UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

VINCENT KIPNG'ETICH KOECH

REG NO: P58/76055/2012

RESEARCH PROJECT

Using Image Steganography Technique to Obscure Information from Unauthorized Users

A Case Study of *Smartware Solutions Ltd.*

SUPERVISOR: PROF. WAGACHA PETER WAIGANJO

A Project Report Submitted in Partial Fulfillment of the Requirements for the Award of Masters of Science in Computer Science of the University of Nairobi.

October 2016

DECLARATION

This research project is a presentation of my original research work. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

Student Name: **VINCENT KIPNG'ETICH KOECH** Registration No: **P58/76055/2012**

Signature: …….. Date: …….

In my capacity as supervisor of the candidate, I certify that the work reported in this research project was carried out by the candidate under my supervision.

PROF. WAGACHA PETER WAIGANJO

Signature: …….. Date: …….

DEDICATION

This study is dedicated to my parents; my mother, Esther Boit, and my late father, Joshua Boit, both of whom gave me the foundation of something they had never enjoyed in totality – education. Ever since then, I have been able to appreciate the value of reading and lifelong learning. To my mother, Esther, I owe you a great depth of "thank you" for the tireless support that you gave me including hope and wisdom to carry on, thanks a lot for consistently reminding me that "knowledge, wisdom, money and power is the name of the game". To my late father, Joshua, you could not witness my success because you were stolen from us by the cruel hand of death.

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to my supervisor Prof. Peter Waiganjo you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career has been priceless.

I also wish to acknowledge my sincere appreciation to the following people without whom this research work would not have been successful. It may not be possible to mention all by names, but the following are singled out for their exceptional help. Without using any particular order, my profound gratitude goes to my other supervisors Dr. Samuel Ruhiu, Dr. Daniel Orwa, Mr. Christopher Moturi and Ms. Christine Mulanda without them this project would not have been successful. They accorded me the much needed scholarly guidance, instructive feedback and constructive criticisms. My indebtedness goes to my brothers John Koech, Philip Koech, Edward Koech, Weldon Koech and Charles Koech including their families for providing the necessary support. To my sisters Emily Boit and Evaline Boit including, their families for making me realize my dream and propping me up when all seemed to be in vain. To my brothers in law, Richard Maritim and David Cheruiyot for their motivational endeavors. To my cousins Robert Langat and Dr. Winrose Kirui including their families for paving the way in our family tree on academic endeavours. To my workmates and colleagues at KEMI for the support accorded to me during my study. Much appreciation goes my respondents for positively responding to research instruments at very short notice. I am grateful to all the research respondents, who provided me with the required information. It's not possible to mention by name all those who contributed to the completion of this project. Last but not least, I wish to express my dearest gratitude to my research assistants for your much-needed support in this study. Finally to the Almighty God who gave me strength and endurance.

Thanks to you all.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

CCTV **:** Closed Circuit Television

DCT **:** Discrete Cosine Transformation

DFT **:** Discrete Fourier Transformation

DWT : Discrete Wavelength Transformation

DSA **:** Digital Signature Algorithm

DT : Distortion Technique

EBE : Edges Based Embedding

ECB : Embedding in Coefficient Bits

GB : Gigabyte

GHTZ : Gigahertz

HS : Histogram Shifting

LC : Labelling Connectivity

LR : Lossless Reversible

LSB : Least Significant Bit

MF : Masking and Filtering

MPHD : Mapping Pixel to Hidden Data

PIB : Pixel Intensity Based

PVD : Pixel Value Differencing

RPE : Random Pixel Embedding

SDLC : System Development Life Cycle

SIH : Secure Information Hiding

SQL : Structured Query Language

SUS : System Usability Scale

TB : Texture-Based

TCP/IP : The Transmission Control Protocol / Internet Protocol.

DEFINITIONS OF CENTRAL TERMS

Cyphertext	Refers to encrypted data.
Cover image	An image containing an embedded message.
Cryptography	The art of protecting information in an unreadable format.
Encryption	The translation of data into a secret code.
Plain text	Refers to any message that is not encrypted - also called clear text.
Router	A networking device that forwards data packets between networks
Steganalysis	The art of discovering and rendering useless covert messages.
Steganography	A means of overlaying one set of information on another (a cover).
Stego image	The result of combining the cover image and the embedded message.
Stego text	It is the result of applying some steganographic process to a plain text.

ABSTRACT

Steganography is the art and science of invisible communication, which plays a vital role in information security. With the rise of the Internet, one of the most fundamental factors is the security of information. It involves hiding the fact that communication is taking place, by providing a method of writing hidden information in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography is usually implemented computationally, where cover works are tweaked in such a way that a secret message can be embedded within them. In order to embed secret data in a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because in the embedding process steganography actually replaces this redundant data with the secret message. In image steganography, the information is hidden exclusively in images.

An information hiding tool based on steganography technique that was developed to hide and retrieve information. The tool was deployed to an ICT security firm where clients gave their user input after interacting with the technique. Testing and evaluation of the tool was carried out by encrypting and decrypting information. Requirement gathering and analysis was carried out by using the findings from the case study to determine the requirements. The design was done using requirement specifications and analysis where a tool was selected based on the selected framework. Implementation was carried out by engaging a system in day-to-day business or organization's operations. Various tests were carried out and deployment of the tool was done by putting into use. Maintenance was also carried out to guarantee robustness.

The tool was able to meet the majority of information hiding requirements which included perceptual transparency, payload capacity, robustness and computational complexity. This method was considered valuable because apart from hiding information with a high threshold, it was also able to hide files regardless of the format. The majority of the ICT consultants had interacted with data hiding tools, mediums, domains and techniques, hence simplifying the study because they were able to make immense contributions pertaining to the improvement of the steganography tool. On testing, the technique was positively accepted by the ICT consultants together with the end users with a utility and usability scores of 76.59% and 71.67% respectively.

CHAPTER ONE – INTRODUCTION

1.1 Introduction

"Steganography" is a combination of two Greek words "*Seganos*", meaning secret/covered and "*graphy*" meaning drawing/writing. Therefore, steganography literally means, "*secret writing*", "*secret drawing*", "*covered writing*" or "*covered drawing*". "It is the art and science of hiding information such that its presence cannot be detected while a communication is happening" (Mulunda et al., 2013).

"One of the reasons that intruders can be successful is that in most cases the information they would wish to access from a system is in a form that they can read and comprehend. One solution to this problem is through the use of steganography", (Rahmani, 2014). In contrast to cryptography, the aim is not to keep out others from knowing the hidden information, but it is to keep out others from thinking that the information exists.

"The growing possibilities of modern communications needs a special means of security, especially on computer networks. Network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding and, more particularly, steganography", (Changder et al., 2010).

The study of image steganography was mainly supported by the fact that modern day social media technologies are driven by images. E.g. Facebook, twitter, Instagram, WhatsApp, Messenger, Telegram etc. Also most of the technological systems nowadays rely mainly on images i.e. Geographical Information Systems, Medical Imaging, CCTV Surveillance etc. All these is proves that technology relies mainly on images and hence is an area which should not be ignored.

1.2 Background of the Problem

"Steganography can be traced back to the ancient Greece, where they used to select messengers and shave their head, they would then write a message on their head. Once the

message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers' hair to see the secret message", (Babu et al., 2008).

"Another method was where someone would peel wax off a tablet that was covered in wax, write a message underneath the wax then re-apply the wax. The recipient of the message would simply remove the wax from the tablet to view the message", Babu et al. (2008).

"During World War II invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye", Babu et al. (2008).

"The modern formulation of steganography comes from the prisoner's problem proposed by, where two prisoners named *Alice* and *Bob* wish to communicate in secret to hatch an escape plan. All of their communications pass through a warden named *Eve* who will throw them in solitary confinement if she suspects any type of secret communication. So they must find out some way of hiding their secret message which gave the birth of steganography. The warden is free to examine all communication exchanged between *Alice* and *Bob* which can either be active or passive. An active warden will try to alter the communication with the suspected hidden information deliberately in order to remove the information whereas a passive warden takes the note of covered communication, informs the others and allows the message to pass through. The assumption that can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as the secret key steganography, otherwise, it is public key steganography", (Simmons, 1984).

1.3 Problem Statement and Research Purpose

1.3.1 Problem Statement

"The internet is one of the most powerful modern tools of information and communication technology and the underlying issue has always been the security of information. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may

also be necessary to keep the existence of the message secret. The technique that will be used to implement this is called steganography", (Petitcolas et al., 1999).

"Many governments have created laws to either limit the strength of cryptographic systems or to prohibit it altogether, forcing people to study alternative methods of securing information transfer", (Dunbar, 2002). "Business has also started to realize the potentials of steganography in communicating trade secrets or new product information", (Morkel et al., 2005).

1.3.2 Research Purpose

The research purpose was to design and deploy an information hiding solution that may help users sharing information while using computers so that such information may reach the target person(s) without being detected by other computer users when carrying out day to day tasks. Many solution developers, as well as military organizations and intelligence networks in the past, have attempted to build such solutions using cryptography in order to improve the level of privacy and secrecy when passing information. The main focus of this study, therefore, was to serve as a springboard to such solution developers, military organizations and intelligence networks who have struggled over the years wasting a lot of time as well as resources in the quest of pursuing solutions to such related problems.

1.4 Research Outcomes and Significance of the Study

1.4.1 Research Outcomes

"Technology has not only changed lives in Kenya but it has completely redefined the country's business and the social set-up", (Kabukuru, 2010). Although Kenyans did not invent computers, they have taken an unprecedented increase in the innovation of technology-oriented products such as the M-Pesa - money transfer service, Sportpesa - a sports betting solution, Uber – taxi booking service, M-Farm - a farm produce buying and selling tool and Kilimo Salama - an insurance compensation tool for farmers etc.

The outcome of this research work helped computer users to have easy, timely, effective and efficient access to information without others eavesdropping on it. In the long run, the

end product this study was able to develop and deploy a solution that can enable passing of information securely over the network.

1.4.2 Research Significance

"The significance of this study is to achieve a solution that will covert communication. So, a fundamental requirement of this steganography technique is that the hider message carried by stego-media should not be sensible to human beings", (Emmadi, 2015).

"It will also avoid drawing suspicion through the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas", (Amin et al., 2003). Examples of application areas may include storage, transmission and retrieval of sensitive information such as written wills, intelligence information, medical reports and trade secrets.

1.5 Research Objectives/Questions and Hypothesis

This project is based on a study that investigates information related problems faced by ICT security personnel, solution developers, military organizations and intelligence networks while passing information to others with the help of computer networks. The study, therefore, will be guided by the following objectives:-

1.5.1 Objectives

a) To identify the challenges faced by information users whenever they try to hide information from those who may not be authorized.

b) To develop an information hiding tool based on steganography technique that can be used to hide and retrieve information.

c) To test and evaluate the validity, utility and usability of the technique by encrypting and decrypting information, using images.

1.5.2 Justification of the Study

There is some evidence to support the need to provide quality ICT security solutions in organizations. A recent study of technical operations in organizations concurs with this observation, concluding that: "In every organization, computer users are affected in one way or another by the current ICT security breaches and threats" (Adams and Sasse, 1999).

1.5.3 Hypothesis

Most of the ICT consultants together with end users encounter difficulties when it comes to securing information from unauthorized access. Whenever this happens, such users sought for help, information whenever they are faced with such difficulties by sharing information with colleagues in the workplace, consulting the ICT experts and searching for solutions on the Internet, such solutions may only be optimal but not ideal.

1.6 Research Assumptions/Limitations

1.6.1 Study Assumptions

"The sender and receiver must have shared some secret information before exchanging any hidden data. Steganography assumes that prior information is shared by two communicating parties. Pure steganography however requires no prior information is shared by two communicating parties". (Katzenbeisser and Petitcolas, 2016).

1.6.2 Study Limitations

"A limitation is some aspect of the study that the researcher knows may negatively affect the results, but over may not be easy to control", (Mugenda and Mugenda, 1999). It is important to stress the exploratory nature of this study and its limitations, such limitations includes; lack of key technical leadership and expertise for identifying useful application areas, not all problems can be solved using steganography technique. This technique may not be applied in some exceptional cases where users must be willing to adopt the technique. Typical computer users may not necessarily be motivated, goal-seekers who prefer new ways of doing things.

CHAPTER TWO – LITERATURE REVIEW

2.1 Review of Previous Research

A literature review is a process of searching, collecting, analyzing and drawing a conclusion from all discussions and issues raised in the various body of relevant literature that simply makes use of other people work that are related to the topic of the project. These reviews can be books, journals, technical reports, conference proceedings, anonymous references, publications, web pages and e-books containing the topic that has been studied.

This chapter reviews the literature related to data hiding tools and techniques. It particularly focuses on the techniques used in data hiding tools, platform-level interoperability and examples of tools that can help ICT security firms. At the end, a technique for helping users to secure data is proposed.

2.2 Data Hiding Tools and Techniques

"Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems", (Khare et al., 2011). Digital "Steganography" techniques include:

2.2.1 Finger Printing

"Cryptography can be used for encrypting the fingerprint after scanning to ensure the safe transfer and storage. At the authentication stage, both stored during the enrolment and received by the server fingerprint data are being deciphered for the matching procedure. The result is the security of fingerprint data, as it cannot be used or modified without the correct decryption with the corresponding private key. In general, cryptography can be used also to monitor the integrity of the fingerprint to confirm the authenticity of the source", (Cox et al., 1997)

2.2.2 Biometrics

"It is the automated recognition of individuals based on their behavioural and biological characteristics. Biometric recognition means by measuring behavioural and biological characteristics of an individual in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning

procedure, in this way the identity of a specific user is determined. Because it is difficult to misplace, shared biometric identifiers are considered more reliable for recognition of a person than traditional token or knowledge based methods. Fingerprints are unique for each finger of a person, including identical twins. Face recognition is the process of identification of a person by their facial image", (Kumar and Begum, 2011).

2.2.3 Encryption

"In cryptography, the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, whereas steganography even conceals the existence of the message. The system is broken when the attacker can read the secret message. Breaking a steganography system need the attacker to detect that steganography has been used", (Amin et al., 2003)

2.2.4 Watermarks

"Watermarking pays most of its attribute to the robustness of the message and its ability to withstand attacks of removal, such as image operations, the audio operations in the case of images and audio files being watermarked respectively", (Licks and Jordan, 2005).

2.2.5 "Steganography"

Image "steganography" a better approach than cryptography. The purpose of image processing is to make the quality of an image better so that the required operations can be easily performed on it. Image steganography is performed on the desired format which is suitable. "Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter of the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it", (Doshi et al., 2012).

2.3 Steganography in Digital Mediums

2.3.1 Text Steganography

“Text steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts”, (Bennett, 2004). “Text steganography is believed to be the trickiest due to deficiency of redundant information which is present in image, audio or a video file. The structure of text documents is identical with what we observe, while in other types of documents such as in the picture, the structure of the document is different from what we observe. Therefore, in such documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output”, (Shahreza, 2007). “Unperceivable changes can be made to an image or an audio file, but, in text files, even an additional letter or punctuation can be marked by a casual reader”, (Bender, et al., 1996). “Storing text file requires less memory and it's faster as well as easier communication makes it preferable to other types of steganographic methods”, (Shahreza, 2007).

2.3.2 Audio Steganography

“The basic model of Audio steganography consists of Carrier, Message and Password. The carrier is also known as a cover-file, which conceals the secret information. The message is the data that the sender wishes to remain it confidential. The message can be plain text, image, audio or any type of file. The password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file”, (Jayaram, et al., 2011).

2.3.3 Video Steganography

“Video-Steganography refers to using video as a cover object to hide some secret message inside the video file by using some embedding procedure. A video contains a set of frames, which are played back at fixed frame rates based on the video standards. An image is a

collection of pixels and each pixel is a mixture of three primary colors RGB. Pixels in the image are shown row by row horizontally. Data hiding in the video/images gets less troubled as contrasted to other multimedia files. When data is hiding in an image its size increase. So compression techniques are required. Video/image size can be decreased by compression technique. There are two types, compression techniques lossy and lossless", (Doerr, and Dugelay., 2003).

2.3.4 Network Steganography

When taking a cover object as network protocols, such as TCP, UDP, ICMP, IP, etc., where the protocol is used as a carrier, is known as network protocol steganography. In the OSI network layer model, there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

2.3.5 Image Steganography

Image steganography takes the advantage of limited power of the human visual system (HVS). Here, unlike watermarks which embed added information in every part of an image, only the complex parts of the image hold added information. Straight message insertion will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in "noisy" areas of the image that will attract less attention.

2.3 Image Steganography Technique

2.3.1 Spatial Domain Method

"There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. The general advantages of the spatial domain technique is that there is less chance of degradation of the original image and more information can be stored in an image", Cox et al. (1997).

2.3.1.1 Least Significant Bit (LSB)

"The most common method used for hiding data in images are the 'Least Significant Bit (LSB) "Insertion technique" in which the LSB of the pixel values is replaced with the data to be encoded in binary form. Other techniques include the "Masking Technique" in which the original bits are masked with data bits and the 'Filtering Technique' in which certain

transformations are done on the image to hide data. The last two techniques hide data by marking an image in a manner similar to paper watermarks, but, there are some drawbacks with these methods which hinders their use", (Yang et al., 2008).

2.3.1.2 Pixel Value Differencing (PVD)

"Based on the fact that our human vision is sensitive to slight changes in the smooth regions, while can tolerate more severe changes in the edge regions, the PVD-based methods have been proposed to enhance the embedding capacity without introducing obvious visual artefacts into stego images. In PVD-based schemes, the number of embedded bits is determined by the difference between the pixel and its neighbour. The larger the difference amount is, the more secret bits can be embedded. Usually, PVD based approaches can achieve more imperceptible results compared with those typical LSB-based approach with the same embedding capacity. However, based on extensive experiments and analysis, we find that most existing PVD based algorithms perform bad to resist some statistical analysis even with a low embedding capacity, e.g. 10% bits per pixel", (Luo et al., 2011).

2.3.1.3 Edges Based Data Embedding Method (EBE)

"Edge Detection algorithm hides secret data into pixels that make up the extracted edges of the image carrier. The secret data can be of any type, and they are actually concealed into the three LSBs of the pixels of the image carrier, but not in every pixel, only in the ones that are part of the edge detected by the edge detection algorithm" (Bassil et al., 2012).

2.3.1.4 Random Pixel Embedding Method (RPE)

"This method hides data randomly, i.e., data is hidden in some randomly selected pixel. Random pixel is generated by using Fibonacci algorithm", (BrahmaTeja et al., 2012)

2.3.1.5 Mapping Pixel to Hidden Data Method (MPHD)

"Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbours are selected in a counter-clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbours lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbour pixels based on some features of that pixel", (Bhattacharyya et al., 2011).

2.3.1.6 Labelling or Connectivity Method (LC)

"A morphological processing starts at the peaks in the marker image and spreads throughout the rest of the image based on the connectivity of the pixels. Connectivity defines which pixels are connected to other pixels. A group of pixels that connected based on Connectivity types, called an Object", (Motameni et al., 2007).

2.3.1.7 Pixel Intensity Based Method (PIB)

"This technique maps, data by modifying the grey level of the image pixels. Modification Steganography is a technique to map data by modifying the gray level values of the image pixels. This technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels is selected based on a mathematical function. The gray level values of those pixels are examined and compared", (Potdar et al., 2004).

2.3.1.8 Texture-Based Method (TB)

"In this technique the secret and host images are divided into blocks of a specific size and each block in secret image is taken as a texture pattern for which the most similar block is found among the blocks of the host image. The embedding procedure is carried on by replacing these small blocks of the secret image with blocks in the host image in such a way that least distortion would be imposed on it", (Tsai et al., 2009).

2.3.1.9 Histogram Shifting Methods (HS)

"In histogram-based data hiding technique, the crucial information is embedded into the image histogram. Pairs of peak points and zero points are used to achieve low embedding distortion with respect to providing low data hiding capacity", (Hu et al., 2009).

2.3.2 Transform Domain

"Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain", (Johnson and Katzenbeisser, 2000).

2.3.2.1 Discrete Cosine Transformation

"DCT is a general transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands, namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the information in a middle frequency band does not scatter the watermark information to most visual important parts of the image, i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted. Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of information into a DCT block", (Kaur, et al., 2011).

2.3.2.2 Discrete Fourier Transformation Technique (DFT).

"The DFT-based technique is similar to the DCT based technique, but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions. Although it increases the overall complexity of the process", (Tiwari et al 2014).

2.3.2.3 Discrete Wavelet Transformation Technique (DWT).

"A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyse a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). This method transforms the object in the wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object", (Graps, 1995).

2.3.2.4 Lossless or Reversible Method (LR)

The proposed method uses a similar scheme with the RCM compression. The compression scheme splits images, then divides into host sections and watermark block. The compression process is performed by embedding watermark blocks into initial blocks. In the RCM

compression method, implementation of a shift operation increases the compression on an image in light or dark intensity. Therefore, this proposed method implements the shift operation as a step in the algorithm.

2.3.2.5 Embedding in Coefficient Bits (ECB)

"An embedded code represents a sequence of binary decisions that distinguish an image from the null or all gray images. Since the embedded code contains all lower rate codes embedded at the beginning of the bit stream, effectively, the bits are ordered in importance. Using an embedded code, an encoder can terminate the encoding at any point, thereby allowing a target rate or distortion metric to be met exactly. Typically, some target parameter such as bit count is monitored in the encoding simply stops. Similarly, given a bit stream, the decoder can cease decoding at any point and can produce reconstructions corresponding to all lower-rate encodings", (Shapiro, 1993).

2.3.3 Distortion Technique

"Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion", (Reddy and Raja, 2009)."Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is used to match the secret message required to transmit", (Katzenbeisser, 2000). "The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered", (Kruus, et al., 2003).

2.3.4 Masking & Filtering (MF)

"The technique hides' information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image", (Johnson and Jajodia 1998).

2.4 Steganographic Method Performance

2.4.1 Factors Affecting a Steganographic Method

The effectiveness of any steganographic method can be determined by comparing stego-image with the cover Image. There are some factors that determines the efficiency of a technique as indicated in Table 2.1.

Table 2.1 *Factors Affecting a Steganographic Method*

No.	**Factor**	**Explanation**
1.	**"Payload Capacity"**	"The size of information can be embedded into image".
2.	**"Perceptual Transparency"**	"After hiding process into cover image, perceptual quality will be degraded into stego-image as compared to cover-image".
3.	**"Robustness"**	"After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise".
4.	**"Tamper Resistance"**	"It should be difficult to alter the message once it has been embedded into stego-image".
5.	**"Computation Complexity"**	"How much expensive it is computationally for embedding and extracting a hidden message"?

2.5 Algorithms Comparative Analysis

Analysis of various methods along with their properties are is shown in table 2.2.

Table 2.2 *Techniques Comparative Analysis*

NO	Technique	Payload Capacity	Perceptual Transparency	Robustness	Tamper Resistance	Computation Complexity
Spatial Domain Techniques						
1.	LSB	"Yes"	"Yes"	"No"	"No"	"No"
2.	PVD	"Yes"	"Yes"	"No"	"No"	"No"
3.	MPHD	"Yes"	"Yes"	"No"	"No"	"No"
4.	LC	"Yes"	"Yes"	"No"	"No"	"No"
5.	TB	"Yes"	"Yes"	"No"	"No"	"No"
6.	HS	"Yes"	"Yes"	"No"	"No"	"No"
7.	EBE	"Yes"	"Yes"	"No"	"No"	"No"
8.	RPE	"Yes"	"Yes"	"No"	"No"	"No"
9.	PIB	"Yes"	"Yes"	"No"	"No"	"No"
Transform Domain Techniques						
10.	DWT	"No"	"No"	"Yes"	"Yes"	"No"
11.	DCT	"No"	"Yes"	"Yes"	"Yes"	"No"
12.	LR	"No"	"No"	"Yes"	"Yes"	"No"
13.	DFT	"No"	"Yes"	"Yes"	"Yes"	"No"
14.	ECB	"No"	"No"	"Yes"	"No"	"Yes"
Distortion Techniques						
15.	DT	"No"	"No"	"Yes"	"No"	"No"
Masking & Filtering						
16.	MF	"No"	"No"	"Yes"	"No"	"No"
Secure Information Hiding Technique						
17.	SIHT	"Yes"	"Yes"	"Yes"	X	"Yes"

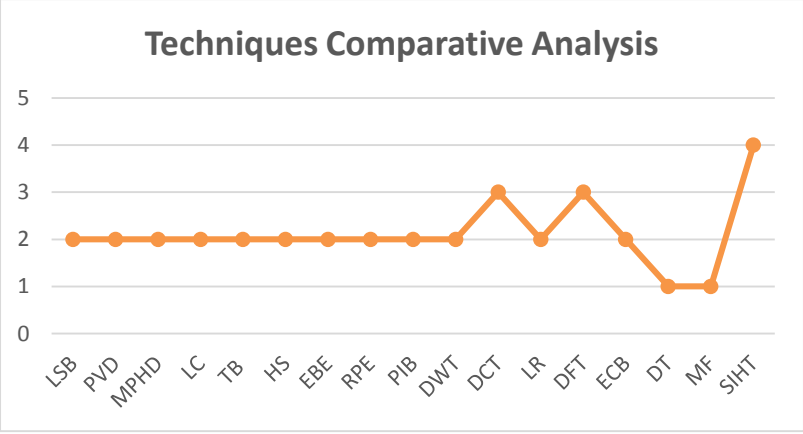

Figure 2.1 *Techniques comparative analysis LSB and ECB selected for the study*

As illustrated in Figure 2.1, the study observed that two techniques met 1 requirement which includes the following techniques: DT and MF. The majority of the techniques was meeting only 2 requirements, this includes LSB, PVD, MPHD, LC, TB, HS, EBE, RPE, PIB, DWT and LR. Two techniques were able to meet 3 requirements, including DCT and DFT. The developed tool was able to meet four out of the possible five requirements which included: Perceptual transparency, payload capacity, robustness and computational complexity. In this case, the developed tool was not only meeting tamper resistance as part of the requirements for information hiding tools.

2.5 Algorithmic Combinations

2.5.1 Least Significant Bit vs Embedding in Coefficient Bits

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been designed. There have been many techniques for hiding information or messages in images in such a manner that alteration made in the image is perceptually indiscernible. Common approaches include LSB, Masking and filtering and Transform techniques.

"The most common method used for hiding data in images are the 'Least Significant Bit (LSB) "Insertion technique" in which the LSB of the pixel values is replaced with the data to be encoded in binary form. Other techniques include the "Masking Technique" in which the original bits are masked with data bits and the 'Filtering Technique' in which certain transformations are done on the image to hide data. The last two techniques hide data by marking an image in a manner similar to paper watermarks, but, there are some drawbacks with these methods which hinders their use", Yang et al. (2008).

"An embedded code represents a sequence of binary decisions that distinguish an image from the null or all grey image. Since the embedded code contains all lower rate codes embedded at the beginning of the bit stream, effectively, the bits are ordered in importance. Using an embedded code, an encoder can terminate the encoding at any point, thereby allowing a target rate or distortion metric to be met exactly. Typically, some target parameter such as bit count is monitored in the encoding simply stops. Similarly, given a bit stream, the decoder can cease

decoding at any point and can produce reconstructions corresponding to all lower-rate encodings", Shapiro (1993).

2.5.2 Pixel Value Differencing vs Distortion Technique

Based on the fact that our human vision is sensitive to slight changes in the smooth regions, while can tolerate more severe changes in the edge regions, the PVD-based methods have been used to enhance the embedding capacity without introducing obvious visual artifacts into stego images. In PVD-based schemes, the number of embedded bits is determined by the difference between the pixel and its neighbour. The larger the difference amount is, the more secret bits can be embedded. Usually, PVD based approaches can achieve more imperceptible results compared with that typical LSB-based approach with the same embedding capacity. However, based on extensive experiments and analysis, we find that most existing PVD based algorithms perform worse to resist some statistical analysis, even with a low embedding capacity, e.g. 10% bits per pixel.

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is used to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

2.5.3 Lossless Reversible vs Masking & Filtering

The lossless reversible method uses a compression scheme. The scheme divides the image into fixed-size blocks, then the blocks are divided into host block and watermark block. The compression process is performed by embedding the watermark blocks into the host blocks. In the RCM compression method, implementation of a shift operation increased the compression ratio of the method on an image with light or dark intensity. Therefore, this method implements the shift operation as a step in the algorithm.

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Masking and filtering techniques, usually restricted to 24 bits and grayscale image, hide information by marking an image, in a manner similar to paper watermarks. The technique performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

The advantages of masking and filtering techniques are that this method is much more robust since the information is hidden in the visible parts of the image. The disadvantage is that the technique can be applied only to grayscale images and restricted to 24 bits.

CHAPTER THREE – RESEARCH METHODOLOGY

3.1 Research Design

This is an exploratory study to investigate the information hiding issues faced by ICT consultants and end users when executing ICT tasks. Data was collected from members of the target population by use of questionnaires in order to determine the current ICT security related challenges faced by that population. It was, therefore, descriptive survey research which brings out quantifiable information from the sample.

"Descriptive survey research is intended to produce statistical information about aspects of science that interests the policy makers and innovators. The choice of the descriptive survey research design was made based on the fact that in this study, the researcher is interested in the state of affairs already existing and no variable was manipulated", (Langrish et al., 1972).

3.2 Research Methods

3.2.1 Target Population

In order to determine the sample size to be used in the study, DELPHI technique was engaged. "It is a widely used and accepted method for achieving convergence of opinion concerning real-world knowledge within certain topic areas", (Dalkey and Helmer, 1963). "As a rule of thumb 15 to 30 people in homogeneous groups", (Yammarino, 1992). "10 to15 people produce good results in a homogeneous panel and if iterations are required a minimum of 3 should be considered", (Ziglo et al., 2009). "For heterogeneous groups, that is, people with expertise on a topic, but from different social or professional groups, only 5 to10 experts are needed", (Bromme, 2001). "Delphi studies use panels of 15 to 35 people", (Fick, 2003). It was concluded that the larger the group, the more reliable their aggregate judgment tends to be.

According to ICT Authority of Kenya (2014), East African Data Handlers is the leading data recovery organization in Africa. It provides its services to corporate, government as

well as individuals. Smartware Solutions was selected as the case study because East Africa Data Handlers outsource their information security services from this organization.

The study, therefore, targeted ICT consultants together with clients who report security related issues to the selected ICT firm (*smartware solutions Ltd*). The ICT consultants were selected based on their respective areas of expertise while end users were selected with respect to client organizations and the level of interaction with ICT technologies in such organizations. This was done so as to give every member of both groups an equal chance of being selected.

3.2.2 Sample Size and Sampling Procedures

The stratified random sampling technique was adopted in the study. This technique is appropriate, especially when representing not only the overall population but also the key subgroups of the population. The two subgroups in this study comprised of ICT consultants and end users. This was further broken down into the area of expertise and client organization groups respectively.

The total population of ICT consultants was 10 but only 9 were responsive. For end users, the total population was 40 but only 27 were responsive as indicated in Table 3.1.

Table 3.1 *Sampling of ICT Consultants*

No.	Area of Expertise	Number	Responsive
1.	ICT Security	4	4
2.	Programming and Software Development	3	3
3.	Systems Analysis and Design	3	2
	Total	**10**	**9**

The end users were drawn from 10 different organizations who are active clients of the selected ICT security firm. A total of 40 ICT oriented end users operates in such organizations as summarized in Table 3.2.

Table 3.2 *Sampling of end users*

No.	Organization	Number	Responsive
1.	ABNO Softwares International	7	5
2.	Bebma Consulting Group	3	2
3.	Dantez Systems & Technologies	4	4
4.	FAWE Kenya Chater	6	3
5.	Hiddekel Ventures	4	3
6.	Mynt Group	5	3
7.	Pestle Enterprises	4	3
8.	Ritech Solutions	2	2
9.	Sysmasters Technologies	4	1
10.	Toturin Investment Group	1	1
	TOTAL	**40**	**27**

3.2.3 Research Instrument

"Data collection instrument is a device used to collect data in an objective and a systematic manner for the purpose of the research", Mugenda and Mugenda (1999). "Data collection instruments can be questionnaires, interview schedules, and available records. A questionnaire is a data collection instrument filled in by respondents for the purpose of the research study", (Morris, 2001). The study employed questionnaires as a data collection instrument. "Questionnaires are preferred because they allow respondents to give much of their opinions pertaining to the researched problem", (Dempsey, 2004. "The information obtained from questionnaires is free from bias and researchers influence and thus accurate and valid data is guaranteed" (Sekaran, 2006).

3.2.4 Instrument Validity

Piloting was conducted to help to improve and validate the instrument. "Validity of an instrument is improved through expert judgment. As such, the researcher sought assistance from ICT security experts and the sampled respondents to the piloting phase in order to improve the content validity of the instrument", (Adhiambo, 2015).

3.2.5 Reliable Instrument

"Reliability is a measure of the degree to which a research instrument yields consistent results or data after repeated trial", Mugenda and Mugenda (1999). To enhance the reliability of the instrument, a pilot study was conducted three times within the organization. "The reason behind pre-testing is to assess the clarity of the questionnaire items. Those items found to be inadequate or vague was modified to improve the quality of the research instrument thus increasing its reliability", Mugenda and Mugenda (1999).

3.3 Steganography Tool Design

In the design, the waterfall methodology was employed.

3.3.1 Waterfall Methodology

"Waterfall SDLC model is a sequential software development process in which progress is regarded as flowing increasingly downwards through a list of phases that must be executed in order to successfully build a computer software", Bassil (2012). "The model describes a possible software engineering practice", (Kan, 2002). "The Waterfall model defines several consecutive phases that must be completed one after the other and moving to the next phase only when its preceding phase is completely done", (Bassil, 2012).

3.3.2 Why the Waterfall Model was selected:

The waterfall model is more suitable when the requirements are well known, product definition is stable, technology is understood, there are no ambiguous requirements, adequate resources with required expertise are available freely and the project is short. This, therefore, prompted its selection and use in this study as illustrated in Figure 3.1.

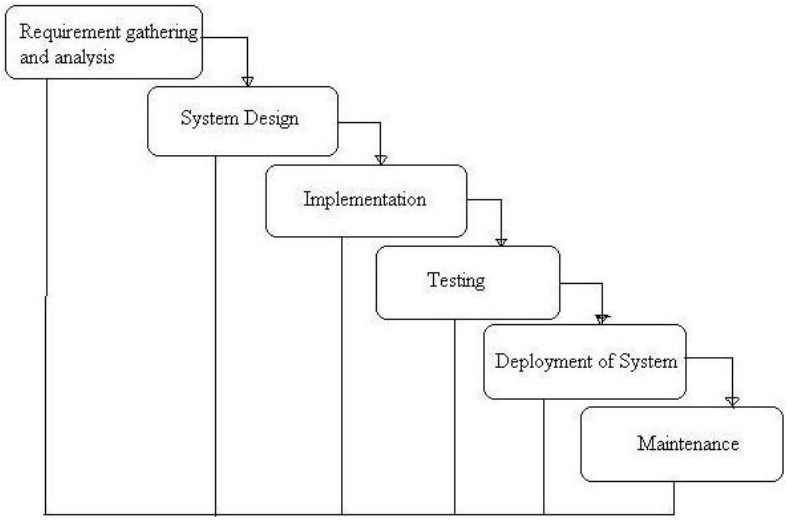

Figure 3.1 *Waterfall Model Adopted from* Bassil (2012).

Requirement gathering and analysis was carried out by using the findings from the case study to determine the requirements. The design was done using requirement specifications and analysis where a system was selected based on the selected framework. Implementation was carried out by engaging a system in day-to-day business or organization's operations. Testing took place where system validation, utility and usability tests were carried out. Deployment of the tool is where it was put into use. Maintenance was also carried out to guarantee robustness.

3.3.3 Steganography Design of the Technique

The tool is designed with two modules to serve the function of encrypting and decrypting. Microsoft.Net framework was used for programming using C#. Net language. One of the tools in this language that was resourceful for pictures and images is automatic conversion to bitmap images, hence there is no prior need for images to be in any format which saves a lot of time especially for novice users.

Two algorithms were implemented, i.e. least significant bit (LSB) and embedding of coefficient bits (ECB). For LSB data are written starting from the least significant bit. In this case, the significance of every bit doubles from the previous layer, hence the quality of the image decreases moving towards the upper layer. This reduces the possibility of

distorting the image as well as minimizing the perceptual transparency as well. For ECB the embedding process was carried out in such a way that in the embedding process, steganography actually replaces redundant data with the secret message. Therefore the number of bits contained in any selected image was able to accommodate the size of the selected file with respect to the file size in terms of width, height and the number of pixels.

Before encryption was done, the users were prompted to browse for the image to be used as a cover and also the file to be hidden. A filename was also requirement and the location for saving, as this helps to avoid losing its content. On decrypting, the user was just required to locate the cover works, then the location to save the decrypted file.

3.4 Steganography Framework

The basic operation is to hide a confidential message using a cover. Caution has to be taken to ensure that the message remains secret from unauthorized users. The decryption process basically is the reverse of the encryption. The whole process is illustrated in Figure 3.2.

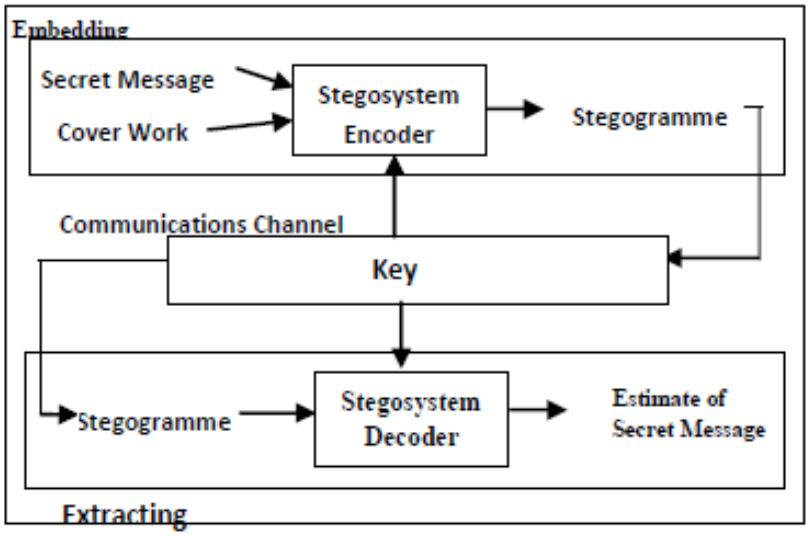

Figure 3.2 *Framework of the technique adopted from (Deepa and Umarani, 2013).*

"Two inputs required for the embedding process are a secret message and the cover work that are used to construct a stegogramme that contains a secret message. The inputs are passed through the stego-system encoder to embed the message within an exact copy of

the cover work. The stego-system requires a key which is also used in the extraction phase. The resulting output from the stego-system encoder is the stegogramme that contains the secret message. This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stego-system decoder where an estimate of the secret message is extracted", (Hussein, 2014), as illustrated in Figure 3.3.

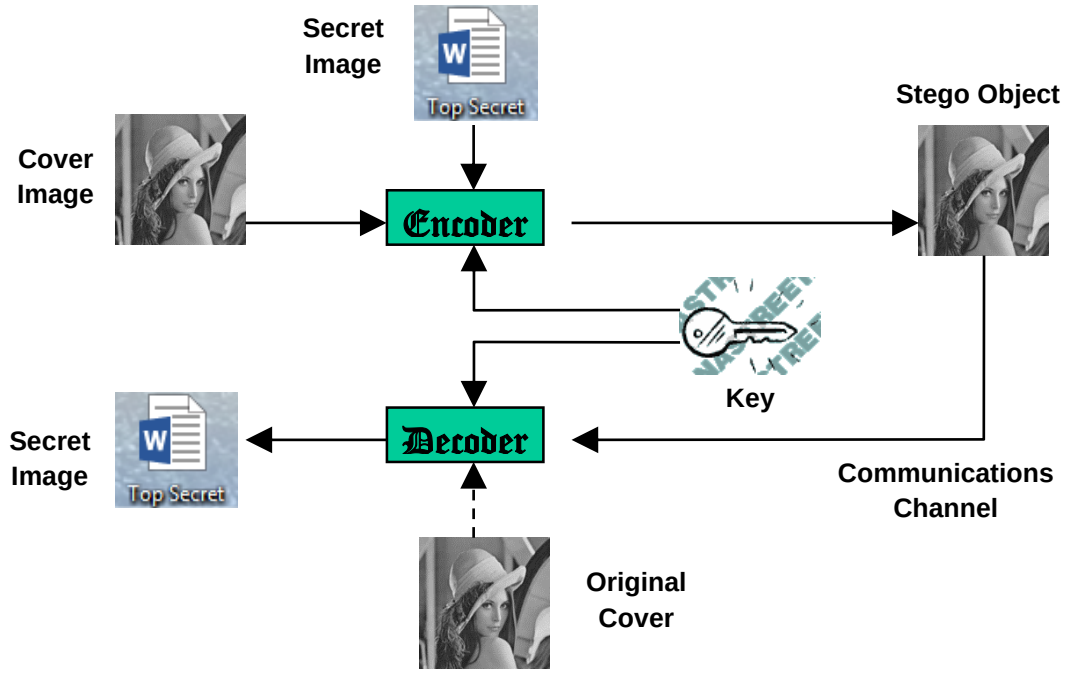

Figure 3.3 *Generic Process of Encoding and Decoding*

Algorithm adapted from (Chang, 2003).

Algorithm to embed the text message[2]:-
Step 1: Read the cover image and the text message which is to be hidden in the cover image.
Step 2: Convert the text message in binary format.
Step 3: Calculate the LSB of each pixel of the cover image.
Step 4: Replace the cover image of the LSB with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Mean square Error (MSE) and the Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

“The technique used in implementing this is the least significant bits and embedding coefficient bits. The advantage of this technique is that the cost of cracking the hidden message is extremely high, the data cannot be easily decoded without the key using image manipulation techniques, any type of image, 8 or 24 bits can be used, there is no increase in the size of the image due to data in it and there are no constraints on the choice of the image”, Chang et al. (2003).

3.5 Sources of Data/Information and Relevance of Data to the Problem

The study targeted mainly ICT security consultants together with end users operating in a real working environment. The respondents of the study were selected from the ICT organizational unit based on the kind of roles and responsibilities performed. Using this criterion, novice users were highly avoided where possible, hence minimizing invalid responsiveness in the long run.

In order to improve the reliability of the instrument, the researcher employed test - retest technique, whereby the questionnaires were administered thrice in the pilot sample at time 1, time 2 and time 3. Critical assessment was carried out to ensure some degree of consistency of the responses on each pair of the pilot questionnaires to make a judgment on their reliability

3.6 Tools, Procedures and Methods for Data Collection and their Justification

Descriptive survey research procedure was adopted where questionnaires were administered to ICT security consultants together with the end users. “It is a method of collecting information by administering a questionnaire to a sample of individuals”, (Orodho, 1992). “Descriptive survey is ideally a process of collecting data in order to test a hypothesis or to answer questions concerning the status of the subject in the study”, Mugenda and Mugenda (1999).

Prior arrangements were made with the management of the institutions where the data collection took place by liaising with the management of the respective institutions. The researcher visited each section and established a rapport with the section members before administering the questionnaires. The filled-in exercise of the questionnaires was collected at an agreed time period of time.

3.6.1 Tools, Procedures and Methods for Data Collection

The most suitable research instrument for descriptive survey research design is a questionnaire. Questionnaires were used to capture input from the respondents. The questionnaires comprised mostly closed-ended and some few open-ended questions for ease of analysis. “Questionnaires gave respondent's freedom to express their views or opinion and also made suggestions while maintaining anonymity”, (Gay, 1976). Furthermore, questionnaires are generally less expensive and they do not consume a lot of time in their administration.

3.6.2 Justification

The mixed method which involves the use of previous information and expert opinions from various ICT consultants and end users was adopted. Because of the numbers of issues that were raised by the research questions and the need to associate them with current practice in computing operations. The research was not relying entirely on questionnaires, but it will also engage the experts through consultations.

3.7 Data Analysis Methods and their Justification

The response questionnaires were tabulated and processed by using a computer. The results of the data were analyzed with the help of Microsoft excel formulae and graphs were generated where possible. Data analysis was accompanied with tabulations, calculations of measures of central tendencies and graphical representations.

3.7.1 Data Analysis Methods

“Descriptive statistics of frequencies and percentages is used to summarize data efficiently. Data from the open-ended item in all the questionnaires was read thoroughly and recorded for qualitative data analysis. The data was then being evaluated and analyzed for usefulness in answering research questions and also for report writing”, (William, 2009).

3.7.2 Justification

Descriptive statistics were preferred analysis technique because it enables analysis of data using appropriate techniques. It also enables, checking data for errors as well as comparing different methods for consistent findings.

3.8 Limitations of Methodology and how they will be addressed

3.8.1 Limitations of Methodology

"Limitations are conditions beyond the control of the researcher that may restrict the conclusion of the study and their application to other situations", (Meredith, 1998). There may be cases of exaggerated feedback or outright misinformation. A briefing was conducted to develop a rapport with the interviewees thereby minimizing the chances of wrong feedback. The researcher using communication skills will try to control the attitudes of the respondents as they respond to the questions. This is because many of them may have their own perceptions of various computer security issues in a real working environment, finally the technology related phobia attached to the use of computers and technology as a whole may also affect the response.

3.8.2 Overcoming Limitations

The mixed methods were employed in data collection and analysis to provide an important tool to overcome limitations of qualitative and quantitative research. In a sequential quantitative-qualitative design, quantitative research guided the selection of cases in qualitative studies, results from qualitative interviews helped to identify unobserved heterogeneity in quantitative data as well previously unknowns, explaining variables and results from the qualitative part of mixed methods design helped in understanding previously incomprehensible statistical findings.

CHAPTER FOUR - ANALYSIS & INTERPRETATIONS

4.1 Introduction

As indicated in 3.2.1 “Target Population”, DELPHI technique was engaged to determine the sample size. “As a rule of thumb 15 to 30 people in homogeneous groups”, (Yammarino, 1992). “For heterogeneous groups, that is, people with expertise on a topic, but from different social or professional groups, only 5 to10 experts are needed”, (Bromme, 2001). “Delphi studies use panels of 15 to 35 people”, (Fick, 2003).

This study required an adequate number of respondents in order for the feedback to be representative where possible. A total of 50 questionnaires was distributed, these comprised of 10 for ICT experts and 40 for end users. The number of questionnaires returned was 36, out of these, 9 was from ICT experts while 27 was from the end users. This resulted in a response rate of 72%, which was deemed to be very good and sufficient for data analysis. ”50% return is adequate, 60% is good and more than 70% is very good”, (Herman, 1979). As a result, a return rate of 70% was deemed to be very good and sufficient for data analysis. The respondents were quite cooperative and the data collected was taken to be a true representation of the respondent’s views due to the independence of the method of data collection. The returned questionnaires were cleaned and analyzed using Microsoft Excel spreadsheets.

4.2 Bio Data

Computer end users together with ICT consultant’s information was collected in terms of their age, gender, academic qualification and ICT experience.

4.2.1 Age Distribution

To determine the age distribution, the users and ICT consultants together with the end users indicated the respective age. Their responses are shown in Table 4.1.

Table 4.1 *Distribution of ICT consultants and End Users by age*

Age	Frequency	Percentage
"18-25 Years"	11	31
"26-35 Years"	9	25
"36-45 Years"	9	25
"46-55 Years"	6	17
"56-65 Years"	1	3
	36	**100**

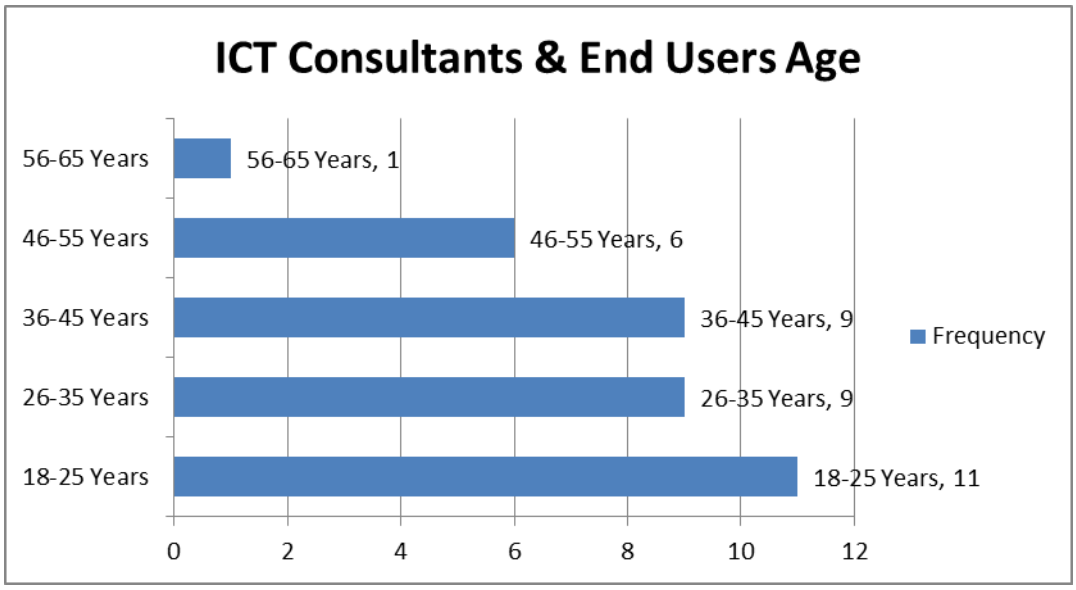

Figure 4.1 *ICT Consultants and End Users Age Distributions*

As illustrated in Figure 4.1, the study observed that 30% of the ICT consultant's and end users were between the ages of 18-25 years, 25% between the age of 26-35 years, 25% between the age of 36-45 years, 17% between the age of 46-55 years and 3% were between the ages of 56-65 years. The study observed that the institution attracted young ICT personnel than their old counterparts; this is attributed to the fact that majority of young ICT practitioners have vast ICT knowledge and they are willing to share this information for the development of the ICT industry. Furthermore, this suggested that most of the end users were fresh graduates, this could be attributed to the fact that most private firms prefer employing fresh graduates then take them through training instead of paying good salaries to older people.

4.2.2 Gender Distribution

To determine the gender distribution, the end users and ICT consultants indicated the gender. Their responses are shown in Table 4.2.

Table 4.2 *Distribution of ICT Consultants and End Users by gender*

Gender	Frequency	Percentage
Male	23	64%
Female	13	36%
Total	**36**	**100%**

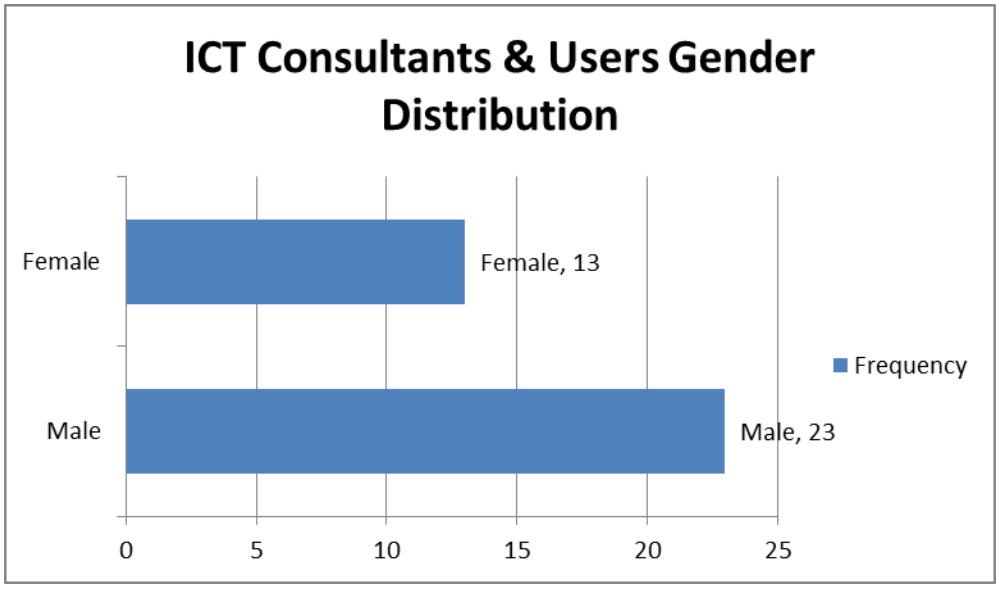

Figure 4.2 *ICT Consultants and End Users Gender Distributions*

As illustrated in Figure 4.2, the study observed that 64% of the ICT consultants were males compared to 36% females. This is attributed to the fact that ICT consultancy is an area that is dominated by males than females; most of the ICT areas of specialization attract more males than females.

4.2.3 Academic Qualification

To determine the academic qualification, the ICT consultants together with the end users were asked to indicate their academic qualification. The responses were analyzed as shown in Table 4.3.

Table 4.3 *Distribution of Academic Qualification for ICT Consultants and End Users*

Academic Level	Frequency	Percentage
KCPE	12	33%
KCSE	9	25%
Diploma	8	22%
Bachelors	6	17%
Masters	1	3%
PHD	0	0%
Total	**36**	**100%**

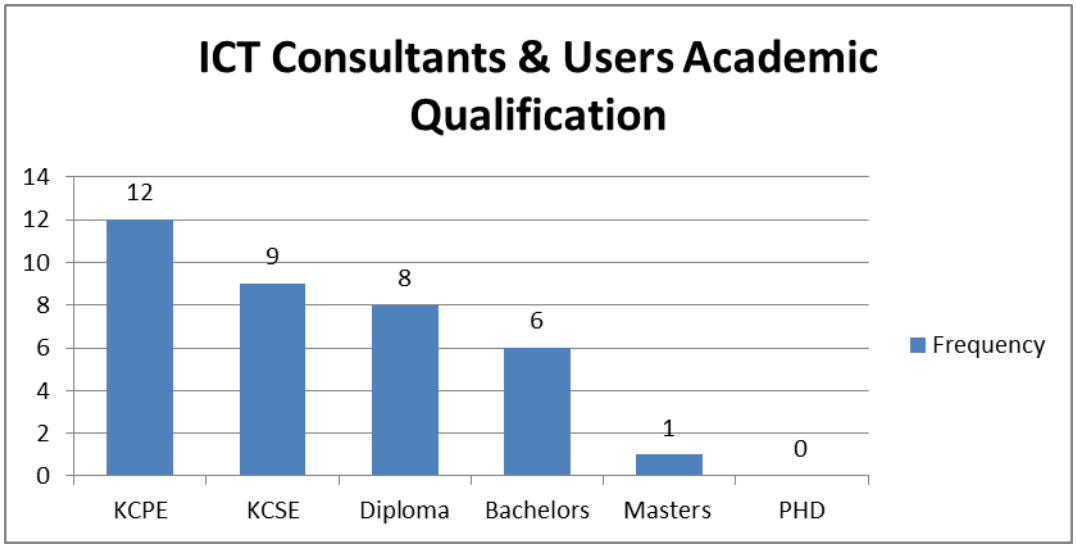

Figure 4.3 *ICT Consultants and Users Qualification*

As illustrated in Figure 4.3, the study observed that 33% of the end users have acquired KCPE qualification, 25% KCSE, 22% Diploma, 17% Bachelors, 3% Masters and 0% Ph.D. This is attributed to the fact that the end users did not require much knowledge and skills to carry out computer errands hence lower level qualification. Hence end user requires a low level of technical skills to carry out basic tasks.

4.2.4 Level of Experience

To determine the level of experience, the ICT consultants together with the end users were asked to indicate their level of experience. The responses were analyzed as shown in Table 4.4.

Table 4.4 *Distribution ICT Consultants & Users Level of Experience*

Experience	Frequency	Percentage
"01 – 05 Years"	11	31%
"06 – 15 Years"	10	28%
"16 – 25 Years "	10	28%
"26 – 35 Years"	4	11%
"36 – 35 Years"	1	3%
Total	**36**	**100%**

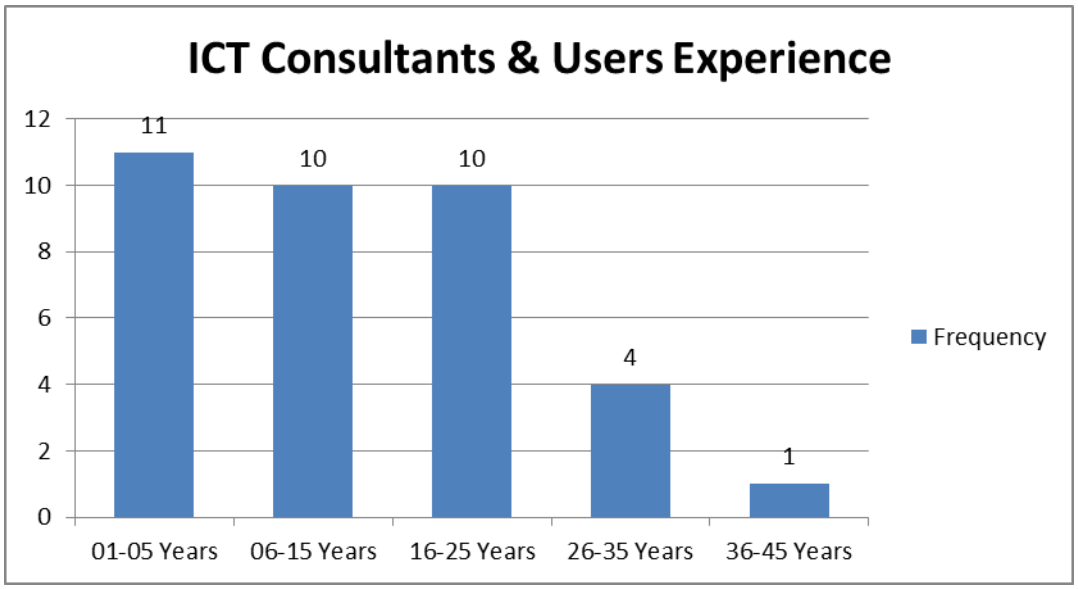

Figure 4.4 *ICT Consultants & Users Experience*

As illustrated in Figure 4.4, the study observed that 30% of the computer end users had experience ranging from "1–5 years", 28% "6-15 years", 28% "16-25 years", 11%, "26-35 years" and 3% 36-45 years. This could be attributed to the fact that most of the end users had never been exposed in a real working environment since the majority of them were fresh graduates. Generally, end users require a shorter period of time to perform basic tasks.

4.3 Information Hiding Tools & Techniques

The study inquired about the various information hiding tools and techniques from the ICT consultants in terms of the tools, mediums and domains.

4.3.1 Information Hiding Tools

To determine the information hiding tools and techniques, the ICT consultants were asked to indicate the various information security tools and technique aspects pertaining to the study. The responses were analyzed and as shown in Table 4.5.

Table 4.5 *Distribution of ICT Consultants Information Hiding Tools*

Tool	Frequency	Percentage
Biometrics	0	0%
Cryptography	4	44%
Finger Printing	0	0%
Steganography	5	56%
Water Marking	0	0%
Total	**9**	**100%**

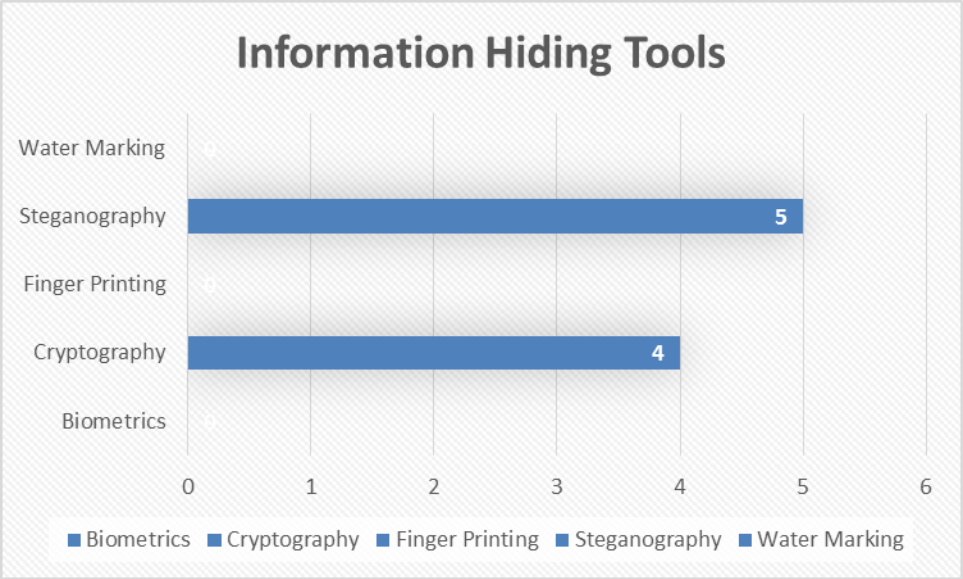

Figure 4.5 *ICT Consultants Information Hiding Tools*

As illustrated in Figure 4.5, the study observed that 0% of the ICT consultants had interacted with biometrics, 44% cryptography, 0% fingerprinting, 56% steganography and 0% watermarking. The study observed that most of the ICT consultants were exposed to cryptography and "steganography". This is attributed to the fact that cryptography and steganography are more popular as opposed to the other mechanisms of information hiding.

4.3.2 Information Hiding Mediums

To determine the information hiding mediums, the ICT consultants were asked to indicate the various information hiding mediums pertaining to the study. The responses were analyzed as shown in Table 4.6.

Table 4.6 *Distribution of ICT Consultants Information Hiding Mediums*

Medium	Frequency	Percentage
Audio	0	0%
Image	2	40%
Network	0	0%
Text	3	60%
Video	0	0%
Total	**5**	**100%**

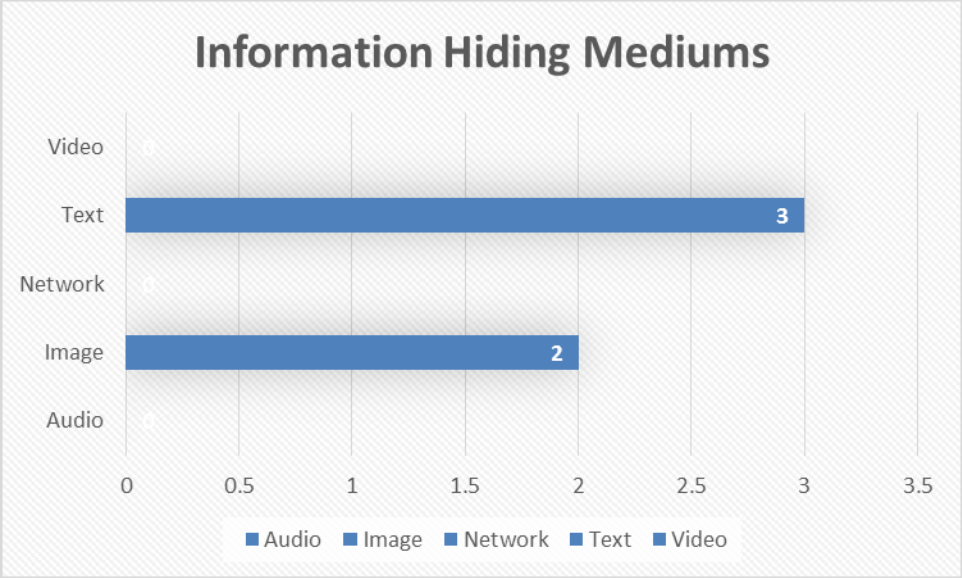

Figure 4.6 *ICT Consultants Information Hiding Mediums*

As illustrated in Figure 4.6, the study observed that 0% of the ICT consultants had used, audio as a medium of information hiding, 40% image, 0% network, 60% text and 0% video. The study observed that most of the ICT consultants were exposed to text and image "steganography". This attributes to the fact that text and image steganography are more popular as opposed to the other

mediums. This was attributed to the technologies that were deployed and also the expertise that was showcased by the ICT consultants.

4.3.2 Information Hiding Domains

To determine the information hiding domains, the ICT consultants were asked to indicate the various information hiding domains pertaining to the study. The responses were analyzed as shown in Table 4.7.

Table 4.7 *Distribution of ICT Consultants Information Hiding Domains*

Domain	Frequency	Percentage
Distortion	1	50%
Masking & Filtering	1	50%
Spatial	0	0%
Transform	0	0%
Total	**2**	**100%**

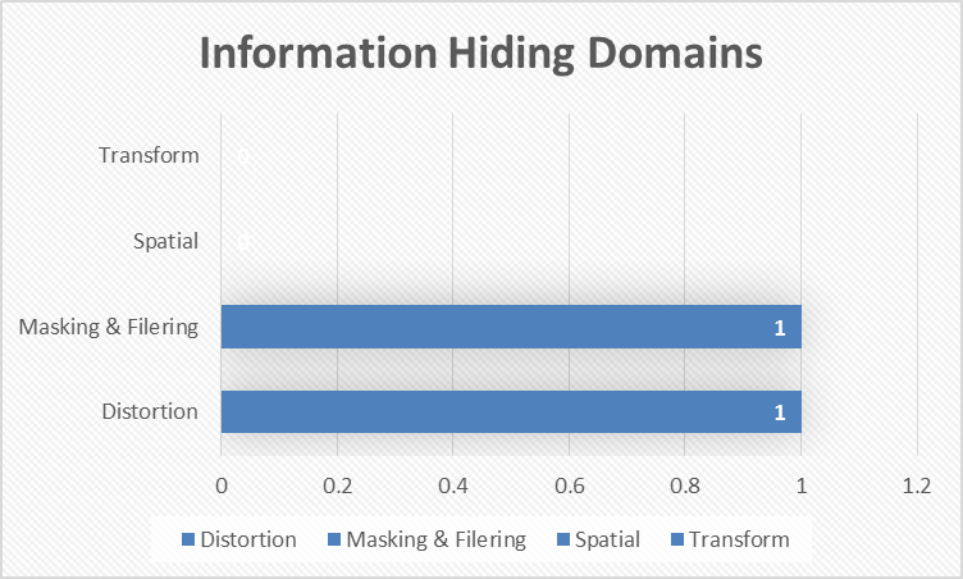

Figure 4.7 *ICT Consultants Information Hiding Domains*

As illustrated in Figure 4.7, the study observed that 50% of the ICT consultants had employed distortion as a domain, 50% masking and filtering, 0% spatial, and 0% transform. The study observed that most of the ICT consultants were exposed to distortion and masking & filtering

techniques. This attributes to distortion together with masking and filtering are easy to implement with less computing power required.

4.4 Information Hiding Challenges

To determine the information hiding challenges, end users were taken through a session where all the challenges were explained in detail in table as indicated in table 2.1 "*Factors Affecting a Steganographic Method*", they were then asked to indicate the various information hiding challenges they have experienced in the past pertaining to the study. The responses were analyzed as shown in Table 4.8.

Table 4.8 *Distribution of ICT Consultants and Users Challenges*

Challenge	Frequency	Percentage
Payload Capacity	12	33%
Perceptual Transparency	10	28%
Robustness	7	20%
Tamper Resistance	4	11%
Computational Complexity	3	8%
Total	**36**	**100%**

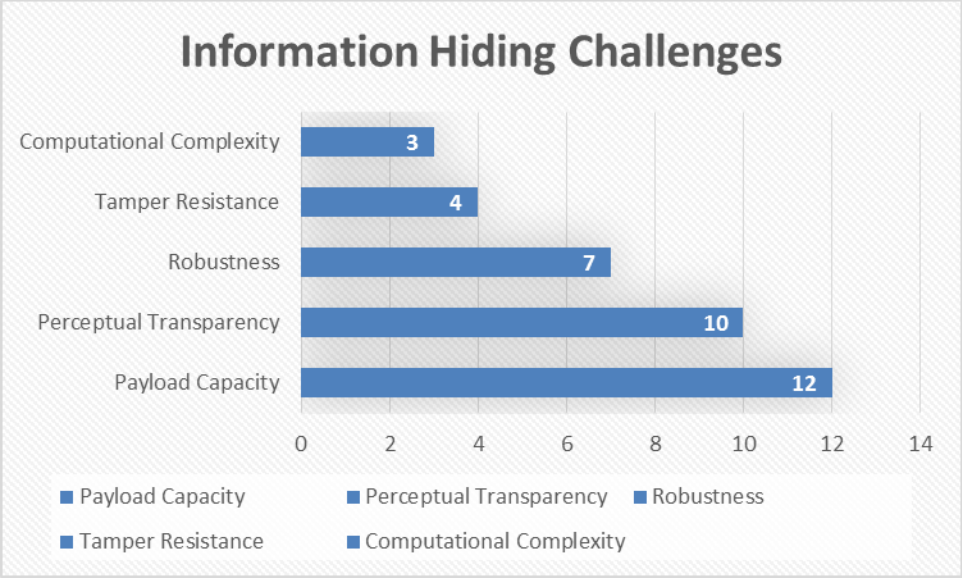

Figure 4.8 *ICT Consultants and Users Challenges*

As illustrated in Figure 4.8, the study observed that 33% of the ICT consultants together with the end users believed that the number one challenge when it comes to information hiding is payload capacity, 28% perceptual transparency, 20% robustness, 11% temper resistance and 8% computational complexity. This is attributed to the fact that the majority of the existing information hiding tools does not cater for payload capacity and perceptual transparency.

4.5 Payload Capacity Threshold

To determine the payload capacity threshold, the tool was subjected to various images of different sizes. The findings were analyzed as shown in Table 4.9.

Table 4.9 *Payload Capacity Threshold Distribution*

Image Size (KB)	Bitmap Size (KB)	Height (Pixels)	Width (Pixels)	Height*Width	Payload (KB)
1	0.44	151	151	22,801	58.97
6	5.62	177	284	50,268	129.97
2	1.72	180	280	50,400	130.77
7	6.78	168	300	50,400	131.24
11	10.01	194	259	50,246	130.33
259	258.75	596	692	412,432	1,489.99
102	101.08	640	960	614,400	1,599.99
128	127.00	536	962	515,632	1,339.00
582	581.33	768	1,024	786,432	2,045.99
331	330.61	1,088	1,920	2,088,960	5,439.99
2134	2,133.25	1,920	2,160	4,147,200	12,794.99
2587	2,586.45	2,560	1,920	4,915,200	12,799.99
2666	2,665.68	2,448	3,264	7,990,272	20,807.99
987	986.61	3,840	2,160	8,294,400	21,599.99
3,662	3,661.18	2,432	3,648	8,871,936	23,103.99
5,681	5,680.74	3,240	4,320	13,996,800	36,449.99
5,681	5,680.74	3,240	4,320	13,996,800	36,450.99
5,681	5,680.74	3,240	4,320	13,996,800	36,451.99

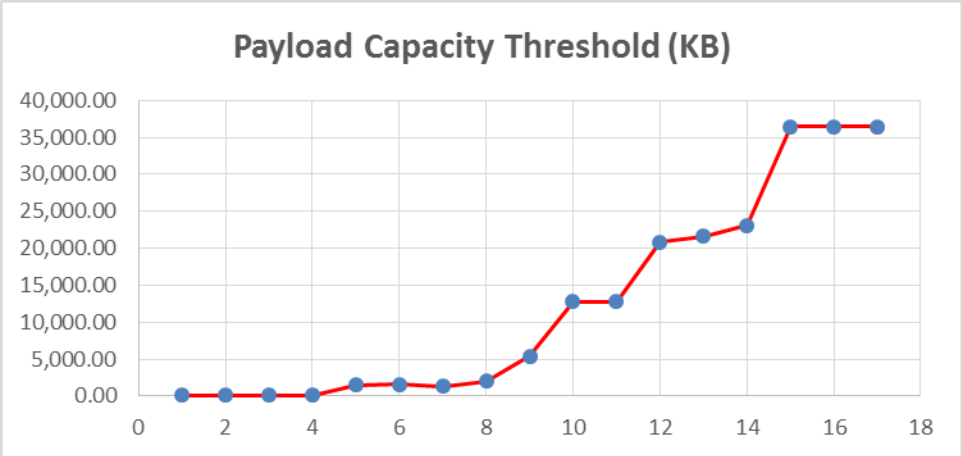

Figure 4.9 *Payload Capacity Threshold*

As illustrated in Figure 4.9, the study observed that the higher the size of the image, the higher the quantity of data that it can hide. But however, this may not be true in a case where the image has a short width and height. This is because the edges based data embedding algorithm require an image with adequate height and width because the data quantity embedded determines by bitmap pixels. In this situation, therefore when selecting the image to be used, then two considerations needs to be factored i.e. the height and width of the image.

4.6 Testing and Implementation

This section provides an overview of the testing and implementation. Validation, utility and usability testing were carried out:

4.6.1 Validation Testing

This involved testing the modules to check its behavior as defined by the scope of the study. The main concern of validation testing was to verify the modules incorporated in the tool against specified requirements. It checks whether the modules are behaving as per the expectations.

4.6.1.1 Validation Testing Methodology

"The methodology involves testing the modules of the tool for errors and bugs. This test was carried out by engaging the two modules that were implemented in the tool. This testing is listed under the black-box testing method, black box testing is performed while giving inputs and getting

the expected output with the focus of the validity of the tool, where the tool is checked for user-expected working conditions as well as potential exception and edge conditions", (Everett and McLeod, 2007). The results were as shown in table 4.10.

Table 4.10 *Validation Testing Results*

No	Module	Test Step(s)	Expected Outcomes	Results
1.	Encryption	Select an image, then select a file to encrypt. Use the encryption module to encrypt the file.	An encrypted file comprising of an image and file.	Pass
2.	Decryption	Select the encrypted file. Input a file name for your new file, then decrypt.	Decrypted file comprising of the file alone.	Pass

Key:

Pass Complies with the requirement **Fail** Does not comply with the requirement
Other Level of compliance not defined

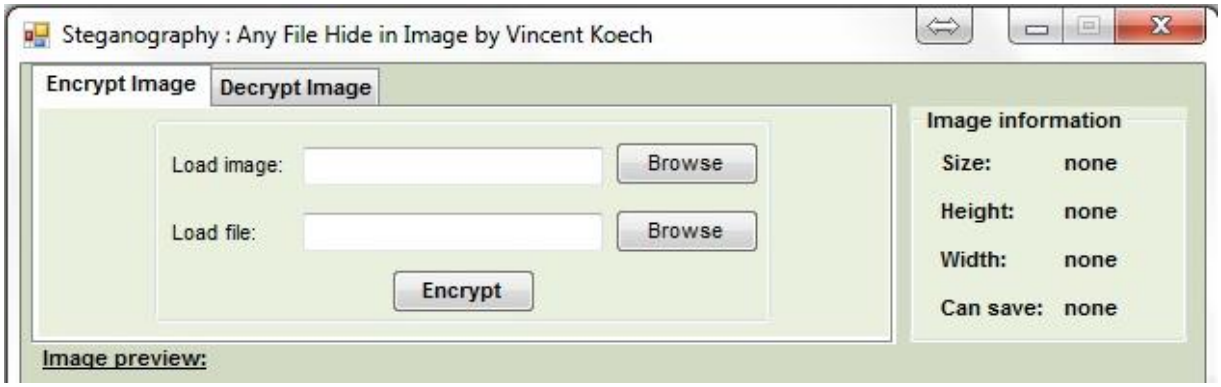

Figure 4.10 *Validation Testing: Encryption*

Figure 4.11 *Validation Testing: Decryption*

4.6.1.2 Validation Testing Observation

Validation testing was in the affirmative since the two modules were able to secure a result of "pass", meaning it complies with the desired results.

4.6.2 Utility Testing

Utility testing is usually a black-box testing, which describes what the system does.

4.6.2.1 Utility Testing Methodology

The tool was tested subjecting with some inputs and making observations on the output. The results are as shown in table 4.11.

Table 4.11 *Utility Testing Frequency of Responses*

NO	QUESTION	VALUE	FREQ	%
1.	Using steganography tool saved me time as compared to other solutions	"Strongly disagree"	0	0.00
		"Disagree"	0	0.00
		"Neutral"	3	8.33
		"Agree"	5	13.89
		"Strongly agree"	**28**	**77.78**
2.	Using steganography tool helped me improve my data security	"Strongly disagree"	0	0.00
		"Disagree"	1	2.78
		"Neutral"	3	8.33
		"Agree"	3	8.33

		“Strongly agree”	**29**	**80.56**
3.	Using steganography tool provided timely and speedy transmission of secure information	“Strongly disagree”	0	0.00
		“Disagree”	2	5.56
		“Neutral”	2	5.56
		“Agree”	2	5.56
		“Strongly agree”	**30**	**83.33**
4.	Using steganography tool helped me receive timely and speedy, secure feedback from the people I interact with	“Strongly disagree”	1	2.78
		“Disagree”	3	8.33
		“Neutral”	3	8.33
		“Agree”	3	8.33
		“Strongly agree”	**27**	**75.00**
5.	Using steganography tool I was able to manage my secure information	“Strongly disagree”	0	0.00
		“Disagree”	1	2.78
		“Neutral”	3	8.33
		“Agree”	3	8.33
		“Strongly agree”	**29**	**80.56**
6.	Using steganography tool provided instant and easy access to my secure information	“Strongly disagree”	0	0.00
		“Disagree”	3	8.33
		“Neutral”	3	8.33
		“Agree”	3	8.33
		“Strongly agree”	**27**	**75.00**
7.	Using steganography tool I was able to interact with others easily	“Strongly disagree”	2	5.56
		“Disagree”	3	8.33
		“Neutral”	3	8.33
		“Agree”	5	13.89
		“Strongly agree”	**23**	**63.89**

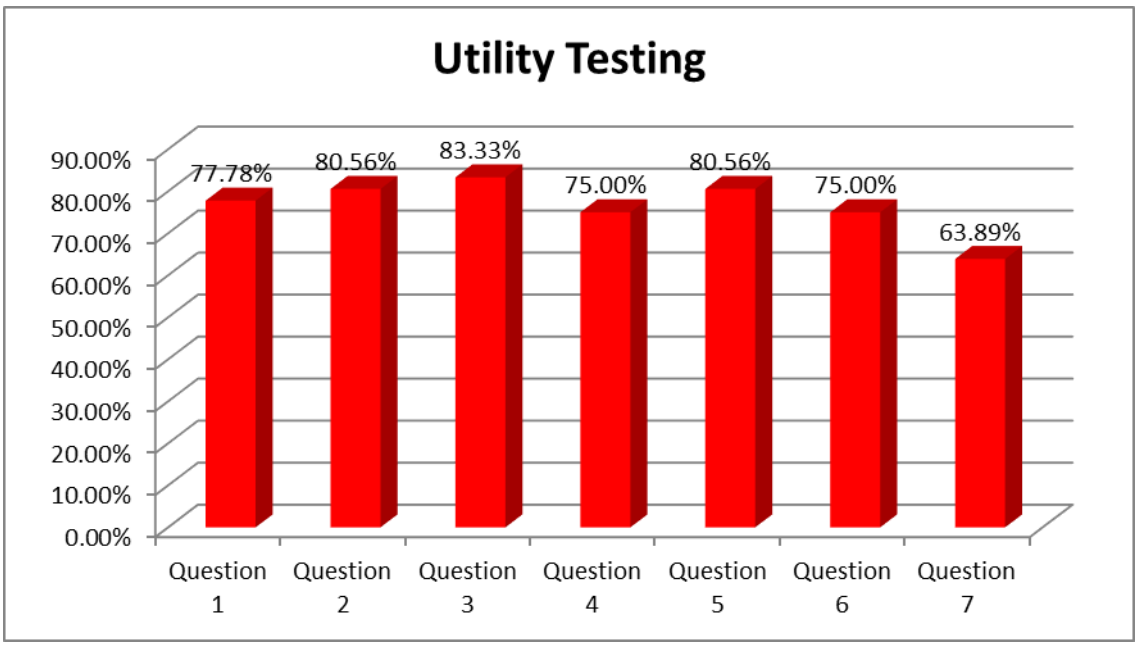

Figure 4.12 *Utility Testing: Strongly Agree Summary*

4.6.2.2 Utility Testing Observation

As illustrated in figure 4.12, the study observed that 77.78% of the respondents were able to agree that steganography tool saved them time as compared to other solutions, 80.56% agreed that steganography tool helped to improve my data security as compared to other solutions, 83.33% agreed that steganography tool provided timely and speedy transmission of secure data, 75% agreed that steganography tool helped to receive timely and speedy, secure feedback from the people during interaction, 80.56% agreed that steganography tool was able to help in the management of secure data, 75% agreed that steganography tool provided instant and easy access to secure data and 63% agreed that using steganography tool helped in interaction with others easily as compared to other solutions.

4.6.2.3 Interpreting Scores

Utility testing was confirmed affirmative with an average score of 76.59%. This implies that users were able to agree that steganography tool was meeting their information security needs. As a result, this indicates that the tool was able to perform its tasks as anticipated.

4.6.3 Usability Test

"Usability testing refers to evaluating a product or service by testing it with representative users", (Brooke, 1996). The process of achieving this test was done mainly through interacting with the tool and observing the user interface design. User perceptions was also allowed as part of the test.

4.6.3.1 Usability Testing Methodology

"System Usability Scale (SUS) provides a quick and reliable tool for measuring the usability. It consists of a 10 item questionnaire with five response options for respondents; from strongly agree to strongly disagree. SUS allows respondents to evaluate a wide variety of products and services, including hardware, software, mobile devices, websites and applications", Brooke (1996).

4.6.3.2 SUS Scale adopted from Brooke (1996).

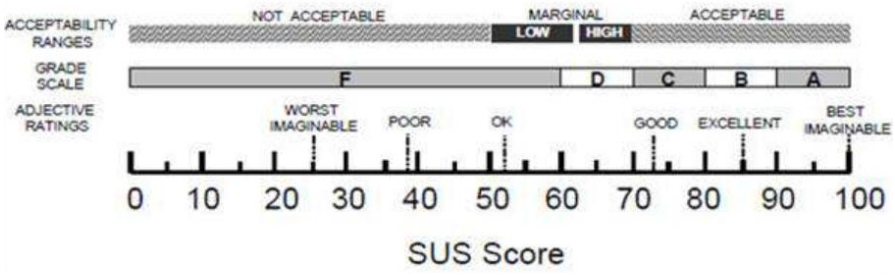

Figure 4.13 *SUS Scale*

Note:

Based on the above SUS scale, the following interpretations were used at Best imaginable, B: Excellent, C: Good, D: Ok, E: Poor and F: Worst imaginable

4.6.3.3 SUS Questionnaire Results, Questions adapted from Brooke (1996).

SUS questionnaire results are as indicated in table 4.12.

Table 4.12 *Usability Testing Frequency of Responses*

NO	QUESTION	VALUE	FREQ	%
1	"I think that I would like to use this tool frequently"	"Strongly disagree"	0	0.00
		"Disagree"	1	2.78

		"Neutral"	5	13.89
		"Agree"	6	16.67
		"Strongly agree"	**24**	**66.67**
2	"I found the tool unnecessarily complex"	**"Strongly disagree"**	**27**	**75.00**
		"Disagree"	3	8.33
		"Neutral"	3	8.33
		"Agree"	3	8.33
		"Strongly agree"	0	0.00
3	"I thought the tool was easy to use"	"Strongly disagree"	0	0.00
		"Disagree"	0	0.00
		"Neutral"	4	11.11
		"Agree"	4	11.11
		"Strongly agree"	**28**	**77.78**
4	"I think that I would need the support of a technical person to be able to use this tool"	**"Strongly disagree"**	**25**	**69.44**
		"Disagree"	5	13.89
		"Neutral"	5	13.89
		"Agree"	1	2.78
		"Strongly agree"	0	0.00
5	"I found the modules in this tool were well integrated"	"Strongly disagree"	0	0.00
		"Disagree"	3	8.33
		"Neutral"	3	8.33
		"Agree"	4	11.11
		"Strongly agree"	**26**	**72.22**

6	"I thought there was too much inconsistency in this tool"	**"Strongly disagree"**	**27**	**75.00**
		"Disagree"	3	8.33
		"Neutral"	3	8.33
		"Agree"	3	8.33
		"Strongly agree"	0	0.00
7	"I would imagine that most people would learn to use this tool very quickly"	"Strongly disagree"	0	0.00
		"Disagree"	0	0.00
		"Neutral"	1	2.78
		"Agree"	10	27.78
		"Strongly agree"	**25**	**69.44**
8	"I found the tool very cumbersome to use"	**"Strongly disagree"**	**20**	**55.56**
		"Disagree"	9	25.00
		"Neutral"	5	13.89
		"Agree"	2	5.56
		"Strongly agree"	0	0.00
9	"I felt very confident using the tool"	"Strongly disagree"	0	0.00
		"Disagree"	0	0.00
		"Neutral"	2	5.56
		"Agree"	5	13.89
		"Strongly agree"	**29**	**80.56**
10	"I needed to learn a lot of things before I could get going with this tool"	**"Strongly disagree"**	**27**	**75.00**
		"Disagree"	3	8.33
		"Neutral"	3	8.33

		"Agree"	2	5.56
		"Strongly agree"	1	2.78

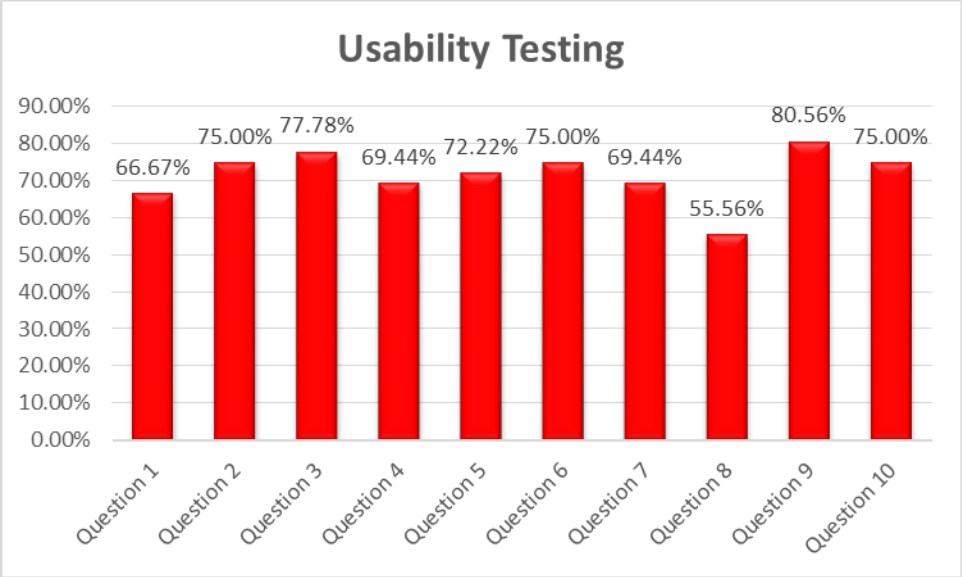

Figure 4.14 *SUS Metrics Summary*

4.6.4.4 Usability Testing Observation

As illustrated in figure 4.14, the study observed that 66.67% of the respondents expressed their desire to use steganography tool frequently, 75% found the tool to be very simple to use, 83.33% agreed that the tool provided timely and speedy transmission of secure data, 75% agreed that the tool helped to receive timely and secure feedback from others, 80.56% agreed that the tool was able to help in the managing of secure data, 75% agreed that the tool provided instant and easy access to secure data and 63% agreed that using the tool helped in easy interaction with others.

4.6.3.5 Interpreting Scores

"A SUS score above a 68% would be considered above average and anything below 68 is below average, however, the best way to interpret the results involves "normalizing" the scores to produce a percentile ranking", Brooke (1996). The average achieved score of 71.67% was considered above average meeting the minimum threshold of usability testing.

CHAPTER FIVE - CONCLUSION & RECOMMENDATION(S)

In this section, conclusion and recommendations are explained and the extent to which the research objectives have been achieved. The study focused on the development of an information hiding tool using the image steganography technique, deploying the tool to an ICT security firm where clients can interact with the tool as well as giving their input and testing performance, utility and usability by encrypting and decrypting information.

5.1 Conclusion

The study was able to point out several aspects pertaining to information hiding tools and techniques. The conclusions were closely tied to the objectives indicated below:

5.1.1 Information Hiding Challenges

According to the study, 33% of the ICT consultants together with the end users (who had been taken through the challenges as shown in table 2.1 *Factors Affecting a Steganographic Method*) believed that the number one challenge when it comes to information hiding is payload capacity, 28% perceptual transparency, 20% robustness, 11% temper resistance and 8% computational complexity. This is attributed to the fact that the majority of the existing information hiding tools does not cater for payload capacity and perceptual transparency as this two are absolute requirements for information hiding.

5.1.2 Development of an Information Hiding Tool Using Image Steganography Technique

According to our study, two techniques were able to meet the 60 % requirement, including “Discrete Cosine Transformation Technique (DCT)” and “Discrete Fourier Transformation Technique (DFT)”. The developed tool, Secure Information Hiding Technique (SIHT) was able to meet 80% of the requirements which included: Perceptual transparency, payload capacity, robustness and computational complexity. In this case, the developed tool was not only meeting tamper resistance as part of the requirements for information hiding tools.

5.1.3 Validity, Utility and Usability Testing by Encrypting and Decrypting Information.

Validity testing was in the affirmative since the two modules for encryption and decryption was able to secure a result of “pass”, meaning it complies with the desired results.

On utility testing, the technique positively accepted by the ICT consultants together with the end users as well. From the research findings, a good number of the respondents with an average of 76.59% had a positive attitude towards the tool. Most of them welcomed the tool and they were confident that it would help in hiding information away from unauthorized users.

In usability testing, the technique was positively accepted by the ICT consultants together with the end users. From the research findings, an average of 71.67% users of the respondents had a positive attitude towards the tool. The achieved score of 71.67% is above average, indicating that the usability of the tool was generally agreed by the ICT consultants and end users as well.

5.1.4 Comparison with Other Studies

This study extends previous findings from other studies as indicated in the literature review (Table 2.1 *Factors Affecting a Steganographic Method*), which concurs that the quantity of information transmitted "payload" is important when considering various information hiding tools and techniques.

All the tests carried out above were considered to be above average ranging from 71.67% - 80%. According to Brooke et al. (1996), "a SUS score above a 68% would be considered above average". In this situation therefore, the test scores were considered to be related because of the closeness in the range. This implies that the tool was positively identified and accepted by the users together with the ICT consultants.

The study was able to compare the various algorithms, based on the performance of those algorithms. With respect to the desired attributes, it was easy to come up with algorithmic combination of least significant bit (LSB) and embedding of coefficient bits (ECB). According to Chang et al. (2003), "the advantage of performing image steganography algorithmic combinations is that the cost of cracking the hidden message is extremely increased, the data cannot be easily decoded without the key using image manipulation techniques, any type of image, 8 or 24 bits can be used, there is no increase in the size of the image due to data in it and there are no constraints on the choice of the image" This is considered to be an innovation that has been realized by the study.

5.2 Recommendations

Based on the findings various recommendations were made:

a) The image steganography tool should be put into use in small and medium ICT security firms to secure information from unauthorized users at all times. This can help improve the security of information in such small and medium firms with little or no much revenue to spend on expensive security systems.

b) The image steganography techniques should be used in the design and development of information security systems because based on the study it has proved that it can hide information and transfer it securely over the network with a guarantee of high payload capacity, minimum perceptual transparency, high robustness and low computational complexity.

5.3 Future Research Suggestions

Explore the possibility of coming up with different algorithmic combinations to guarantee temper proof information hiding tools with minimum computational complexity. This can be done with respect to the analysis that was done in the literature review as shown in Table 2.5 (*Algorithms Comparative Analysis).* Also apart from the implementation that was carried out which was utilizing Least Significant Bits and Embedding Coefficient Bits algorithms as shown in section 2.5 (*Algorithmic Combinations*), the other suggested combinations of Pixel Value Differencing vs Distortion Technique and Lossless Reversible vs Masking & Filtering can be implemented.

REFERENCES

1. Adams, A. and Sasse, M.A., 1999. Users are not the enemy. *Communications of the ACM*, *42*(12), pp.40-46.
2. Adhiambo, A.O., 2015. *Influence of information communication and technology tools on the performance of relief aid projects in Kenya: The case of Red Cross organization in Nairobi County* (Doctoral dissertation, University of Nairobi).
3. Babu, K.S., Raja, K.B., Kiran, K.K., Devi, T.M., Venugopal, K.R. and Patnaik, L.M., 2008, November. Authentication of secret information in image steganography. In *TENCON 2008-2008 IEEE Region 10 Conference* (pp. 1-6). IEEE.
4. Bassil, Y., 2012. A simulation model for the waterfall software development life cycle. *arXiv preprint arXiv:1205.6904*.
5. Bennett, K. (2004). Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text.
6. Bhattacharyya, S., Banerjee, I. and Sanyal, G., 2011. Multimedia based Steganography using PMM and M4M. *IJCA Spec. Issue Netw. Secur. Cryptogr.*, pp.24-33.
7. BrahmaTeja, K.N., Madhumati, D.G. and Rao, K.R.K., 2012. Data hiding using EDGE based steganography. *International Journal of Emerging Technology and Advanced Engineering*, *2*(11), pp.285-290.
8. Bromme, R., Rambow, R. and Nückles, M., 2001. Expertise and estimating what other people know: The influence of professional experience and type of knowledge. *Journal of experimental psychology: Applied*, *7*(4), p.317.
9. Brooke, J., 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry*, *189*(194), pp.4-7.
10. Chang, C.C., Hsiao, J.Y. and Chan, C.S., 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, *36*(7), pp.1583-1595.
11. Changder, S., Ghosh, D. and Debnath, N.C., 2010, November. Linguistic approach for text steganography through Indian text. In *Computer Technology and Development (ICCTD), 2010 2nd International Conference on* (pp. 318-322). IEEE.
12. Cox, I.J., Kilian, J., Leighton, F.T. and Shamoon, T., 1997. Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, *6*(12), pp.1673-1687.
13. Dalkey, N. and Helmer, O., 1963. An experimental application of the Delphi method to the use of experts. *Management science*, *9*(3), pp.458-467.
14. Deepa, S. and Umarani, R., 2013. A Study on Digital Image Steganography. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(1), pp.54-57.
15. Dempsey, J. and Rowe, J.K., 2004. Why poststructuralism is a live wire for the Left. *Radical theory/critical praxis: making a difference beyond the academy*, pp.32-51.
16. Doerr, G. and Dugelay, J.L., 2003. A guide tour of video watermarking. *Signal processing: Image communication*, *18*(4), pp.263-282.

17. Doshi, R., Jain, P. and Gupta, L., 2012. Steganography and its Applications in Security. *International Journal of Modern Engineering Research (IJMER)*, *2*(6), pp.4634-4638.
18. Dunbar, B., 2002. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment. *Sans Institute*, *2002*, pp.1-9.
19. Everett, G.D. and McLeod Jr, R., 2007. *Software testing: testing across the entire software development life cycle*. John Wiley & Sons.
20. Fick, D.M., Cooper, J.W., Wade, W.E., Waller, J.L., Maclean, J.R. and Beers, M.H., 2003. Updating the Beers criteria for potentially inappropriate medication use in older adults: results of a US consensus panel of experts. *Archives of internal medicine*, *163*(22), pp.2716-2724.
21. Gay, N.C., 1976. The change of shape of a viscous ellipsoidal region embedded in a slowly deforming matrix having a different viscosity—a discussion. *Tectonophysics*, *35*(4), pp.403-407.
22. Graps, A., 1995. An introduction to wavelets. *IEEE computational science and engineering*, *2*(2), pp.50-61.
23. Herman, G.T., 1979. Image reconstruction from projections. Implementation and applications. *Image reconstruction from projections. Implementation and applications., by Herman, GT. Berlin (FR Germany): Springer, 12+ 284 p.*, *1*.
24. Hu, Y., Lee, H.K. and Li, J., 2009. DE-based reversible data hiding with improved overflow location map. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(2), pp.250-260.
25. Hussein, M.A.A.H., 2014. *Video Data Steganography Based on Discrete Cosine Transform Method* (Doctoral dissertation, University of Baghdad).
26. Jayaram, P., Ranganatha, H.R. and Anupama, H.S., 2011. Information hiding using audio steganography–a survey. *The International Journal of Multimedia & Its Applications (IJMA) Vol*
27. Kabukuru, W., 2010. Mobile banking: Kenya leading a new revolution. *New African*, *494*, pp.76-77.
28. Kan, S.H., 2002. *Metrics and models in software quality engineering*. Addison-Wesley Longman Publishing Co., Inc.
29. Kaur, B., Kaur, A. and Singh, J., 2011. Steganographic approach for hiding image in DCT domain. *International Journal of Advances in Engineering & Technology*, *1*(3), p.72.
30. Kenya, I.C.T., 2013. Authority (2014). *Kenya National ICT Master Plan for 2013/14-2017*, *18*.
31. Khare, P., Singh, J. and Tiwari, M., 2011. Digital Image Steganography. *Journal of Engineering Research and Studies*, *2*, pp.101-104.
32. Kruus, P., Scace, C., Heyman, M. and Mundy, M., 2003. A survey of steganography techniques for image files. *Advanced Security Research Journal.[On line]*, *5*(1), pp.41-52.
33. Kumar, D.A. and Begum, T.U.S., 2011. A novel design of electronic voting system using fingerprint. *International Journal of Innovative Technology & Creative Engineering*, *1*(1), pp.12-19.

34. Langrish, J., Gibbons, M., Evans, W.G. and Jevons, F.R., 1972. *Wealth from knowledge: Studies of innovation in industry*. Springer.
35. Licks, V. and Jordan, R., 2005. Geometric attacks on image watermarking systems. *IEEE multimedia*, *12*(3), pp.68-78.
36. Luo, W., Huang, F. and Huang, J., 2010. Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on information forensics and security*, *5*(2), pp.201-214.
37. Meredith, J., 1998. Building operations management theory through case and field research. *Journal of operations management*, *16*(4), pp.441-454.
38. Morkel, T., Eloff, J.H. and Olivier, M.S., 2005, June. An overview of image steganography. In *ISSA* (pp. 1-11).
39. Morris, T., May, J., Godden, J. and Nicholson, E., 2001. Small/medium enterprise assessment and strategy development. *Bulgaria: US Agency for International Development*.
40. Motameni, H., Norouzi, M., Jahandar, M. and Hatami, A., 2007. Labeling method in Steganography. *World Academy of Science, Engineering and Technology*, *30*, pp.349-354.
41. Mugenda, O. and Mugenda, A., 1999. Research Methods: Quantitative and Qualitative Techniques. *Nairobi: African Centre for Technology Studies*.
42. Mulunda, C.K., Wagacha, P.W. and Adede, A.O., 2013. Genetic Algorithm Based Model in Text Steganography. *The African journal of information systems*, *5*(4), p.2.
43. Orodho, J.A., 1992. Women's Work and the Informal Sector in Kenya: A Study of Some Small-scale Women Enterprises in Mombasa District. *Eastern Africa Social Science Research Review*, *8*(2), p.20.
44. Petitcolas, F.A., Anderson, R.J. and Kuhn, M.G., 1999. Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), pp.1062-1078.
45. Potdar, V.M. and Chang, E., 2004, June. Grey level modification steganography for secret communication. In *Industrial Informatics, 2004. INDIN'04. 2004 2nd IEEE International Conference on* (pp. 223-228). IEEE.
46. Rahmani, M.K.I. and Kamiya Arora, N.P., 2014. A Crypto-Steganography: A Survey. *International Journal of Advanced Computer Science and Application*, *5*, pp.149-154.
47. Sekaran, U., 2006. *Research methods for business: A skill building approach*. John Wiley & Sons.
48. Shapiro, J.M., 1993. Embedded image coding using zerotrees of wavelet coefficients. *IEEE Transactions on signal processing*, *41*(12), pp.3445-3462.
49. Simmons, G.J., 1984. The prisoners' problem and the subliminal channel. In *Advances in Cryptology* (pp. 51-67). Springer US.
50. Tiwari, A., Yadav, S.R. and Mittal, N.K., 2014. A review on different image steganography techniques. *International Journal of Engineering and Innovative Technology (IJEIT)*, *3*(7), pp.121-124.
51. Tsai, P., Hu, Y.C. and Yeh, H.L., 2009. Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Processing*, *89*(6), pp.1129-1143.
52. William, W., 2009. *Research methods in education*. Pearson Education India.

53. Yammarino, F.J. and Markham, S.E., 1992. On the application of within and between analysis: Are absence and affect really group-based phenomena?.
54. Yang, C.H., Weng, C.Y., Wang, S.J. and Sun, H.M., 2008. Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, *3*(3), pp.488-497.
55. Ziglo, M.J., Nelson, A.E., Heo, G. and Major, P.W., 2009. Argon laser induced changes to the carbonate content of enamel. *Applied Surface Science*, *255*(15), pp.6790-6794.

APPENDICES

Appendix A: - User Manual

The user manual contains all essential information for the user to make full use of the information hiding tool. This manual includes a description of the tool functions and capabilities, and step-by-step procedures for system access and use.

1. **Tool Capabilities**

The tool is capable of performing the following operations among others:

i. Encrypting information
ii. Decrypting information

2. **Software Requirements**

   Install visual studio 2008 or above and ensure that the following components are installed and running correctly:

   - Microsoft SQL Server Compact 3.5 SP2 x64 ENU
   - Microsoft.NET Framework 4 Multi-Targeting Pack
   - Microsoft Visual Studio 2010 Express Prerequisites X64 ENU
   - Microsoft Visual C# 2010 Express ENU

3. **Operating Instructions**

   a. **Encrypting Information**

      - Browse for the cover image
      - Browse for the secret file
      - Click encrypt
      - Browse for location of storage
      - Type the file name
      - Click save

   b. **Decrypting Information**

      - Browse for the encrypted file
      - Browse for the location to save the file
      - Click decrypt

APPENDIX B: Cover Letter

Dear User/Staff Member,

My name is Vincent Kipng'etich Koech, a Master's student at The University of Nairobi taking Computer Science. You are invited to participate in a research project under the title: Information Hiding Technique for an ICT Security Firm (Steganography).

The purpose of this research is to get your views from computer users and ICT experts pertaining to security problems that they encounter while interacting with ICT Technologies. This study has been approved by the director of *Smartware Technologies Ltd.*

Please be assured that all the views would be treated in confidence and therefore your personal information should not be written on the questionnaire. Filling this questionnaire would not take more than 10 minutes of your time.

The questionnaire contains eight questions. The findings in this study may be shared on request. Should you have any queries or comments regarding this survey, you are welcome to contact me through:

Vincent Kipng'etich Koech

University of Nairobi

College of Biological and Physical Sciences

School of Computing and Informatics

Cellphone: 0722 280826

Email: vkoech@students.uonbi.ac.ke

Yours sincerely

Vincent Kipng'etich Koech

APPENDIX C: Research Questionnaire

Instruction:

Please answer the questions herein honestly and as simply as possible by either ticking (√) on one of the options or by giving the required needed. Your participation would be highly appreciated.

SECTION A: BACKGROUND INFORMATION

1. Please tick your category: Consultant [ ] End User [ ]
2. Please tick your gender: Male [ ] Female [ ]
3. Please indicate your age bracket:

   Below 18-25 [ ] 26-35 [ ] 36-45 [ ] 46-55 [ ] 56-65 [ ]

SECTION B: LEVEL OF KNOWLEDGE & SKILLS

4. Please indicate academic qualification:
   KCPE [ ] KCSE [ ] Diploma [ ] Bachelors [ ] Masters [ ] PHD [ ]
5. Please indicate your ICT level of experience:
   1-5 Years [ ] 6-15 Years [ ] 16-25 Years [ ] 26-35 Years [ ] 36-45 Years [ ]

SECTION C: INFORMATION HIDING CHALLENGES

6. With respect to information security, which of the following do you think is the biggest challenge when it comes to hiding information. Payload Capacity [ ] Perceptual Transparency [ ] Robustness [ ] Temper Resistance [ ] Computational Complexity [ ]

SECTION D: INFORMATION HIDING TOOLS & TECHNIQUES

7. With respect to information security, which information hiding tool have you interacted with in the past? Biometrics [ ] Cryptography [ ] Finger Printing [ ] Steganography [ ] Water Marking [ ]

8. If your answer was steganography above, please indicate the medium it was using

   Audio [ ] Image [ ] Network [ ] Text [ ] Video [ ]

9. If your answer was steganography above, please indicate the domain it was using
   Distortion [ ] Masking & Filtering [ ] Spatial Domain [ ] Transform Domain

Thank you for taking time to respond to this questionnaire.

APPENDIX D: Utility Questionnaire

Instruction:

With the aid of the steganography tool, for each of the following mark one box that best describes your level of agreement with the solution provided. Answer the questions herein honestly and as simply as possible by ticking (√) on one of the options where applicable.

SECTION A: SYSTEM UTILITY

No	Category	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Using steganography tool saved me time as compared to other solutions					
2.	Using steganography tool helped me improve my data security as compared to other solutions					
3.	Using steganography tool provided timely and speedy transmission of secure data					
4.	Using steganography tool helped me receive timely and speedy, secure feedback from the people I interact with					
5.	Using steganography tool I was able to manage my secure data					
6.	Using steganography tool provided instant and easy access to my secure data					
7.	Using steganography tool I was able to interact with others easily as compared to other solutions					

Provide a reason(s) for any of the categories above if your choice is neutral, disagree or strongly disagree.

a) Neutral ……..……

b) Disagree……..……

c) Strongly Disagree ……...……

Thank you for taking the time to respond to this questionnaire.

APPENDIX E **Usability Questionnaire**

SECTION B: System Usability Scale (SUS) Questionnaire Adopted From Brooke (1996).

Instructions: For each of the following questions tick (√) one box that best describes your answer.

No	Category	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	I think that I would like to use this technique more frequently.					
2.	I found this technique unnecessarily complex					
3.	I thought this technique was easy to use					
4.	I think that I would need assistance to be able to use this technique.					
5.	I found the various functions in this technique were well integrated.					
6.	I thought there was too much inconsistency in this technique					
7.	I would imagine that most people would learn to use this technique very quickly.					
8.	I found the technique very cumbersome to use.					
9.	I felt very confident using the technique.					
10.	I needed to learn a lot of things before I could get going with this technique.					

Provide a reason(s) for any of the categories above if your choice is neutral, disagree or strongly disagree.

a) Neutral ……..……

b) Disagree……..……

c) Strongly Disagree ……...……

Thank you for taking the time to respond to this questionnaire.

APPENDIX F: Code Analysis

```
using System;
using System.Drawing;
using System.Windows.Forms;
using System.IO;

namespace Text2Image
{
    public partial class FrmSteganography : Form
    {
        public FrmSteganography()
        {
            InitializeComponent();
        }

        //public values:
        string loadedTrueImagePath, loadedFilePath,
saveToImage,DLoadImagePath,DSaveFilePath;
        int height, width;
        long fileSize, fileNameSize;
        Image loadedTrueImage, DecryptedImage ,AfterEncryption;
        Bitmap loadedTrueBitmap, DecryptedBitmap;
        Rectangle previewImage = new Rectangle(20,160,490,470);
        bool canPaint = false, EncriptionDone = false;
        byte[] fileContainer;

        private void EnImageBrowse_btn_Click(object sender, EventArgs e)
        {
            if (openFileDialog1.ShowDialog() == DialogResult.OK)
            {
                loadedTrueImagePath = openFileDialog1.FileName;
                EnImage_tbx.Text = loadedTrueImagePath;
                loadedTrueImage = Image.FromFile(loadedTrueImagePath);
                height = loadedTrueImage.Height;
                width = loadedTrueImage.Width;
                loadedTrueBitmap = new Bitmap(loadedTrueImage);

                FileInfo imginf = new FileInfo(loadedTrueImagePath);
                float fs = (float)imginf.Length / 1024;
                ImageSize_lbl.Text = smalldecimal(fs.ToString(), 2) + " KB";
                ImageHeight_lbl.Text = loadedTrueImage.Height.ToString() + "
Pixel";
                ImageWidth_lbl.Text = loadedTrueImage.Width.ToString() + "
Pixel";
                double cansave = (8.0 * ((height * (width / 3) * 3) / 3 - 1))
/ 1024;
                CanSave_lbl.Text = smalldecimal(cansave.ToString(), 2) + "
KB";

                canPaint = true;
                this.Invalidate();
            }
        }

        private string small decimal(string in, int dec)
```

```
        {
            int i;
            for (i = inp.Length - 1; i > 0; i--)
                if (inp[i] == '.')
                    break;
            try
            {
                return inp.Substring(0, i + dec + 1);
            }
            catch
            {
                return inp;
            }
        }

        private void EnFileBrowse_btn_Click(object sender, EventArgs e)
        {
            if (openFileDialog2.ShowDialog() == DialogResult.OK)
            {
                loadedFilePath = openFileDialog2.FileName;
                EnFile_tbx.Text = loadedFilePath;
                FileInfo finfo = new FileInfo(loadedFilePath);
                fileSize = finfo.Length;
                fileNameSize = justFName(loadedFilePath).Length;
            }
        }

        private void Encrypt_btn_Click(object sender, EventArgs e)
        {
            if (saveFileDialog1.ShowDialog() == DialogResult.OK)
            {
                saveToImage = saveFileDialog1.FileName;
            }
            else
                return;
            if (EnImage_tbx.Text == String.Empty || EnFile_tbx.Text ==
String.Empty)
            {
                MessageBox.Show("Encrypton information is incomplete!\nPlease
complete them frist.", "Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
            }
            if (8*((height * (width/3)*3)/3 - 1) < fileSize + fileNameSize)
            {
                MessageBox.Show("File size is too large!\nPlease use a larger
image to hide this file.", "Error", MessageBoxButtons.OK,
MessageBoxIcon.Error);
                return;
            }
            fileContainer = File.ReadAllBytes(loadedFilePath);
            EncryptLayer();
        }

        private void EncryptLayer()
        {
            toolStripStatusLabel1.Text ="Encrypting... Please wait";
```

```
            Application.DoEvents();
            long FSize = fileSize;
            Bitmap changedBitmap = EncryptLayer(8, loadedTrueBitmap, 0,
(height * (width/3)*3) / 3 - fileNameSize - 1, true);
            FSize -= (height * (width / 3) * 3) / 3 - fileNameSize - 1;
            if(FSize > 0)
            {
                for (int i = 7; i >= 0 && FSize > 0; i--)
                {
                    changedBitmap = EncryptLayer(i, changedBitmap, (((8 - i)
* height * (width / 3) * 3) / 3 - fileNameSize - (8 - i)), (((9 - i) * height
* (width / 3) * 3) / 3 - fileNameSize - (9 - i)), false);
                    FSize -= (height * (width / 3) * 3) / 3 - 1;
                }
            }
            changedBitmap.Save(saveToImage);
            toolStripStatusLabel1.Text = "Encrypted image has been
successfully saved.";
            EncriptionDone = true;
            AfterEncryption = Image.FromFile(saveToImage);
            this.Invalidate();
        }


        private Bitmap EncryptLayer(int layer, Bitmap inputBitmap, long
startPosition, long endPosition, bool writeFileName)
        {
            Bitmap outputBitmap = inputBitmap;
            layer--;
            int i = 0, j = 0;
            long FNSize = 0;
            bool[] t = new bool[8];
            bool[] rb = new bool[8];
            bool[] gb = new bool[8];
            bool[] bb = new bool[8];
            Color pixel = new Color();
            byte r, g, b;

            if (writeFileName)
            {
                FNSize = fileNameSize;
                string fileName = justFName(loadedFilePath);

                //write fileName:
                for (i = 0; i < height && i * (height / 3) < fileNameSize;
i++)
                    for (j = 0; j < (width / 3) * 3 && i * (height / 3) + (j
/ 3) < fileNameSize; j++)
                    {
                        byte2bool((byte)fileName[i * (height / 3) + j / 3],
ref t);
                        pixel = inputBitmap.GetPixel(j, i);
                        r = pixel.R;
                        g = pixel.G;
                        b = pixel.B;
```

```
                        byte2bool(r, ref rb);
                        byte2bool(g, ref gb);
                        byte2bool(b, ref bb);
                        if (j % 3 == 0)
                        {
                            rb[7] = t[0];
                            gb[7] = t[1];
                            bb[7] = t[2];
                        }
                        else if (j % 3 == 1)
                        {
                            rb[7] = t[3];
                            gb[7] = t[4];
                            bb[7] = t[5];
                        }
                        else
                        {
                            rb[7] = t[6];
                            gb[7] = t[7];
                        }
                        Color result = Color.FromArgb((int)bool2byte(rb),
(int)bool2byte(gb), (int)bool2byte(bb));
                        outputBitmap.SetPixel(j, i, result);
                    }
                i--;
            }
            //write file (after file name):
            int tempj = j;

            for (; i < height && i * (height / 3) < endPosition -
startPosition + FNSize && startPosition + i * (height / 3) < fileSize +
FNSize; i++)
                for (j = 0; j < (width / 3) * 3 && i * (height / 3) + (j / 3)
< endPosition - startPosition + FNSize && startPosition + i * (height / 3) +
(j / 3) < fileSize + FNSize; j++)
                {
                    if (tempj != 0)
                    {
                        j = tempj;
                        tempj = 0;
                    }
                    byte2bool((byte)fileContainer[startPosition + i * (height
/ 3) + j / 3 - FNSize], ref t);
                    pixel = inputBitmap.GetPixel(j, i);
                    r = pixel.R;
                    g = pixel.G;
                    b = pixel.B;
                    byte2bool(r, ref rb);
                    byte2bool(g, ref gb);
                    byte2bool(b, ref bb);
                    if (j % 3 == 0)
                    {
                        rb[layer] = t[0];
                        gb[layer] = t[1];
                        bb[layer] = t[2];
```

```
                    }
                    else if (j % 3 == 1)
                    {
                        rb[layer] = t[3];
                        gb[layer] = t[4];
                        bb[layer] = t[5];
                    }
                    else
                    {
                        rb[layer] = t[6];
                        gb[layer] = t[7];
                    }
                    Color result = Color.FromArgb((int)bool2byte(rb),
(int)bool2byte(gb), (int)bool2byte(bb));
                    outputBitmap.SetPixel(j, i, result);

                }
            long tempFS = fileSize, tempFNS = fileNameSize;
            r = (byte)(tempFS % 100);
            tempFS /= 100;
            g = (byte)(tempFS % 100);
            tempFS /= 100;
            b = (byte)(tempFS % 100);
            Color flenColor = Color.FromArgb(r,g,b);
            outputBitmap.SetPixel(width - 1, height - 1, flenColor);

            r = (byte)(tempFNS % 100);
            tempFNS /= 100;
            g = (byte)(tempFNS % 100);
            tempFNS /= 100;
            b = (byte)(tempFNS % 100);
            Color fnlenColor = Color.FromArgb(r,g,b);
            outputBitmap.SetPixel(width - 2, height - 1, fnlenColor);

            return outputBitmap;
        }


        private void DecryptLayer()
        {
            toolStripStatusLabel1.Text = "Decrypting... Please wait";
            Application.DoEvents();
            int i, j = 0;
            bool[] t = new bool[8];
            bool[] rb = new bool[8];
            bool[] gb = new bool[8];
            bool[] bb = new bool[8];
            Color pixel = new Color();
            byte r, g, b;
            pixel = DecryptedBitmap.GetPixel(width - 1, height - 1);
            long fSize = pixel.R + pixel.G * 100 + pixel.B * 10000;
            pixel = DecryptedBitmap.GetPixel(width - 2, height - 1);
            long fNameSize = pixel.R + pixel.G * 100 + pixel.B * 10000;
            byte[] res = new byte[fSize];
            string resFName = "";
```

```
            byte temp;

            //Read file name:
            for (i = 0; i < height && i * (height / 3) < fNameSize; i++)
                for (j = 0; j < (width / 3) * 3 && i * (height / 3) + (j / 3)
< fNameSize; j++)
                {
                    pixel = DecryptedBitmap.GetPixel(j, i);
                    r = pixel.R;
                    g = pixel.G;
                    b = pixel.B;
                    byte2bool(r, ref rb);
                    byte2bool(g, ref gb);
                    byte2bool(b, ref bb);
                    if (j % 3 == 0)
                    {
                        t[0] = rb[7];
                        t[1] = gb[7];
                        t[2] = bb[7];
                    }
                    else if (j % 3 == 1)
                    {
                        t[3] = rb[7];
                        t[4] = gb[7];
                        t[5] = bb[7];
                    }
                    else
                    {
                        t[6] = rb[7];
                        t[7] = gb[7];
                        temp = bool2byte(t);
                        resFName += (char)temp;
                    }
                }

            //Read file on layer 8 (after file name):
            int tempj = j;
            i--;

            for (; i < height && i * (height / 3) < fSize + fNameSize; i++)
                for (j = 0; j < (width / 3) * 3 && i * (height / 3) + (j / 3)
< (height * (width / 3) * 3) / 3 - 1 && i * (height / 3) + (j / 3) < fSize +
fNameSize; j++)
                {
                    if (tempj != 0)
                    {
                        j = tempj;
                        tempj = 0;
                    }
                    pixel = DecryptedBitmap.GetPixel(j, i);
                    r = pixel.R;
                    g = pixel.G;
                    b = pixel.B;
                    byte2bool(r, ref rb);
                    byte2bool(g, ref gb);
```

```
                    byte2bool(b, ref bb);
                    if (j % 3 == 0)
                    {
                        t[0] = rb[7];
                        t[1] = gb[7];
                        t[2] = bb[7];
                    }
                    else if (j % 3 == 1)
                    {
                        t[3] = rb[7];
                        t[4] = gb[7];
                        t[5] = bb[7];
                    }
                    else
                    {
                        t[6] = rb[7];
                        t[7] = gb[7];
                        temp = bool2byte(t);
                        res[i * (height / 3) + j / 3 - fNameSize] = temp;
                    }
                }

            //Read file on other layers:
            long readedOnL8 = (height * (width/3)*3) /3 - fNameSize - 1;

            for (int layer = 6; layer >= 0 && readedOnL8 + (6 - layer) *
((height * (width / 3) * 3) / 3 - 1) < fSize; layer--)
                for (i = 0; i < height && i * (height / 3) + readedOnL8 + (6
- layer) * ((height * (width / 3) * 3) / 3 - 1) < fSize; i++)
                    for (j = 0; j < (width / 3) * 3 && i * (height / 3) + (j
/ 3) + readedOnL8 + (6 - layer) * ((height * (width / 3) * 3) / 3 - 1) <
fSize; j++)
                    {
                        pixel = DecryptedBitmap.GetPixel(j, i);
                        r = pixel.R;
                        g = pixel.G;
                        b = pixel.B;
                        byte2bool(r, ref rb);
                        byte2bool(g, ref gb);
                        byte2bool(b, ref bb);
                        if (j % 3 == 0)
                        {
                            t[0] = rb[layer];
                            t[1] = gb[layer];
                            t[2] = bb[layer];
                        }
                        else if (j % 3 == 1)
                        {
                            t[3] = rb[layer];
                            t[4] = gb[layer];
                            t[5] = bb[layer];
                        }
                        else
                        {
                            t[6] = rb[layer];
```

```
                            t[7] = gb[layer];
                            temp = bool2byte(t);
                            res[i * (height / 3) + j / 3 + (6 - layer) *
((height * (width / 3) * 3) / 3 - 1) + readedOnL8] = temp;
                        }
                    }

            if (File.Exists(DSaveFilePath + "\\" + resFName))
            {
                MessageBox.Show("File \"" + resFName + "\" already exist
please choose another path to save file",
"Error",MessageBoxButtons.OK,MessageBoxIcon.Error);
                return;
            }
            else
                File.WriteAllBytes(DSaveFilePath + "\\" + resFName, res);
            toolStripStatusLabel1.Text = "Decrypted file has been
successfully saved.";
            Application.DoEvents();
        }

        private void byte2bool(byte inp, ref bool[] outp)
        {
            if(inp>=0 && inp<=255)
                for (short i = 7; i >= 0; i--)
                {
                    if (inp % 2 == 1)
                        outp[i] = true;
                    else
                        outp[i] = false;
                    inp /= 2;
                }
            else
                throw new Exception("Input number is illegal.");
        }

        private byte bool2byte(bool[] inp)
        {
            byte outp = 0;
            for (short i = 7; i >= 0; i--)
            {
                if (inp[i])
                    outp += (byte)Math.Pow(2.0, (double)(7-i));
            }
            return outp;
        }

        private void Decrypt_btn_Click(object sender, EventArgs e)
        {


            if (DeSaveFile_tbx.Text == String.Empty || DeLoadImage_tbx.Text
== String.Empty)
            {
```

```
                MessageBox.Show("Text boxes must not be empty!", "Error",
MessageBoxButtons.OK, MessageBoxIcon.Error);

                return;
            }

            if (System.IO.File.Exists(DeLoadImage_tbx.Text) == false)
            {
                MessageBox.Show("Select image file.", "Error",
MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                DeLoadImage_tbx.Focus();
                return;
            }

            DecryptLayer();
        }

        private void DeLoadImageBrowse_btn_Click(object sender, EventArgs e)
        {
            if (openFileDialog3.ShowDialog() == DialogResult.OK)
            {
                DLoadImagePath = openFileDialog3.FileName;
                DeLoadImage_tbx.Text = DLoadImagePath;
                DecryptedImage = Image.FromFile(DLoadImagePath);
                height = DecryptedImage.Height;
                width = DecryptedImage.Width;
                DecryptedBitmap = new Bitmap(DecryptedImage);

                FileInfo imginf = new FileInfo(DLoadImagePath);
                float fs = (float)imginf.Length / 1024;
                ImageSize_lbl.Text = smalldecimal(fs.ToString(), 2) + " KB";
                ImageHeight_lbl.Text = DecryptedImage.Height.ToString() + "
Pixel";
                ImageWidth_lbl.Text = DecryptedImage.Width.ToString() + "
Pixel";
                double cansave = (8.0 * ((height * (width / 3) * 3) / 3 - 1))
/ 1024;
                CanSave_lbl.Text = smalldecimal(cansave.ToString(), 2) + "
KB";

                canPaint = true;
                this.Invalidate();
            }
        }

        private void DeSaveFileBrowse_btn_Click(object sender, EventArgs e)
        {
            if (folderBrowserDialog1.ShowDialog() == DialogResult.OK)
            {
                DSaveFilePath = folderBrowserDialog1.SelectedPath;
                DeSaveFile_tbx.Text = DSaveFilePath;
            }
        }

        private void Form1_Paint(object sender, PaintEventArgs e)
```

```
        {
            if(canPaint)
                try
                {
                    if (!EncriptionDone)
                        e.Graphics.DrawImage(loadedTrueImage, previewImage);
                    else
                        e.Graphics.DrawImage(AfterEncryption, previewImage);
                }
                catch
                {
                    e.Graphics.DrawImage(DecryptedImage, previewImage);
                }
        }

        private string justFName(string path)
        {
            string output;
            int i;
            if (path.Length == 3)   // i.e: "C:\\"
                return path.Substring(0, 1);
            for (i = path.Length - 1; i > 0; i--)
                if (path[i] == '\\')
                    break;
            output = path.Substring(i + 1);
            return output;
        }


        private string justEx(string fName)
        {
            string output;
            int i;
            for (i = fName.Length - 1; i > 0; i--)
                if (fName[i] == '.')
                    break;
            output = fName.Substring(i + 1);
            return output;
        }

        private void Close_btn_Click(object sender, EventArgs e)
        {
            this.Close();
        }

        private void linkLabel1_LinkClicked(object sender,
LinkLabelLinkClickedEventArgs e)
        {
            System.Diagnostics.Process.Start("vincentkoech@gmail.com");

        }

    }
}
```