh and Rahangdale (2014) had an average PSNR of 58. The PSNR value of 61 is an indication that, the security of the stego video is very high. The MSE values obtained show that, the bit error rate is minimal and the difference between the pixels of the received video and the original video is insignificant.

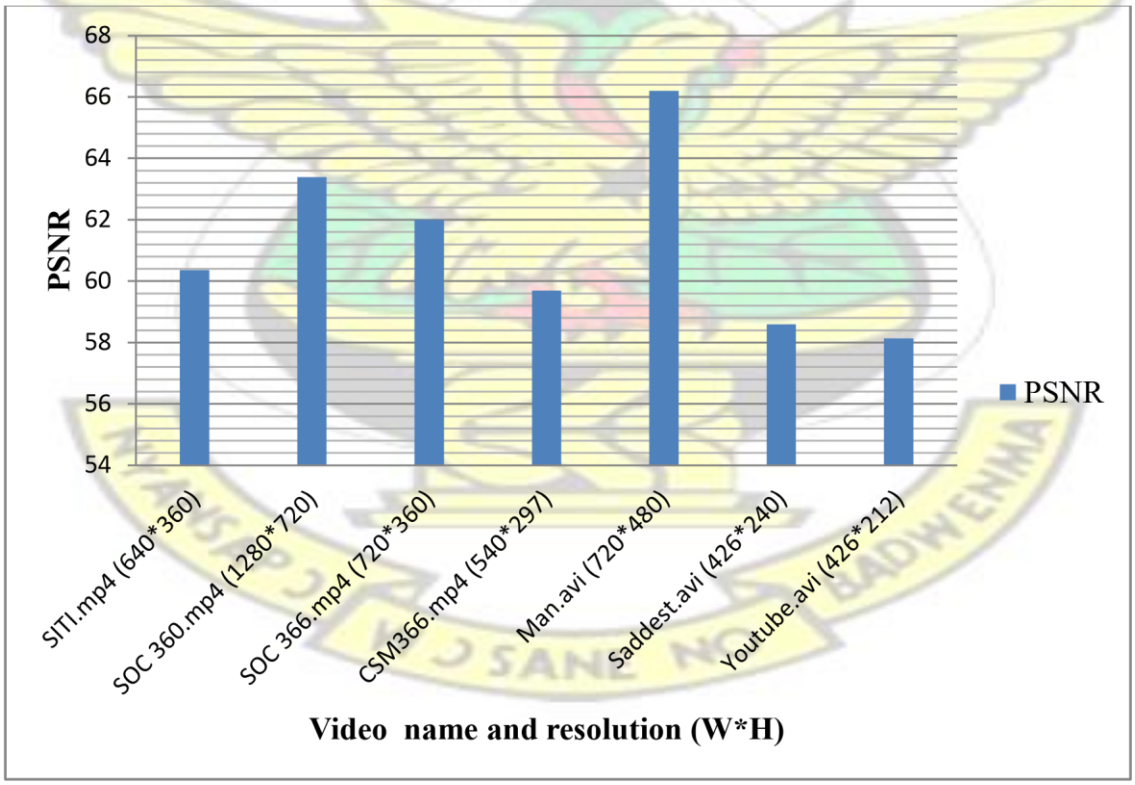

Figure 4.16: PSNR vs. Video Resolution

Fig 4.16 demonstrates the differences in PSNR with respect to the video capacity. Different values of PSNR are given to show the video quality. Differences in the video resolutions resulted in the PSNR variations.

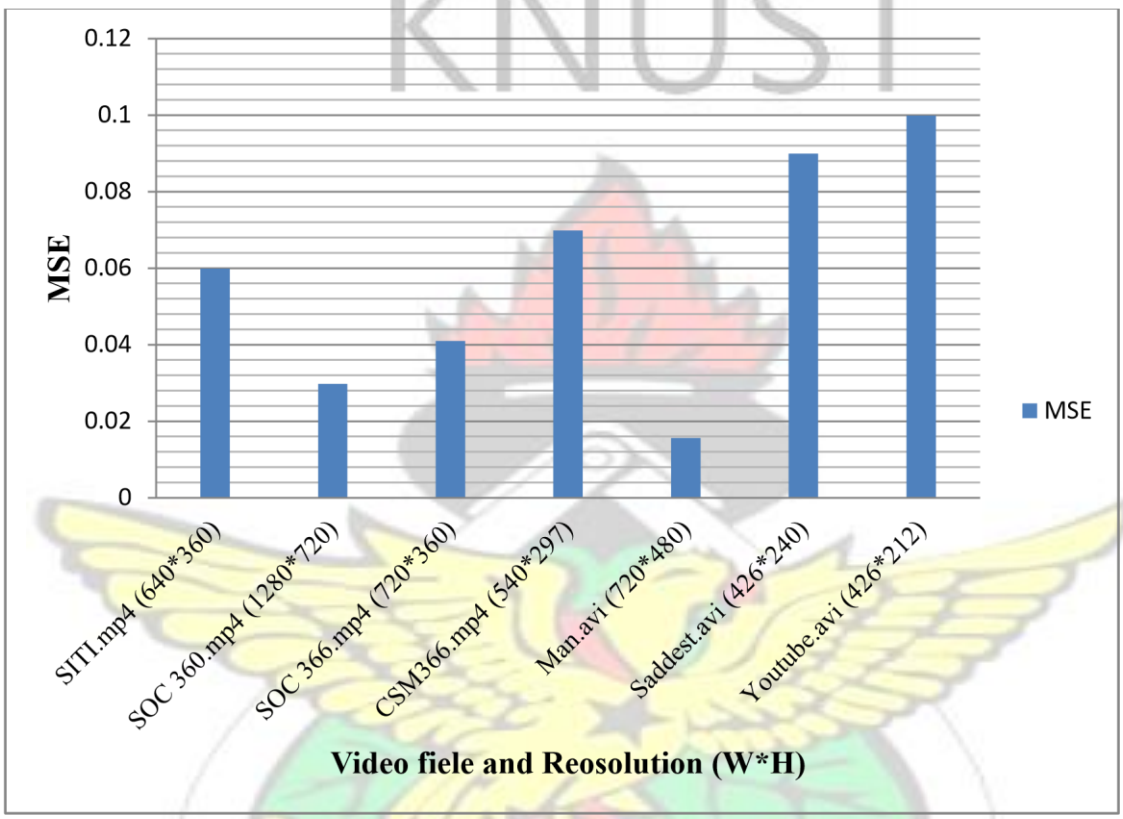

Figure 4.17: MSE vs. Video Resolution

Fig 4.17 shows the variation in MSE with different video resolutions. The MSE is a mean square error between the cover frame of the original video and the cover frame of the stego video.

The proposed system was analysed with different file sizes in the same cover video. This was done to test the quality and the security of the system with small and large file sizes. In table 4.4, text files of different sizes were embedded in the same cover video to determine the variations in PSNR and MSE.

Table 4.4: PSNR and MSE variations with varied file sizes

Video File	File Size	PSNR Variation	MSE
SOC 360.mp4 (1280*720) 45 frames	123 chars (File A)	68.2185	0.0098
	633 chars (File B)	68.0448	0.0102
	867 chars (File C)	65.1423	0.0199
	1,200 chars (File D)	63.3886	0.0298

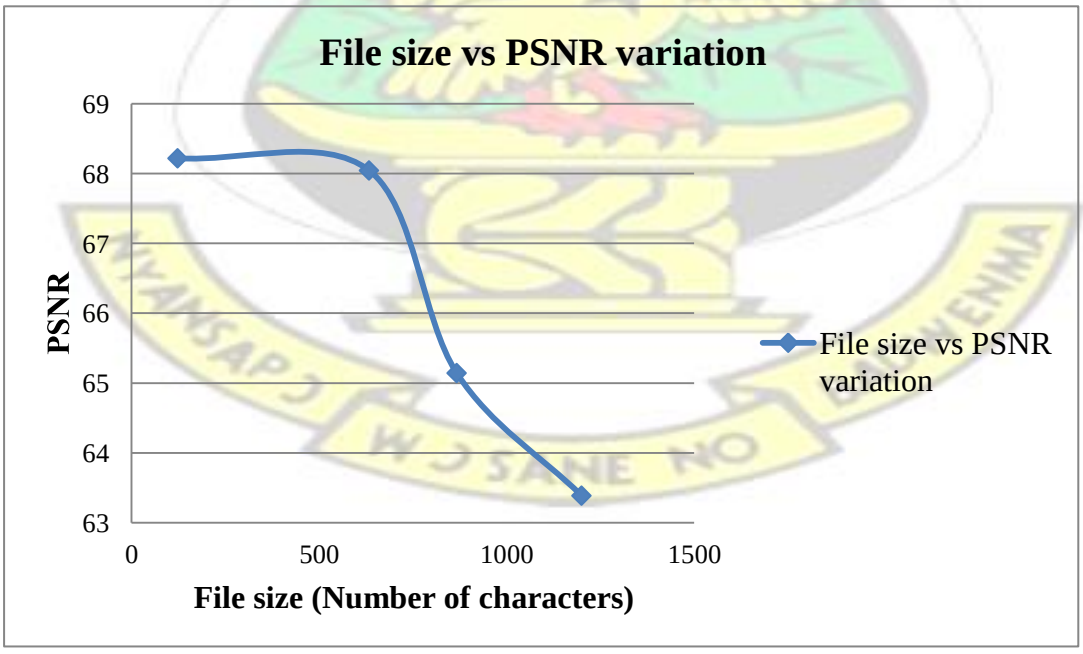

Figure 4.18: PSNR and File Variations

The GRAPH in fig 4.18 shows that , as the file size of the secret embedded message increases, there is variation in the PSNR values. The PSNR values decreases as the file size increases. This simply means, as more files are embedded, the quality of the video will be low and that will compromise the security of the system. Though the proposed system has high embedding capacity, any file size which is chosen and beyond the allowable limit or threshold will distort the video. PSNR is an abbreviated form of Peak-Signal to Noise-Ratio which is a video quality metric that measures the quality of the stego video by comparing the frame of the original video and the frame of the stego video.

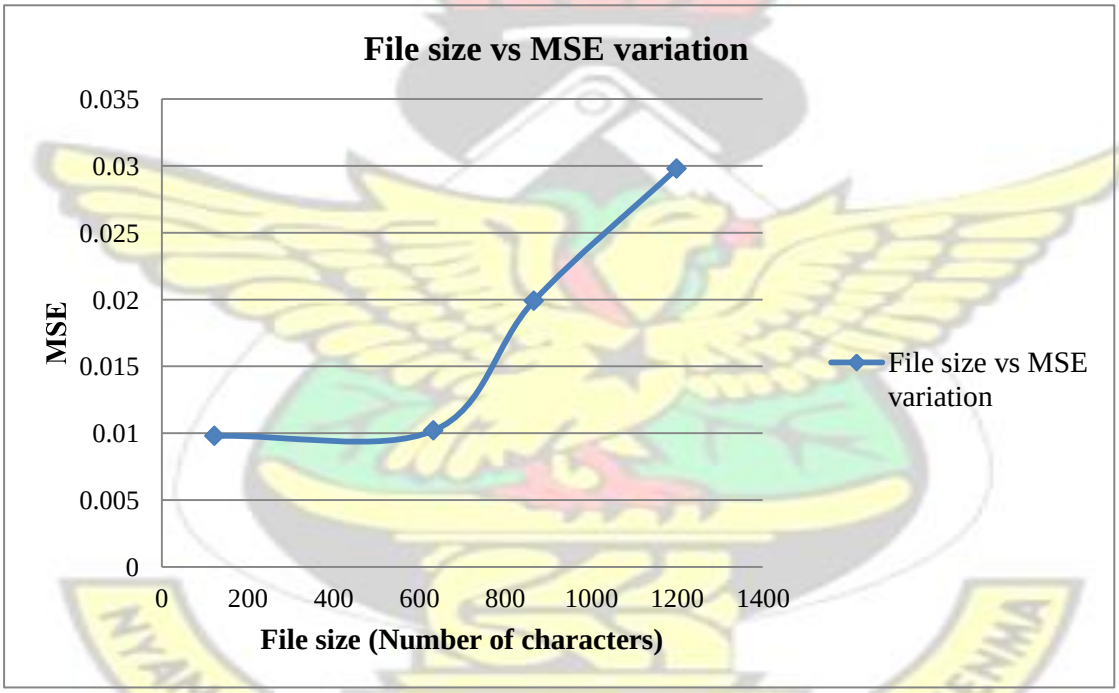

Figure 4.19: MSE Variation with different file sizes

The GRAPH in fig 4.19 shows that, as the file size of the secret embedded message increases, there is variation in the MSE values. The MSE values increase as the file size increases. This simply means, as more files are embedded, there will be distortion in the video. Since distortions are perceptible to the human eye, the security

of the system would be broken. The mean square error, abbreviated MSE is the measure of distortion between the frame of the original video and the frame of the cover video. The objective of providing a high security system that makes it difficult for eavesdroppers to detect hidden message is achieved as a results of the low MSE and the high PSNR values.

Most steganographic applications or software currently in the market increase the size of the resultant file after embedding. Also most of them accept video input of .avi extensions only. One major outcome this research was expected to achieve is to use most video files extension in existence like mp4, mpeg, flv and not only avi.
Objectively the quality of the video should remain same irrespective of file type. Conceptually, the resultant file size is supposed to increase when using other embedding techniques. This is effectively so, because noise is being added to the low bits which will always increase the size.

The results and analysis of the proposed system revealed that when a file is embedded in a cover video, the properties of the original video and the stego video are the same. The resolution, length, number of frames, and bit rate and size of the stego video is the same as the original video. This revelation brings to light the efficiency and the effectiveness of the proposed system. The size of video in steganography depends on many factors such as embedding algorithm, video file format, compression techniques and container. The size of a video cannot be same when the video has been changed, unless appropriate compression and embedding algorithm is applied to re-encode the video to get the same size. The system proposed in this study achieved same size after embedding by employing LSB and Huffman code to reencode the video. The principle of LSB is that, the data is stored in an existing bits of the video frame, no

additional bytes is added. Huffman code also uses variable length to encode the bits of the message string. To this end, a compression technique utilised in this proposed system necessitated the larger embedding capacity. The table 4.5 shows the comparison of Original Vieo Size and Stego Video Size.

Table 4.5: Comparison of Original Vieo Size and Stego Video Size

Video File	**Resolution (W*H)**	**Number of frames**	**Number of Characters**	**Original Video Size(MB)**	**Stego Video Size**
SITI.mp4	640*360	40	1200	81	81
SOC 360.mp4	1280*720	45	1200	126	126
SOC 366.mp4	720*360	44	1200	108	108
CSM366.mp4	540*297	39	1200	143	143
Man.avi	720*480	57	1200	48.2	48.2
Saddest.avi	426*240	38	1200	61.4	61.4
Youtube.avi	426*212	32	1200	99.1	99.1

The results in table 4.5 shows that, the size of the stego file, video resolution and other properties remained same. It can therefore be observed that, the size of the stego video is equivalent to the original cover video size, hence the need for combining RSA, Huffman code compression and LSB insertion.

Interestingly, the compression algorithm of the proposed system can be used to reduce the size of any file without the entire process of steganography. This can be utilised to create more storage space. Huffman code compression is applied to some

different file sizes to know the extent of reduction in size. Table 4.6 shows the results of the compression.

Table 4.6: Compression of Same File Type with different Sizes

File Type	Original File Size (MB)	Compressed File Size(MB)	Percentage Reduced (%)
Text file (.txt)	125	67	46.4
	118.3	65.1	45
	82.2	59.1	28.1
	50	38	24

The results in table 4.6 show that, as the file size increases the percentage of reduction in size also increases. It can therefore be observed that, the larger the file size, more compression is achieved. However, different file types compresses differently.

Table 4.7: Compression of Different File Type with the same File Size

File Type	File Size	Compressed Size	Percentage Reduced
Text (.txt)	125	67	46.4
Database (.sql)	125	64.5	48.4

Image (jpeg)	125	69.3	44.6
PDF (.pdf)	125	67.9	45.7

The results in table 4.7 shows that different file types compresses differently. Database files (.sql) have more compression ability, followed by text files (.txt), DPF files (.pdf) and lastly Image files (jpeg). Ordinarily, image files are less compressed due to its binary nature. Nonetheless, the focus of this research is not on which file type compressed better than the other. The objective is to show that, all file types experienced some level of compression.

4.3 Performance Evaluation of Proposed System

As demonstrated in fig 3.2, steganographic application or systems are evaluated on some basic views. The metrics for performance evaluations are security, capacity and robustness. The proposed system has numerous operational merits. Firstly, the system achieved a great embedding capacity. The proposed system has an average embedding capacity of 765979 which is the highest as compared to previous works. The maximum embedding capacity is approximately 71%. This means that the proposed system is able to take in large size of data without any noticeable distortion. Secondly, the proposed system has the advantage of more security. Though people can download the video, they cannot view the content unless the intended recipient. The imperceptibility of the proposed system makes it more secure to attacks. There is no distortion observed. In the event that distortion is noticed it may be taken as shortage of quality during video taking. The security of the system is attributed to the algorithms

for encryption and embedding. RSA algorithm is proven to be the most secured cryptographic algorithm. LSB insertion algorithm is also much secured when large size file is to be embedded.The third performance criterion upon which the system is evaluated is robustness. The proposed system is very robust and can withstand high embedding capacity without the video losing its quality. The PSNR average value of 61 is an indication that, the proposed system is robust. The proposed system achieved a very high PSNR values and low MSE values indicating that, the quality of the stego video isn't different from the original video.

4.4 Summary Of Findings

The results obtained from the proposed system revealed some interesting findings. It is observed that the proposed system has low computational complexity. That is, it computationally less expensive to hide and extract the data. The low computational complexity is as a result of the use of LSB for embedding. LSB is believed to have low computational complexity and high embedding capacity. The proposed system is characterized with robustness, high embedding capacity and high security. The embedding capacity achieved in the proposed system is higher than anticipated. This shows that the proposed system is not prone to attack by hackers and intruders. The proposed system has the ability to withstand large embedding capacity without distortion in video quality. The system is very consistent and platform independent.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.0 Introduction

This final chapter closes the discussion of the study. It talks briefly about steganography and cryptography in general. Following the discussion, the findings of the study are also mention as well as the achieved of objective of the study.

Conclusions and recommendations are also drawn from the study.

5.1 Conclusion

As the internet revolution progresses steadily, hackers and attackers may reveal the content of secret or sensitive information of individuals or organisations. The most appropriate scientific remedy to the problems is steganography, data compression and cryptography. The role of steganography is to hide the existence of a message by employing some communication techniques such that the hidden message is not seen or discovered. Cryptography however, hides the content of the message whereas compression reduces the size of the hidden data.This research brings to light the concept of effectively combining steganography, compression and cryptography specifically RSA cryptographic algorithm, Huffman code compression with LSB insertion. The preference of RSA over any other cryptographic algorithm is due to its ability to provide better security for large file size thereby reducing computational complexity. From the

results obtained in this research, it can be concluded that when steganography is combined with cryptography and compression, higher levels of security, capacity and robustness are achieved. The distortion experienced in this study is negligible; therefore the study achieved increased security by the high PSNR values and low MSE and BER values. Again, in order not to send files of enormous or large size, a compression algorithm was introduced and implemented in this study. A lossless compression algorithm popularly called Huffman coding was used on the message to be hidden to increase the amount or the capacity. Hence, for a higher security the message is encrypted and for more embedding capacity appropriate compression technique is used to get encrypted compressed message for embedding. Lastly, most of the steganographic applications already in existence can hardly handle all type of video file sizes. The most commonly one normally used is the .AVI. The proposed system deals with different type of video files including .AVI, MP4, MPEG and .flv. The use of RSA encryption and Huffman code with LSB in video steganography is contemporary field and has stupendous purview of research or study.

5.2 Recommendations

After going through the study successfully, I make the following recommendations for the betterment of message security, robustness and capacity.

- RSA algorithm is generally slow in speed when implemented on CPU system, a study should therefore be conducted to see how possible best to enhance the speed of RSA algorithm for CPU implementation.
- Since spatial domain which LSB belongs to is susceptible to noise, further research should be conducted on how to make it noise free for high level security.

- To further increase the security of data in the near future, studies must be conducted on how to increase the security of the communication medium for complete optimal security.

REFERENCES

Ahmed, Z. H. (2014). *Comparison of data hiding using LSB and DCT for image* (Doctoral dissertation, Universiti Tun Hussein Onn Malaysia).

Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M. (2012). A survey on steganography techniques in real time audio signals and evaluation. *International Journal of Computer Science Issues (IJCSI), 9*.

Al-Vahed, A., & Sahhavi, H. (2011). An overview of modern cryptography. *World Applied Programming*, *1*(1), 3-8.

Balgurgi, P. P., & Jagtap, S. K. (2012, January). Audio steganography used for secure data transmission. In *Proceedings of International Conference on Advances in Computing* (pp. 699-706). Springer India.

Basheer, R & Safiya M.K (2014).Video data hiding in selective pixels of forbidden zone using mapping function. International Journal of Advanced Computer Technology (IJACT).ISSN:2319-7900.

Bateman, P., & Schaathun, H. G. (2008). Image steganography and steganalysis. *Department Of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom, 4th August*.

Bhaumik, A. K., Choi, M., Robles, R. J., & Balitanas, M. O. (2009). Data hiding in video. *International Journal of Database Theory and Application*, *2*(2), 9-16.

Bodhak, P. V., & Gunjal, B. L. (2013). Improved Protection In Video Steganography Using DCT & CDCS. International Journal of Scientific & Engineering Research, Volume 4, Issue 11, ISSN:2229-5518

Bodhak, P. V., & Gunjal, B. L. (2012). Improved protection in video steganography using dct & lsb. *International journal of engineering and innovative technology (IJEIT)*, *1*(4).

Budhia, U., Kundur, D., & Zourntos, T. (2006). Digital video steganalysis exploiting statistical visibility in the temporal domain. *Information Forensics and Security, IEEE Transactions on*, *1*(4), 502-516.

Chae, J. J., & Manjunath, B. S. (2000). Data hiding in video. In *Image Processing, 2000. ICIP 99. Proceedings. 1999 International Conference on* (Vol. 1, pp. 311-315). IEEE.

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography, second edition*. Morgan Kaufmann.

Das, S., Das, S., Bandyopadhyay, B., & Sanyal, S. (2011). Steganography and Steganalysis: different approaches. *arXiv preprint arXiv:1111.3758*.

Dengre , A. R., Gawande, A. D. Deshmukh, , A. B.(June, 2013). Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video . International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(6), 2319 – 4847.

Deshmukh, P. R. & Rahangdale, B. (2014).Data Hiding using Video Steganography. International Journal of Engineering Research & Technology (IJERT).ISSN: 22780181.Vol. 3 Issue 4,

Dhupar, K. K. (n.d). Data communication.http://www.di.unipi.it/~bonucce/11Datacommunication.pdf (accessed 2015 November 27).

Diffie, W. & Hellman, M. (1976). "New Directions in Cryptography" (PDF). IEEE Transactions on Information Theory. IT-22: 644–654.

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, *2012*(1), 1-16.

Elbayoumy, M., Elmogy, M., Abouelfetouh, A., & Elhadary, R. (2014). A Proposed Technique For Hiding Data Into Video Files. *International Journal of Computer Science Issues (IJCSI)*, *11*(2), 68.

Elminaam, D. S. A., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *IJ Network Security*, *10*(3), 216-222.

Eltyeb E. A bed Elgabar,(2013)"Comparison of LSB Steganography in BMP and JPEG Images", International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307, Volume-3, Issue-5.

Encyclopeadia Britannica (n.d) "Cryptology"http://www.britannica.com/topic/cryptology (accessed 2015 December 02).

Furht, B., Muharemagic, E., & Socek, D. (2005). An Overview of Modern Cryptography. *Multimedia Encryption and Watermarking*, 31-51.

Garg, N., Yadav, P. (2014) Comparison of Asymmetric Algorithms in Cryptography ,International Journal of Computer Science and Mobile Computing, IJCSMC Vol.3 Issue.4,pg. 1190-1196.

Gauravaram, P., & Knudsen, L. R. (2010). Cryptographic hash functions. In *Handbook of Information and Communication Security* (pp. 59-79). Springer Berlin Heidelberg.

Gupta, H., & Chaturvedi, S. (2014). Video Steganography through LSB Based Hybrid

Approach. *International Journal of Computer Science and Network Security*, *14*(3), 100.

Gupta, R., Jain, A., & Singh, G. (2012). Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics. *International Journal of Computer Science and Information Technologies*, *3*(3), 4366-4370.

Hariri, M., Karimi, R., & Nosrati, M. (2011). An introduction to steganography methods. *World Applied Programming*, *1*(3), 191-195.

Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.364.3275 accessed 30 november 2015.

Jain, V. (2012). Public-Key Steganography Based On Modified LSB Method. *Journal of Global Research in Computer Science*, *3*(4), 26-29.

Joselin.J., Brintha, S.J., Babu, M. (2015). Role of Digital Signature in Network Security and Cryptography (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 893-895.

Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography*. CRC Press.

Kaur, R. and Singh, T. (2015). Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography. International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 18

Ker, A. D. (2007). Steganalysis of embedding in two least-significant bits. *Information Forensics and Security, IEEE Transactions on*, *2*(1), 46-54.
Kessler, G. C. (2015). An overview of cryptography. http://www.garykessler.net/library/crypto.html#purpose (accessed 2015 November 11)

Khosla, S., & Kaur, P. (2014). Secure Data Hiding Technique using Video Steganography and Watermarking. *International Journal of Computer Applications*, *95*(20).

Khot, R. & Patil, A.S. (2015). Review Paper on Different Types of Steganography. International Journal of Research in Electronics and Computer Engineering (IJRECE) VOL. 3 ISSUE 2 ,ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

Kour, H. & Kaur, S. (2015).Data Hiding Using MLSB Steganography. International Journal of Advanced Research in Computer Science and Software Engineering. Page |994, Volume5, Issue 1,ISSN: 2277 128X

Kumar, R., Shinde, P. R., & Prajapati, G. (2014). Implementation of Data hiding scheme in video.International Journal of Engineering and Innovative Technology (IJEIT).ISSN: 2277-3754,Volume 4, Issue 1

Kundalakesi,M., Sharmathi.R, Akshaya.R (2015) Overview of Modern Cryptography. International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 6 (1), 350-353.

Laskov, P. (2015) Introduction to Computer Security :Foundations of Cryptography. Wilhelm Schickard Institute for Computer Science. http://www.ra.cs.unituebingen.de/lehre/ss11/introsec/03-crypto.pdf (accessed 2015 Deember 01).

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *Wireless Communications, IEEE*, *17*(1), 51-58.

Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2012). Principles and overview of network steganography. *arXiv preprint arXiv:1207.0917*.

Malde, M. P., & Admuthe, M. L. (2013) Data Hiding In Motion Vectors of Video.International Journal of Advanced Research in Computer and Communication Engineering.Vol. 2, Issue 11.

Mathe, R., Atukuri, V., & Devireddy, S. K. (2012). Securing Information: Cryptography and Steganography. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4251 – 4255.

Mazumder, J. A., & Hemachandran, K. (2013). A high capacity and secured color image steganographic technique using discrete wavelet transformation. *International Journal of Computer Science and Information Technologies*, *4*(4), 583-589.

Mohanta, H. K. (2014). Secure Data Hiding using Elliptical Curve Cryptography and Steganography. *International Journal of Computer Applications*, *108*(3).

Natarajan, S., Ganesan, M., & Ganesan, K. (2011). A novel approach for data security enhancement using multi level encryption scheme. *International Journal of Computer Science and Information Technologies*, *2*(1), 469-473.

Odeh, A., & Elleithy, K. (2012). Steganography in Arabic Text Using Zero Width and Kashidha Letters. *International Journal of Computer Science & Information Technology (IJCSIT)*, *4*(3), 1-11.

Oracle Corporation.(2002). DataSecurity Challenges .https://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm (accessed 2015 November 29).

Panford, J. K., Hayfron-Acquah, J. B., Riverson, K., Nueteh, J. T., & Bangura, A. B.(2015) Design Of An Enhanced Cryptographic Hash Function–Digest Length 512 Bits. Researchjournali's Journal of Computer Science, Vol. 2 | No. 4,ISSN 23495391.

Patidar, R., & Patidar K. (2015). Steganography Method Hiding Data in Video. International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 6 (1) , 237-239.

Paul Van De Zande (2001).The Day DES Died.Version 1.0. https://www.sans.org/reading-room/whitepapers/vpns/day-des-died-722 (accessed 2015 December 16)

Pevný, T., & Fridrich, J. (2008). Detection of double-compression in JPEG images for applications in steganography. *Information Forensics and Security, IEEE Transactions on*, *3*(2), 247-258.

Prabakaran, G., & Bhavani, R. A.(2012). High Capacity Video Steganography Based on Integer Wavelet Transform. http://scholar.google.com/scholar?hl=en&q=A+High+Capacity+Video+Steganography+Based+on+Integer+Wavelet+Transform.&btnG=&as_sdt=1%2C5&as_sdtp=(accessed 2015 November 8).

Qi, Q. (2013). *A Study on Countermeasures against Steganography: an Active Warden Approach* (Doctoral dissertation, University of Nebraska).

Ramalingam, M. (2011). Stego Machine–Video Steganography using Modified LSB Algorithm. *World Academy of Science, Engineering and Technology*, *74*, 502-505.

Rana, M. S., Sangwan, B. S., & Jangir, J. S. (2012). Art of Hiding: An Introduction to Steganography. *International Journal of Engineering and Computer Science*, *1*(1), 11-23.

Reddy, V. L., Subramanyam, A., & Reddy, P. C. (2013). A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography. *International Journal of Computer Applications (0975 8887) Volume*, *69*.

Rhoads, G. B. (2007). "Video Steganography".*U.S. Patent No. 7,242,790*. Washington, DC: U.S. Patent and Trademark Office.

Salomaa, A. (2013). *Public-key cryptography*. Springer Science & Business Media.

Sameerunnisa, S.K., Suhasini, K. S. & Kommu, S.(2015).Information Security of Video Steganography Utilizing RSA Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering.ISSN: 2277 128X,Volume 5, Issue 4.

Sarmah, D. K., & Bajpai, N. (2010). A new horizon in data security by Cryptography & Steganography. *IJCSIT) International Journal of Computer Science and Information Technologies*, *1*(4), 212-220.

Schwartz, M. (2010). History ofcommunications. IEEE Communications Magazine. http://www.lk.cs.ucla.edu/data/files/Kleinrock/An%20Early%20History%20Of%20The%20Internet.pdf (accesed November 27, 2015).

Shelke, M. F. M., Dongre, M. A. A., & Soni, M. P. D. (2014). Comparison of different techniques for Steganography in images. *International Journal of Application or Innovation in Engineering & Management*, *3*(2).

Shukla, C. P., & Singh, A. K. (2014). Secure Communication with the help of Encryption in Video Steganography.Current Trends in Technology and Sciences.ISSN: 2279-0535. Volume: 3, Issue: 6

Singh, K., Dhawan, S.& Kaur, J.(2014). Stegnography Using Interpolation and LSB With cryptography on Video Images.International Journal of Software and Web Sciences (IJSWS).ISSN (Print): 2279-0063

Singh, K.U. (2014) Video Steganography: Text Hiding In Video By LSB Substitution. International Journal of Engineering Research and Applications. ISSN : 2248-9622, Vol. 4, Issue 5(Version 1), pp.105-108

Somani, U., Lakhani, K., & Mundra, M. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on* (pp. 211-216). IEEE.

Sumathi, C. P., Santanam, T., & Umamaheswari, G. (2014). A Study of Various Steganographic Techniques Used for Information Hiding. *arXiv preprint arXiv:1401.5561*.

Swathi, A., & Jilani, D. S. (2012). Video Steganography by LSB Substitution Using Different Polynomial Equations. *Madanapalli Institude of Technology and science*.

Taqa, A., Zaidan, A. A., & Zaidan, B. B. (2009). New framework for high secure data hidden in the MPEG using AES encryption algorithm. *International Journal of Computer and Electrical Engineering (IJCEE), 1*(5), 566-571.

Tiwari, A., Yadav, S. R., & Mittal, N. K. (2014). A Review on Different Image Steganography Techniques. *International Journal of Engineering and Innovative Technology (IJEIT), ISSN*, 2277-3754.

Tyagi, S., Agarwal, A., Singh, R., & Singh, M. R. An Approach to Secure Larger Size Data with Authenticity and Integrity. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4) , 2010, 244-248.

Umamaheswari, M., Sivasubramanian, S., & Pandiarajan, S. (2010). Analysis of different steganographic algorithms for secured data hiding. *IJCSNS International Journal of Computer Science and Network Security*, *10*(8), 154-160.

Vahedi, E., Wong, V. W., & Blake, I. F. (2013). An Overview of Cryptography. *Crisis Management: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, 102.

Vegh, L., & Miclea, L. (2015) Improving the Security of a Cyber-Physical System using Cryptography, Steganography and Digital Signatures.International Journal of Computer and Information Technology (ISSN: 2279–0764),Volume 04,–Issue 02,

Venkateswaralu, S., Chhabra, N., & GNI, M. (2012). Secret Key Generation and Eavesdropping detection using Quantum Cryptography. International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (2) ,3348 – 3354.

Wajgade, V. M., & Kumar, D. S. (2013). Enhancing Data Security Using Video Steganography. *International Journal of Emerging Technology and Advanced Engineering*, *3*(4), 549-552.

Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. *Global Journal of Computer Science and Technology*, *10*(1).

Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005, March). Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on* (pp. 324-328). IEEE.

Xu, C., Ping, X., & Zhang, T. (2006, August). Steganography in compressed video stream. In *Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on* (Vol. 1, pp. 269-272). IEEE.