

**Secure Communication Based on
Encryption and LSB Steganography Voice**

الاتصال الآمن لإخفاء الصوت بناءً على التشفير في
البتات الأقل أهمية

By

Emad Tariq Allawi (401320061)

Supervisor

Dr. Sadeq AlHamouz

Master Thesis

Submitted in Partial Fulfillment of the Requirements for the

Master Degree in Computer Science

Department of Computer Science

Faculty of Information Technology

Middle East University

Amman – Jordan

December, 2015

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

رَبِّهِمْ فَاصْبِرْ إِنَّ كِتَابَ اللَّهِ لَهَادٍ لِأُولِي الْأَبْصَارِ
وَالَّذِينَ هُمْ عَنْ آلِهَتِهِمْ كَانُوا عَلَيْكُمْ ذَلِكَ تَقْدِيرُ رَبِّهِمْ
الَّذِي هُمْ كَانُوا بِعِندِهِ لَآتِينَ

(التوبة: ١٠٥)

اللهم لك الحمد كما ينبغي لجلال وجهه وعظيم سلطانه ولك الحمد
والشكر على نعمك التي لا تعد وتحصى .

إلهي لا يطيب الليل إلا بشكرك ، ولا يطيب النهار إلا بطاعتك ، ولا تطيب
اللحظات إلا بذكرك ، ولا تطيب الآخرة إلا بعفوك ، ولا تطيب الجنة إلا
برؤيتك .

إلى من بلغ الرسالة وأدى الأمانة ، ونصح الأمة ، إلى نبي الرحمة ،
ونور العالمين سيدنا محمد صلى الله عليه وسلم .

Authorization statement

I Emad Tariq Allawi Authorize the Middle East University to supply a copy my thesis to libraries, establishment or individuals.

Signature : 

Date: 10/1/2016

اقرار تفويض

انا عماد طارق علاوي أفوض جامعه الشرق الاوسط بتزويد نسخ من رسالتي للمكتبات

اوالمؤسسات او الهيئات او الافراد عنده طلبها.

التوقيع : 

التاريخ : ٢٠١٦/١/١٠

Middle East University
Examination Committee Decision

This is to certify that the thesis entailed "**Secure Communication Based on Encryption and LSB Steganography Voice**" was successfully defended and approved on, 2016.

Examination Committee Members

Signature

Dr. Sadeq AlHamouz (supervisor & Member)

Associate professor, Faculty of information technology
Middle East University (MEU)

Dr. Oleg Vladimirovich viktarov (chairman)

Associate professor, Faculty of information technology
Middle East University (MEU)

Prof. Ahmad T. Al-Taani (external member)

Department of Computer Science
Yarmouk University

Dedication

This thesis is dedicated to all the people who never stopped believing in me.

To My Great Father may god have mercy on him and light his grave.

To My Mother which never stopped supporting me during the journey of my life, to the Mother that made me the man I am.

To My pure hearts Brothers and Sister .

Acknowledgements

I would like to thank my mother and my wife and my kids for their continuous support during my study. I also would like to thank my great supervisor **Dr. Sadeq Al-Hamouz**. in for his support, encouragement, proofreading of thesis drafts, and for helping me throughout my studies, putting me in the right step of scientific research. I would like to thank the Information Technology Faculty members at the Middle East University.

Table of Contents

Secure Communication Based on Encryption and LSB Steganography Voice	I
آية قرآنية	II
Authorization statement	III
اقرار تفويض	IV
Examination Committee Decision	V
Dedication	VI
Acknowledgements	VII
Table of Contents	VIII
List of Figures	X
List of Abbreviations	XII
List of Tables	XIV
Abstract	XV
ملخص	XVI

Chapter One Introduction

1.1 Preface	1
1.2 Problem Statement	2
1.3 Objectives	3
1.4 Motivation	4
1.5 Research questions	4
1.6 Significance of the study and Contribution	4
1.7 Limitations of the Scope	5
1.8 Thesis outline	6
1.9 Background	7
1.9.1 Mobil Devices	7
1.9.2 Steganography Techniques	9
1.9.3 Steganography in Mediums	10
1.9.4 Steganography methods	12
1.9.5 Encryption Techniques	14

1.9.6 Steganography-Encryption Techniques.....	17
1.9.7 Operational Definition.....	19

Chapter Two Literature Review

2.1 Literature review.....	21
2.2 Conclusion or discussion the literature review.....	33

Chapter Three Research methodology

3.1 The Proposed Technique.....	35
3.2 Proposed Methodology.....	39
3.2.1 Sender Algorithm	41
3.2.2 Receiver Algorithm	42
3.3 Summary.....	43

Chapter Four Experimental Results

4.1 Research Tools.....	44
4.1.1 Host Program	45
4.2 Sender procedure.....	45
4.3 Receiver procedure.....	51
4.4 Experimental Results.....	56
4.5 Performance Measures.....	58

Chapter Five Implementation and Results

5.1 Conclusion.....	62
5.2 Future work.....	63
Reference	64
Appendix.....	70

List of Figures

Figures	Page
Figure 1.1 Steganography steps	10
Figure 1.2 LSB coding	14
Figure 1.3 Data Transformation in Serpent	17
Figure 3.1 The proposed Technique	36
Figure 3.2 Sender side	37
Figure 3.3 Receiver side	38
Figure 4.1 Icon Application Interface	46
Figure 4.2 Main Interface	46
Figure 4.3 Browse File	47
Figure 4.4 Path Cover File	48
Figure 4.5 Recorded Audio	48
Figure 4.6 Chooses of Host Program	49
Figure 4.7 Choose Sender	49
Figure 4.8 Send Stego Audio	50
Figure 4.9 Receive Stego Audio	51
Figure 4.10 Notification of New Sound	51
Figure 4.11 Path of Receive Audio	52
Figure 4.12 Media Player Programs	52
Figure 4.13 Listen Recode Audio	53
Figure 4.14 Re-use Main Interface	53

Figure 4.15 Path Stego through Application	54
Figure 4.16 Path StegoOut Application	54
Figure 4.17 Listen Stego Audio	55
Figure 4.18 Notification file	55
Figure 4.19 Graphical comparisons of SNR and PSNR	60

List of Abbreviations

ICT	Information Communication Technology
MDM	Mobile Device Management
LSB	Least Significant Bit
SS	Spread Spectrum
WWW	World Wide Web
AES	Advanced Encryption Standard
IP	Initial Permutation
FP	Final Permutation
DES	Data Encryption Standard
SNR	signal-to-noise ratio
PSNR	Peak signal-to-noise ratio
CD	detail coefficients
CA	approximation coefficients
MSE	Mean squared error
MMS	Multimedia Messaging Service
PVD	Pixel Value Differencing
ARQ	Automatic Repeat Request
MAE	Mean absolute error
GPS	Global Positioning System
GSM	Global System for Mobile Communications
RSA	Rivest, Shamir, Adleman

HAS	human auditory system
HVS	human visual system
LBC	Lowest Bit Coding
WAV	Windows Audio visual
LWT	Lifting Wavelet Transform
SMS	Short Message Service

List of Tables

Table	Page
Table 2.1: shown the result from experimental	23
Table 2.2: The result PSNR from using method in literature review	34
Table 4.1: Explain Results	56
Table 4.2 : Results obtained for 3 bits/sample embedding of encrypt-stego	59
Table 4.3: Results compared	61

Abstract

With the development of Internet community, the multimedia transfer is exposed to different types of attacks, because this transfer occurred in the public communication systems. Daily, thousands of multimedia files are being uploaded and downloaded from many users. Multimedia data like audio takes huge amount of storage space, audio files considered as the most important type of multimedia files that contains sensitive data.

One of the attractive solutions for ensuring secure audio transfer is steganography, which means hiding the secret data in other data without unauthorized users know the existence of the message. Several types of research proposed different algorithms for the embedding and the extraction of a message in audio file. This thesis attempts to enhance the audio steganography by proposing an approach based on audio steganography and encryption techniques.

The proposed approach for hiding the audio from hackers combines steganography and encryption techniques to make the security system robust. The proposed model is implemented by encryption audio using serpent method, then hiding the encryption audio in other audio based on LSB technique.

The obtained results of the proposed study shows when using the voice wav, was time 8 seconds, hidden inside the cover was time 41 second, a frequency 44100 Hz, and 16-bit transfer rate, signal strength 20 dB, Values were as follows: PSNR (60.2855), SNR (35.3686), MSE (0.061195)

Keywords: LSB audio, Encryption; Mobile, Android Operating System, Skype.

الملخص

مع تطور عالم الانترنت، تتعرض وسائط النقل المتعددة لأنواع مختلفة من الهجمات بسبب حدوثها في بيئة مفتوحة وعامة. هناك الالاف من ملفات الوسائط المتعددة التي يتم تحميلها بشكل يومي من قبل العديد من المستخدمين. ويعتبر الصوت احد انواع الوسائط المتعددة التي يستخدم مساحة تخزين كبيرة، والذي غالباً ما يحتوي بيانات هامة وحساسة للمستخدمين، لذلك يجب التركيز على توفير النقل الأيمن له.

احد الحلول المناسبة لضمان نقل الصوت بشكل أمن هو طريقة إخفاء المعلومات، والذي يعرف بأنه طريقة إخفاء البيانات الهامة داخل بيانات اخرى دون السماح للأشخاص غير المخولين من إمكانية معرفة وجود هذه البيانات. هناك العديد من الابحاث التي قدمت خوارزميات مختلفة لتضمين واستخراج البيانات من الصوت. تحاول هذه الأطروحة تحسين إخفاء المعلومات داخل الصوت بواسطة النظام المقترح والذي يعتمد على الدمج مابين تقنيات الإخفاء وتشفير الصوت.

أقترحت هذه الأطروحة نمودجا فعالا لإخفاء الصوت عن المهاجمين، حيث يقوم الباحث بالدمج مابين تقنية الإخفاء وتقنية التشفير لإنشاء نظام قوي وأمن. ويتم تنفيذ النموذج المقترح أولاً عن طريق تشفير الصوت بطريقة (Serpent)، ثم إخفاء الصوت المشفر داخل صوت اخر بواسطة خوارزمية البت الاقل اهمية (LSB).

كما اظهرت النتائج التي تم الحصول عليها من الدراسة المقترحة عند استخدام صوت wav زمنه ٨ ثواني، مخفي داخل غطاء زمنه ٤١ ثانية، بتردد ٤٤١٠٠ هيرتز، وبمعدل نقل ١٦ بت، وبقوة إشارة ٢٠ دسبل، فكانت القيم كالتالي: (SNR (35.3686), PSNR (60.2855),

MSE (0.061195)

الكلمات المفتاحية: البتات الاقل اهمية في الصوت، الموبايل، نظام تشغيل أندرويد، سكايب.

Chapter One Introduction

1.1 Preface

In the recent years, Information and Communication Technology (ICT) field has been in rapid developments, which directly effects in the digital revolution on human life pattern through economic, social and cultural levels.

Mobile applications and services are becoming more popular, such instant message, download of a variety of contents, commerce, banking, and information researches. The result of technology progress has simplified business, enriched entertainment and made personal transactions more suitable by mobile device users. However, it has also opened the door to many of security threats.

The security issues related to mobile devices are different from those relating to computers, e.g. mobile phone may be infected by viruses through instant messages, while personal privacy related to mobile devices is also different. Therefore, there is a large request of researching human factors in mobile data security, especially the antecedents and consequences of users' perception of mobile information security (Liu Y. et al., 2011).

The options for mobile security and enterprises still face unselected challenges, when it comes to investment in the best technology to create security, and managed environments.

The Competitors in the current year's Mobile Data Security classification made up a formidable field of widespread technologies. Items in this classification ranged from mobile access, and platform-specific safety to Mobile Device Management (MDM), and anti-malware tools, as organizations strive to secure important data accessible by there is the mobile workforce.

There are several ways to provide protection for mobile devices, but the best ways to provide protection is to hide information inside other information, that is called steganography. The original information is changed into another form called encryption.

The steganography and encryption utilized as a part of partnerships, governments, and law requirement offices can impart furtively. Encryption secures information and can be discerned; the main thing missing is the mystery key for decoding. Steganography is harder to recognize under conventional movement design examination. Steganography upgrades the security of individual correspondence. Since encryption can be identified, and a few legislatures restrict the utilization of encryption, steganography can be utilized to supplement encryption. Extra layers of security are an advantage to a mystery. In the event, that a steganography message is recognized, there is still the requirement for the encryption key. A shrouded message requires not to be scrambled to qualify as steganography. The strategy for scrambling a message and after that utilizing steganography is mostly utilized by steganography (Yugala, K.2013).

1.2 Problem Statement

Nowadays, the world witnesses a revolution in the field of technological development, especially in the digital devices. The Internet represented multiple solutions to provide knowledge in the connection between different parties, one of these parties is sender, while the other party is receiver, and both parties require high security to reduce risk in the connection, for preventing any intruder from access to the sensitive data.

The problem of intruder is considered a major problem and a threat source to all user-specific information, so it is necessary to develop a mechanism, to provide adequate protection for users working to reduce the risk of hackers, whether the information is important or not.

1.3 Objectives

This study aims at submitting the intruder's resolution of problem on data and transmitting information between parties, which the intruder does through the following steps:

1. Using one of the encryption types for data known as Serpent, which works on encrypting data during the voice recording process by the special program in the mobile.
2. Using one of the Stego types known as Least Significant Bit (LSB), from which the encrypted voice resulted the Serpent process will be hidden.
3. The use of a host program through which the sound output transfers after steganography stage, to the second party.

Therefore, the objective of the encryption use, and steganography together is to increase security and integrity of the data, and the goal of using mediator program is not to make the intruder observe any difference in the size of the data in addition to not locating place, distance, and sample.

1.4 Motivation

The mobile device represents one of the most important transformations of contemporary technology, because it has many properties. Mobile became a replacement solution for many computer users on the Internet, in terms of sending, and receiving information, meet the users' needs, and communicate with each other. This helped in the emergence of many of the problems that threatens the users' acceptance of this technology.

The intruder's problem is considered one of the most important issues that have been focused, due to their risk, and impact on users. So any information exchange process needs security to be able to transfer information easily, and safely through a transmitted encrypted data, and then steganography after that sends it to the second party. This represents a proposal to solve the problem.

1.5 Research questions?

This thesis attempts to solve this problem by focusing on the following questions:

1. Can the proposed technique provide more security of users' audio transfused?
2. What is the effect of using encryption with steganography algorithm in this technique?
3. Will this technique prevent the intruder from detecting protected connections?

1.6 Significance of the Study and Contribution

This thesis is contributed to present a suitable solution for reducing security problem of the audio transmission, and these contributions are summarized as follows:

- 1- Proposing security mechanisms for audio transmission using a combination between encryption and steganography.
- 2- Discussing a variety of issues associated with comparison of data integrity from any type of intruders, and highlights some of these issues with a case study using LSB as steganography and Serpent method as encryption.
- 3- Trying to maintain quality of the service which represents in the audio transmission speed and reducing noise.

The contribution will be clarified in chapters three and four by applying the proposed model with showed the results of experimental.

1.7 Limitations of the Scope

This thesis analyzes the limitations of the relevant audio transmission and proposes some strategies, understanding and investigating the limitations of the secure applications that help researchers to finding better and more robust solutions. The proposed model is implemented to transfer audio between two parties, without observing intruder, by using two devices that support the android operating system. Fixes the limitation of proposed model is presented below:

- 1- Hiding audio through combining steganography and encryption techniques to make the security system robust.
- 2- Encrypting secret audio by using serpent method.

- 3- Hiding encrypted audio by using LSB technique
- 4- Dealing with audio types Windows Audio visual (WAV) extension rather than other audio extensions.
- 5- Chose the Skype program as a host program.

1.8 Thesis Outline

This thesis document contains a number of chapters, in addition to the first chapter, and each chapter has a number of sections:

Chapter two: this chapter presents some of the literature reviews which discuss the previous works in the steganography technique that related with the objective of this thesis.

Chapter three: represents the proposed model, the proposed solution, the supported techniques used in the proposed solution and effectiveness.

Chapter four: this chapter explains the implementation and results of the experimental work.

Chapter five: this chapter summarized conclusion about proposed model, and suggested some ideas for future work to expand this model

1.9 Background

Due to the fast development of computer technology with the internet and the importance of exchanging data between parties, the safety of data transposition in becoming a necessity now days. The data security defined as the protection of data and critical elements, including the systems and hardware that use, store, and transmit that data. In the same time, it aims to ensure business continuity with minimizing business damage by limiting the impact of security incidents (Von Solms, R., and Van Niekerk, J., 2013).

There are several ways to transfer data between the parties; one of these methods is the mobile device. The “smart” devices have been introduced that revolutionized the market. Therefore, many researchers have focused on how to use mobile devices to transfer information securely and they are expecting a major. security incident with mobile phones since there devices become with increased data transmission capabilities and with open and third-party extensible operating systems (Becher, M., et al., 2011).

1.9.1 Mobile Devices

Nowadays, mobile devices are an important part in different fields since they enable the user to access a large variety of ubiquitous services. Where Digital audio players and broadband Internet connections have made it possible for consumers from all around the world to create, exchange and distribute a large digital multimedia files. In addition, sharing digital electronic files using mobile device has grown extremely fast over the last decade (Seleym A., and Darwish D., 2012).

Mobile devices are being widely used by people, especially when adding Internet service, that makes this device is not only used for calling service, but it includes many other services such as; entertainment platform, Global Positioning System (GPS), a small black book and a shopping, and banking tool. in the same time, the mobile phones used has been expanded to send messages, check emails, store contacts, and store important dates.

Mobile communication is vulnerable to security most than wired networks, when the mobile connectivity options have also increased. After standard Global System for Mobile Communications(GSM) , mobile phones now have 3G, 4G, and WLAN connectivity. It means that the mobile users send and receive data packets through wireless method (Zhu, J. et al., 2013).

Although there are a lot of benefits for the mobile, but there are some risks associated with it. The mobile risk includes virus coming from Short Message Service (SMS), Bluetooth and PC, data loss due to theft, or loss of mobile devices, accessed by unauthorized users, and Internet scam or virus infection when accessing network by mobile.

The information transmitted may be vulnerable to interception because the Internet service does not use secure links, thus it is important reduce a chance the information detected during the transmission (La Polla, M. et al., 2013).

With the increase of mobile and Internet communication speech signals which are often used for information transmission, the user needs a strong method to provide security for transmission audio. The mobile services are needed for security services: authentication, integrity, user privacy and non-repudiation, which can be used by a hacker as an access point to the sensitive data.

Although the mobile is used to transfer multimedia data, but the voice transmission is still for the main transmission by a mobile network. The secure voice transmission should be mandatory. Therefore, it should use a strong method to protect secret data for preventing the intruder from understanding the content like Steganography and cryptography (Seleym A., and Darwish D., 2012).

1.9.2 Steganography Techniques

In the recent time, different individuals and organizations have attention for using the secure information through communication media, Steganography one of the tools to provide it. The general concepts of Steganography are the art and science of contact in a way which hides the existence of the communication (Nagaraj, V., et al, 2013).

Steganography which means of Greek origin and essentially means covered writing. Greek words “stegos” meaning “cover” and “grafia” meaning “writing” so it defines as covered writing. Therefore, the steganography is hiding a sensitive data in other data as a cover media with the ability to extract that data lossy or lossless (Nagaraj, V., et al, 2013).

The steganography can shroud media protests as mystery information in other media as spread information, this sight and sound articles incorporates the picture, sound, feature and so on.

Steganography technique used to protect secret data. Previously, this data was hidden on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. While now a day, the sender uses a different method to keep the data confidential to prevent hacking for an unauthorized access of data. There are different steganography techniques

used to protect important data, all techniques use the following terms (Rakhi, and Gawande, S., 2013), as shown in Figure 2.1 .

Cover Media: it is the medium using to hide the presence of secret data.

Secret data: it is the sensitive or important data that should be embedded in other data.

Stego: it is the method in which data is hidden inside other data.

Steganalysis: it is the process by which secret data is to be extracted.

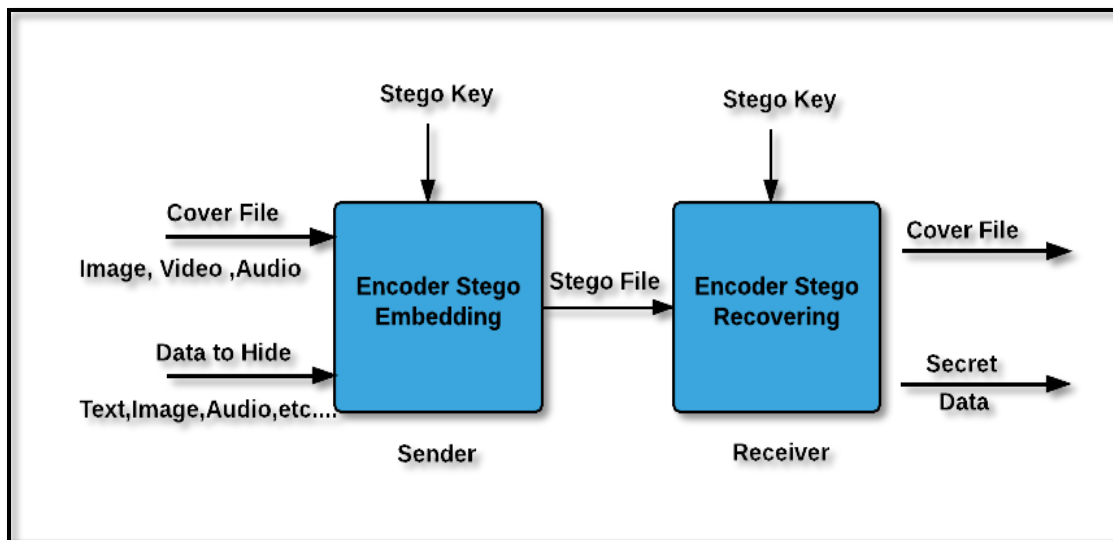


Figure 1.1: Steganography Steps

1.9.3 Steganography in Mediums

Steganography can hide multimedia objects as a confidential data in other media as a cover data, depending on the type of the cover object. That there are many suitable steganography techniques which are followed in order to obtain security, this multimedia

objects includes three major categories of file formats that can be used for steganography (Mandal, P., 2012).

- **Text:** Hiding information in a text is the most important Technique of steganography. The way to hide a secret message in every each letter of every word in a text message.
- **Image:** The images are used as casing objects for steganography. A picture can be represented by a collection of color pixels. The capita pixels can be represented by their optical the properties such as 'brightness', 'chroma', etc. Each of these the properties can be digitally expressed in terms of 1s and 0s. A message is embedded in a digital image through an embedding algorithm, using the confidential key. The output stego image is sent to the receiver. On the other side, it is processed by the extraction algorithm using the same key. Through the transmission of stego image, unauthenticated persons can only notice the transmission of an image, but can't guess the existence of the hidden message.
- **Audio/Video:** In this technique, the secret data is embedded into digitized Audio/Video signal that result for slightly changing in the binary sequence of the file symmetric Audio/Video.

1.9.4 Steganography Methods

Regardless of the type of media that used in the steganography technique, there are a number of steganographic methods that used for this hiding, ranging from invisible ink to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other methods of hiding information, such as (Jayaram P, et al., 2011, Saroha, K., and Singh, P. K. 2010).

1- Least Significant Bit (LSB) Coding

A very popular methodology in the steganography technique is LSB, which considered as the simplest method to embed information in a digital audio file. It replaces some bits (the least important bit) from the secret file in some bytes of original (cover) file to hide a sequence of bytes contains the hidden data.

LSB coding allows for a large amount of data to be encoded. That's usually an effective technique where the LSB replaced doesn't cause important quality degradation, such as in 24-bit bitmaps.

2- Parity Coding

Parity coding used the breaks a signal into Separators samples and embeds each bit of the confidential message from a parity bit. If the parity bit of a selected area does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the area. Thus, the sender has the different selection in encoding the secret bit.

3- Spread Spectrum

The basic Spread Spectrum (SS) technique attempts to disseminate sensitive data over the frequency spectrum of the data signal to the maximum extent possible. This is similar a framework that utilizes an execution of the LSB that spreads the message bits At random over the whole sound file.

However, the SS technique is a different to LSB, because it spreads the secret message over the sound file frequency spectrum by utilizing a code that is free of the genuine sign. As a result, the final signal takes a bandwidth in an overflow of what is actually required for transferring.

4- Echo Hiding

In echo hiding, data is embedded in a sound file by producing an echo into the discrete signal. Echo hiding has advantages of providing a high data transition rate and superior durability when compared to other methods. Only one bit of secret data could be encoded if only one echo were produced from the original signal. Hence, before the encoding process begins, the original signal is split down into blocks. When the encoding procedure is done, the blocks are linked back together to create the last signal.

In this study focused on one of the most important types of media that used in steganography is audio, and using one of the most secreting steganography algorithms is LSB.

The secret messages are being implanted in digital sound by slight change a the binary sequence of a sound (audio) file in audio steganography, where embedding secret messages in digital sound that are usually a more difficult process than inserting messages in other

media, such as digital images. The audio steganography is achieved by controlling the LSB algorithm of each Audio frame by directly replacing the LSBs of the audio samples with the message bits, as shown in Figure 1.2, (Rana, M., and Tanwar, R., 2014).

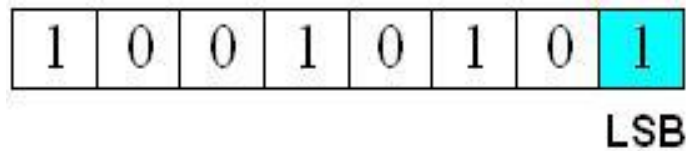


Figure 1.2: LSB coding

The fundamental objective of steganography is to impart safely in a totally imperceptible way and to abstain from attracting suspicion to the transmission of shrouded information. It is not to keep others from knowing the concealed data, yet it is to keep others from feeling that the data even exists. On the off chance that a steganography strategy causes somebody to suspect the bearer medium, and then the technique has fizzled (Rana, M., and Tanwar, R., 2014).

1.9.5 Encryption Techniques

The great development of multimedia data in the digital world, the security of multimedia data is becoming more and more important. One of the major security issues is multimedia data transmitted through the World Wide Web (WWW), such as unauthorized access. In this case, any user needs the cryptography technique which enables the user to transmit multimedia data across any insecure network. Cryptography technique is defined as the encryption and decryption process of text using various mechanisms or algorithms through applied over mathematical function (Rad, R., 2013).

The encryption process is one of the most ways that effects directly in the security field, it is converting original form called a plain-text into an unreadable form called a cipher-text. This cipher-text cannot be easily understood by an intruder and sent across the insecure media (Sheth, R., 2015).

The aim of encryption is considered the methodology of changing plain-text data to cipher-text in order for hiding its meaning and thus prevent any untrustworthy receiver from retrieving the original data, additional to make the cipher-text is unreadable if you do not possess the method to retrieve the information back to original state (Aghajanzadeh, N., et al, 2013).

The cryptography technique divided into two types: the first type is called Symmetric cryptography; the second type is called Asymmetric cryptography techniques. The symmetric-key cryptography is used the same key between parties to achieve the encryption and decryption algorithm while asymmetric-Key cryptography is used two keys: a private key and a public key to achieving the encryption and decryption algorithm (Sheth, R., 2015).

Serpent technique considered as most commonly used in symmetric cryptography to give a suitable security; it is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, the Serpent method is a symmetric key block cipher, Design by Eli Biham, Ross Anderson, and Lars Knudsen. It is considered faster than Data Encryption Standard (DES) and Safer than Triple DES. Its designers combined the design principles of DES with the latest developments of bit-slicing techniques to create a very secure and very fast algorithm.

Serpent utilization bit-slicing to encoding multiple blocks in parallel and also can work with different groups of key lengths. The algorithm's designers boundary themselves to well-understood encoder mechanisms so that they can dependence on the extensive experience and proven techniques of block cipher cryptanalysis (Mona, M., et al, 2014, Rad, R., et al, 2013).

Serpent is a symmetric key calculation that is in view of submitted for AES challenge the strategy works on 128-bit squares of information utilizing as a part of the procedures a 256-bit outside the key. The change stream is separated into 32 uniform rounds rehashed over the information hinder with each round comprising of the (about indistinguishable) succession of basic operations. Each round obliges its uncommon 128-bit round key; following the last round needs two keys, aggregate of 33 diverse round keys are compelled and these are created from the outside key in a different key timetable (Aghajanzadeh, N., et al, 2013).

The encryption process represented changing information. Let P be a 128b plain text, B_i —information. Hinder that enters the i -th round R_i , K_i – the round key, C —encoded cipher text. Before the plaintext piece enters the technique an extraordinary bit reordering purported initial then the Final Permutation (FP) (which is a reverse of IP) is connected to give the cipher-text C . Inside the 32 rounds the genuine encoding is C , as shown in Figure 1.3, (Aghajanzadeh, N., et al, 2013).

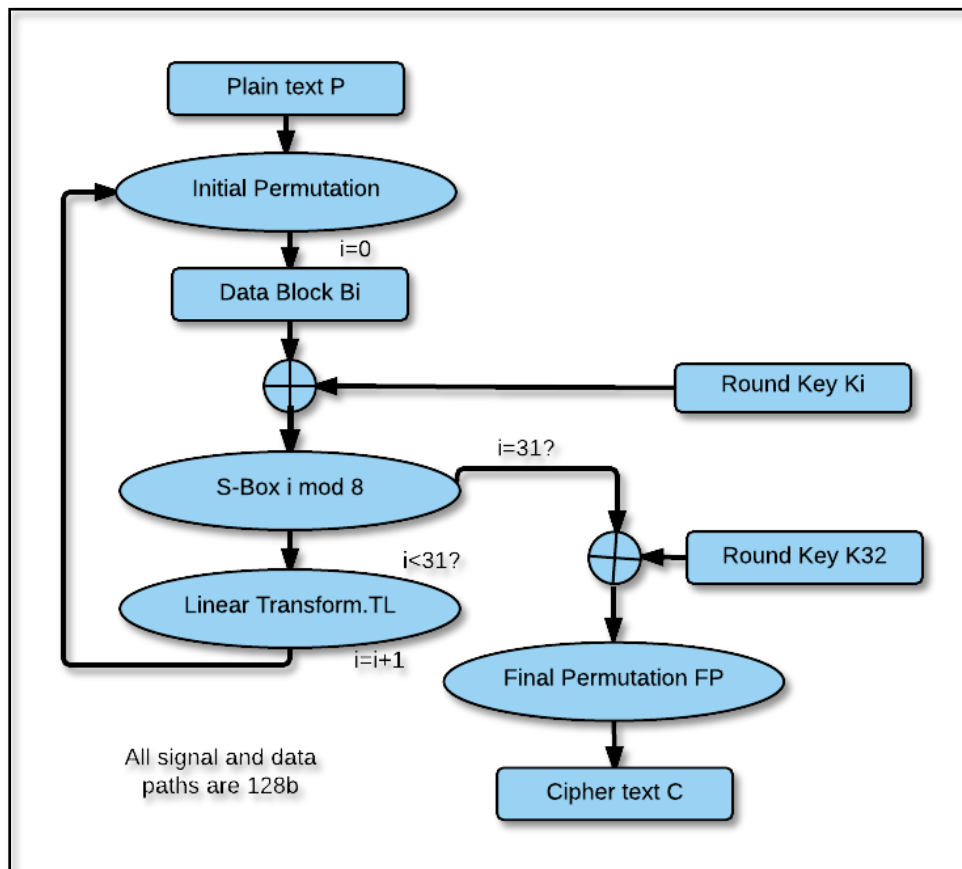


Figure 1.3: Data Transformation in Serpent.

1.9.6 Steganography-Encryption Techniques

With the recent advances in computing technology in our day, the data became a heart of computer communication and the global economy. Thus, the needing for private and personal communication has increased.

For this situation, the security of the information has raised a worry to the individuals. Many methods are heading up to protect the information from diverse assaults and

unauthorized persons. The security issue in computerized correspondence is craved when classified data is being imparted to between two elements utilizing PC correspondence. To give mystery in correspondence the analysts use different systems, Steganography and cryptography are two separate strategies for information security (Gupta, S., et al., 2012).

One of the sorts of correspondence is a cellular telephone that is utilized to diverse individuals, so ought to concentrating on information insurance amid transport starting with one telephone then onto the next and chipping away at join both cryptography and steganography together to make the information concealing framework unbreakable.

In the cryptography framework, the client utilized an encryption key to scramble the message, in spite of the fact that the transmitted this message through the frail open channel, the encryption message is entry to the next side securely, and just the approved client has the suitable unscrambling key to demonstrating the first message (Saeed, M., 2013).

In steganography framework, the mystery message is inserted in another picture or message. Utilizing this innovation even the way that a mystery is being transmitted must be a mystery. The objective of this framework is making the genuine message unintelligible to the spectator (Saeed, M., 2013).

The two technique (Steganography and Cryptography) are different in the technique of data hiding, but they are, in actually, serviceable techniques. Regardless how was sturdy the encryption algorithm, if the secret message is discovered, when that will be exposed to cryptanalysis. The advantage is from combining between Steganography and Cryptography is achieving better security by concealing the existence of an encrypted message. The

resulting steganography can be transmitted without revealing secret information that is being exchanged. However, even if an attacker were to discover the message from the steganography, he at first have to decode the message from digital media, and then he would still require the cryptographic algorithm for decipher the encrypted message (Ahmed, S., Hemachandran, k., 2012).

1.9.7 Operational Definition

1. Mean Square Error (MSE)

It is comparison two signals by providing a quantitative score that describes the degree of similarity, the level of error/distortion between them. One of the signals is an original, while the other is distorted or contaminated by errors. Calculate difference between the original and distorted signals, and quality assessment. Then the MSE may also be regarded as a measure of signal quality, (Wang, Z, and Bovik, A., 2009).

The MSE has many attractive features:

- It is simple.
- It is parameter free and inexpensive to compute.
- The squared error can be evaluated at each sample, independent of other samples.
- It is an excellent metric in the context of optimization.
- The MSE possesses the very satisfying properties of convexity, symmetry, and differentiability.

- The MSE is also a desirable measure.
- It is widely used for assessing a wide variety of signal processing applications, including filter design, signal compression, restoration demising reconstruction, and classification.
- The most often have been compared using the MSE/PSNR. Therefore, it provides a convenient and extensive standard.

2. Signal-to-noise ratio (SNR)

It is used a measure in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power; SNR is typically expressed logarithmically in decibels (dB).It is using measures the quality of a transmission channel or an audio signal over a network channel. The greater the ratio, the easier it is to identify and subsequently isolate and eliminate the source of noise, (Kieser, R, et al.2005).

3. Peak Signal-to-Noise Ratio (PSNR)

It is an expression for the ratio between the maximum possible values (power) of a signal and the power of distorting noise that affects the quality of its representation is usually expressed in terms of the logarithmic decibel scale. Also is most commonly used to measure the quality of reconstruction of lossy compression codecs, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, (Wolf, S. and Pinson,M 2009).

Chapter Two Literature Review

2.1 Literature Review

There are many significant security concerns that need to be addressed when transferring data between the parties. A lot of research has been focused on this area, so presenting a brief of related work that falls within this area.

Alwan, R. H., et al., (2008) a novel approach of image embedding is introduced in this paper. The presented method includes three major steps. First, the image's edge is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used. Finally, a gray level connectivity is implemented using a fuzzy approach and the ASCII code is used for data hiding. The prior bit of the LSB represents the edged image after gray level connectivity, and the remaining six bits represent the original image with very little difference in contrast. The presented method embeds three images in one image and contain as a special case of data embedding, information hiding, identifying and authenticating text embedded within the digital images.

The advantage of the presented method is to keep the original image and the processed ones all in a single file. One of the good compression methods is image-embedding method, in terms of reserving memory space. Moreover, information hiding within digital image can be used for transferring security information. In binary form the two LSBs are used to save text information, coded using ASCII character code.

The eight bits per pixel in an image is another important aspect of the presented method that can be reorganized to represent much information related to the same image or hiding

information. By disturbing two bits only, which it have no effect on the appearance of the image in comparison with the original one.

Al-Taani, A., and Al-issa, A. (2009) in this paper the author suggested a novel steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach is done by dividing the cover into equal sizes blocks and then includes the message in the edge of the block depending on the number of ones in left four bits of the pixel. It is tested on a database that consists of 100 different images.

The major aim of steganography is to hide a message in another one in a way that prevents any attacker to detect or notice the hidden message. The aim of this work is to develop a new method for hiding message in gray-scale images, mainly embedding text data in digital images.

In this paper, the author presented an efficient Steganography path for hiding information within a gray scale image. Two well-known methods were compared by the author, which are PVD and GLM methods. Outcome of experimental results highlighted the impact of the presented method compared with the other methods. In terms of data size PVD method was the best and GLM method was the last. In other results the GLM method proved to be the best while PVD method gave worst results.

Experimental results showed in table (2.1) that the proposed method gave best values for the PSNR measure, which means that there is no difference between the original, and the stegano-images.

Table 2.1: shown the result from experimental

	Size	PSNR
Lena	128	44
	256	47
	512	56
	1024	41
Baboon	128	44
	256	46
	512	49
	1024	50
Peppers	128	43
	256	48
	512	52
	1024	49

This experimental results showed that the proposed approach hide huge information and gave a good visual quality stego-image that can be observed by human eyes.

Mane, A., et al., (2012) explained electronic communication when become an integral and significant part of everyone life because it is simplest, faster and more secure. The study aims is to come up with a technique hiding the presence of a mystery message, and then focused on the steganography as the art of the secret communication. Audio steganography is concerned with hiding data on a cover (host) audio signal in an unperceived way. Hidden data from the stego, or data embedded audio signal, is recovered using a key similar to the one that was employed during the hiding phase.

This study proposed another method of audio steganography by concealing a speech signal inside a music file by bit substitution. The figures also show the closeness of the spectra of unique transporter signal and the carrier signal after embedding the speech inside it. The point of interest of the encoding method is its simplicity. The Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography. The proposed method has been tried effectively on a .wav file at a sampling

frequency of 3000 samples/second with each sample containing 8 bits. Where embedding the message in third LSB and eighth LSB. One can get a clear idea of the two signals. If we compare them, we observe very small changes and these are so small that they cannot be detected when one hears the modified carrier signal. Hence, a very high level of information security is maintained during the transmission of any valuable data.

Gupta, S. et al., (2012) exposed the steganalysis which is the art of detecting the message in the covert communication, and suggested different steganography methods and focused on the LSB steganography. The LSB adjustment technique provides an easy way to inclusion data in images, but the data can be deciphered readily. They used two popular methods; Rivest-Shamir-Adleman (RSA) algorithm and Diffie-Hellman algorithm to encode the information. The results showed that the use of Cryptographic in steganalysis does not affect the time complexity if a Diffie-Hellman algorithm is used rather than RSA algorithm, and this encoding scheme can be used for other steganography methods also.

Deepak, D, et al., (2012) proposed a modification is to the existing LSB algorithm used in audio steganography that increases its robustness, by modifying the least significant of several bytes of an audio file, only minor changes occur in the original sound, most of which cannot be distinguished by the human auditory system. They make use wav files to hide the message since it can be edited and manipulated with ease relatively. The wav file consists of number of channels. In the modified LSB algorithm proposed here, instead of stuffing bit of the message only in the least significant bit in the consecutive bytes of wav file, a pattern is used to stuff bits. Since it is quite easy to encode and decode if we make

use of the same pattern to stuff message bits in different positions of byte in all channels, we stuff the bits in same pattern in all the channels. For example if we use the pattern 3142, then the 1st bit of message is stored at 3rd bit position , 2nd bit of message is stuffed in 1st position, 3rd bit in 4th position, 4th bit in 2nd position, 5th bit in 3rd position and so on.

In this scheme, the authors stuff the entire byte in 1 channel, next the byte in next channel and so on using the same pattern, such as conventional LSB where was stuffing bits in consecutive sequential bytes .This gives the shield against possible attack by trying to read the wav file sequentially.

Hakeem, A. et al., (2014) proposed an approach for hiding secret message into the samples of an audio signal. There are multi-number techniques for audio steganography, where it is focused on the security and payload. When a single technique used, it cannot consider achieving good security and high payload at the same time. In this study, the LSB is used to embed the secret audio in audio samples based on the amplitude of the sample. A threshold is set to decide what number of bits to be embedded in which amplitude sample.

This threshold works as a secret key for the information hidden in the audio samples. The idea is taken from the fact that high amplitude audio samples overrun low amplitude samples which mean that more information bits can be embedded in low amplitude samples and vice versa. This result is showed that the proposed technique hidden a high capacity of information in the standard audio with very simple changes in the standard audio, where the MSE was result (0.00000) and MAE was a result (0.00037).

Mamatha, P, et al., (2014) used the LSB method coding along with the encryption to hide the data in digital audio files. Current technology allows steganography applications to hide any digital file inside any other digital file.

In this study, the researchers used LSB coding gives high bit rate but it is easy to implement and easy to detect. So instead of using simple LSB method alone, combining it with XORing method increases the level of security. This method performs XOR operation on the LSBs and depending on the result of XOR operation and the message bit to be embeds, the LSB of the sample is modified or remains same. The result of this method was MSE 0.00021 and PSNR 36.70 for data of an audio file.

Pradhan, K., and Bhoi, C. (2014) proposed the used to embed text into an audio the proposed system uses LSB technique for the file. The text is encrypted using AES encryption function and data integrity of the audio file will be verified by MD5 hash function. The performance of this system is evaluated through a more secure process based on robustness, security and data hiding capacity.

This study concentrates on a novel randomized steganography algorithm for hiding digital data into uncompressed audio files. The digital message is transformed into ciphertext through the process of the encryption algorithm. For the encryption process, the Author uses AES algorithm. Then the encrypted data is stored in the carrier audio file inside the LSBs of the randomly chosen audio samples. By using a MD5 hash function, the hash is created that is sent to the receiver for verifying the data integrity of the audio file.

As the proposed algorithm is randomized its main advantage being irretrievable in a sense that it is difficult for any third party apart from the original communicating parties to

detect the presence of the secret data into the carrier audio file. The recovery of the sent data is completely in the hands of the proprietor.

The suggested framework for hides messages with provoking minimal auditory degradation. The secured message can be recovered successfully without any mistakes.

The suggested method can be applied for applications that require high-volume robustness versus certain non-malicious attacks. In order robustly hide large volumes of data in audio without causing significant perceptual degradation, hiding techniques must adapt to local characteristics within an audio. The result of this method was PSNR 49.39 for data of an audio file.

Al-Omari, Z., and Al-Taani, A. (2015) this paper shows the different between the digital image steganography and steganalysis. As known the Steganography is the science that involves transferring secret data in a suitable multimedia carrier, e.g., image, audio, and video files, on the other hand Steganalysis is the science of attacking steganography. Away from cryptography technique, security problems can be solved by steganography approach that became the new research hotspot in the field of international information security. The three main evaluation standards of steganography technique are Robustness, imperceptibility, and hiding capacity.

The spatial domains along with the Transform domain are the main image steganography domains. Basically the advantage of the spatial domain is its schemes provide high payload embedding and good visual quality but it is simple and highly vulnerable to security attacks specially the statistical steganalysis, But the transform domain schemes have many more advantages, including its persistence against statistical

attacks along with strong robustness however; they usually hide less capacity of secret information.

Meligy, A. M., et al., (2015) proposed an audio steganography algorithm, for embedding text, audio or image based on Lifting Wavelet Transform (LWT) with modification of LSB technique and three random keys where this key is used to increase the robustness of the LSB technique. The proposed method is tested by Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR). From the result values, they find that using detail coefficients (CD) is better than approximation coefficients (CA) in the embedding process.

This because that CD is high frequencies and the change of it is very low and doesn't make a perceptual effect after reconstructed the audio signal. Also, the SNR values of our proposed method are better than other known methods. The proposed method was implemented and was tested by several audio signals. The secret message used for embedding audio. The authors was calculated the SNR (82.66295) and the PSNR (102.2979) between cover audio and stego, through using a formula to each one.

Saxena, S., (2015) suggested the use of Automatic Repeat Request (ARQ) for error detection & correction. For secure transmission of data, encryption and data hiding are combined in a single step. Host media and secret data are converted into a bit stream. Before encryption of secret data, median filtering is used. The input values are converted to ASCII and then to binary, the host values are converted to binary. Substitution is performed character by character using an encryption key. The LSB of every pixel octet is replaced by

the secret bit stream. Error detection and correction ensures correct transmission of data. In this research are four essential goals as per the following:

1. A message or simply a different image can be hidden in the carrier for scheming out a method for hiding messages in images by slightly modifying the pixel values in an existing image (a carrier).
2. Intended to work in the Fourier /wavelet space instead of the pixel space for extending the schemes to images in graphic formats, which use lossy compression algorithms. Since robustness with respect to small amount of noise and / or to loss of information due to lossy compression is fundamental.
3. The security with respect to known attacks will be investigated by studying the security, efficiency, and robustness of schemes for hiding messages and implementing the algorithms.
4. Exhibiting the execution of the stowing away plans on real imagery.

Gawande, V.,and Deshmukh, R. (2015) proposed a new method for data hiding in binary audio files using optimized bit position to replace a secret bit. This method manipulated blocks, which are sub-divided. The system is considered to be an efficient method for hiding text in audio files such that data can reach the destination in a safe manner without being modified.

In this study, the proposed approach of the system provides a basic view of audio steganography process in sender and receiver side. At the sender side the text message is encrypted by symmetric encryption algorithm is defined an efficient process for providing

security to the message. The encrypted text is passed to embedding phase. In embedding phase encrypted text will be embedded into the cover signal which is in audio format .wav resulting a stego signal. The embedded audio or stego signal contains the encrypted text message which is extracted at the receiver side. When embedding secret message in audio, the size of the message must be lower than audio signal. At the receiver side, stego signal is passed to extractor phase. In extraction process encrypted text will be extracted from embedded audio signal and encrypted text is decrypted.

In decrypter, encrypted text will be decrypted using shared secret key. In symmetric encryption we use either DES or AES. AES provide more security than DES and also choose key size and block size for both encryption and decryption rest of embedding and extraction process is same for both AES and DES.

Jeswani, V. et al., (2015) achieving secure data flow across Android mobiles, accurate time implementation is used for Steganographic algorithm along with encryption. To achieve high-level security for real time Multimedia Messaging Service (MMS) system.

The implement Pixel Value Differencing (PVD) technique with AES encryption on android platform. The security of the data transmission from eavesdropper is one of the important concerns in any communication system. The most effective technique to overcome this security problem and to hide secret information inside some carrier is the steganography. To hide secret information (text, image, audio) an Image is taken as a carrier file and to add more security, encryption is also done on the secret file that will be hidden inside the MMS also The PVD technique is used to hide secret information (text, image, and audio).

Although hiding an image over an image has already been achieved using 4-LSB steganography algorithm but its disadvantage is that the cover image should be of .bmp format and the secret image should be of .jpg format. Meanwhile the effectiveness of this technique is low. But PVD algorithm is used as a solution for this disadvantage; that should provide better security during transferring the data or message(s) from one end to the other end. The main goal of this paper is to extend the data hiding capacity and the data transfer performance as compared to the 4-LSB algorithm hide encrypted secret image inside an image from MMS which acts as a base file having secret data and transmit to the destination securely without any adjustment. Meanwhile there will be a chance for an unauthorized person to modify the data if any deformities occur in the image or on its resolution while inserting the secret message into the image.

Hiding secret data (image, text) into an image from MMS that gives the security during transmission of MMS, PVD steganographic algorithm was successfully implemented. The PVD are found more effective as compared to that of LSB after calculating MSE (3.3) and PSNR (42.9) of the Stego images does the comparison between PVD and LSB algorithm.

Al-Hamami, A., and Hamdi, S. A. (2015) proposed the use of LSB in mobile computing by applying two android mobiles that backing the android working framework, and afterward transferred by the host program. The fundamental objective of utilizing the host project is for transmitting the sound between two gadgets and every gadget situated on an independent system.

The creator is managing LSB system to conceal mystery sound in another sound for assurance sound from any dangers, the capacity of this strategy is concealed every bit from

mystery sound into the last bit every byte from spread sound to create the stego sound. At that point exchange the stego sound to another gathering by utilizing android portable through utilizing one kind of the host program.

There are essential focuses recorded as the accompanying:

1. The sound is managing WAV expansion instead of different sorts of sound augmentation; on the grounds that WAV augmentation contains unique sound with no increases. While the other sort of sounds, as MP3, contains Pressure sound that can be returned the unique sound.
2. The Skype project picked as a host system to exchange sound for some reasons: first, it can exchange sound record without worried about the size or sort of the sound, second, it is anything but difficult to be utilized and neighborly. Third, it is accessible in numerous gadgets and can be utilized as a part of any working framework, While alternate sorts of the host projects support diverse media transmission, however, they don't bolster append document.

Al-Obaidi, F., and Ali, A. (2015) proposed the use LSB to hide message into multiple audio files and this thing is achieved by 1st, 2nd, 3rd, and 4th bits hiding ratios. In comparison between the used bits, hiding results show that the use of 1st bit in LSB method for embedding data is much better than those used bits as expected also according to the results, file's size affects strongly upon the effectiveness of the embedding process while hiding starting position doesn't affect upon the variation of the adopted statistical estimators regardless to which bit is used. Between the statistical estimators that have been adopted here and in testing hiding process, the MAE seems to be the best one.

LSB coding method is proposed among different approaches to hide a secret message inside an audio file and by replacing the first, second, third and fourth bit of the audio file (WAV format) LSB achieved respectively with its equivalent bit in the binary message. The above-mentioned process begins from the starting hiding position that is only known by the encrypted and recipient persons.

A new-audio file having a message hidden into it can be sent successfully by using different ways of LSB technique without any fear of eavesdropper. Starting hiding position doesn't affect upon the statistical estimators in their variation regardless to which bit is used. Results show that MAE can be used as a best estimator in testing hiding process. After all one can ensure that 1st bit in LSB technique is better than other used bits in hiding process. The result of this method was PSNR 46.39 for data of an audio file.

2.2 Conclusion or discussion the literature review

The technological development occurred in the field of Internet and mobile devices led to risks that had both a positive and negative effect, while the positive effect was in terms of security, especially in the area of surveillance; the negative effect was in terms of hacking, mainly the people who always seeking to access others private information.

In this study, several studies were reviewed in the field of security, as shown the table (2.2), since the user reluctant to reveal the voice message by other people but to the receiver as it may contain important information belong to the user only; the main subject was on securing voice transmission via the Internet by the mobile device.

Table 2.2 : The result PSNR from using method in literature review

Name of Researchers	Number of bit	MSR	SNR	PSNR
Mamatha, P. G., (2014)	4 LSB	0.00021	—	36.70
Vineet Jeswani(2015)	3LSB	3.3084	—	42.9346
Fatin, E. M, (2015)	3 LSB	—	35	59

Some studies have focused on providing a solution through the use of encryption or concealment of each proposal solution to the intruder problem, which was a confidence source for some users; but others did not find their needs due to the importance of the information that the user wants to send,

The proposed solution in this study will be by using one of the encryption methods with concealment techniques to get the system through which the information can be transferred safely that will be presented in the next chapter.

Chapter Three Research methodology

This chapter proposes a new method to hide audio WAV inside audio WAV with using 3 bit using LSB technique , after encrypted audio by serpent using key 1024 bits, then send by host program Skype.

3.1 The Proposed Technique

Many researchers presented several solutions to avoid intruder's problem for many used programs in the computers or mobile devices, through technological and programming techniques. This study propos a new technique to solve the intruder's problem, which is always trying to view the sent data by focusing on one of the used encryption methods known as the (serpent), in addition to use the LSB, Figure 3.1 shown the overall design of the proposed technique.

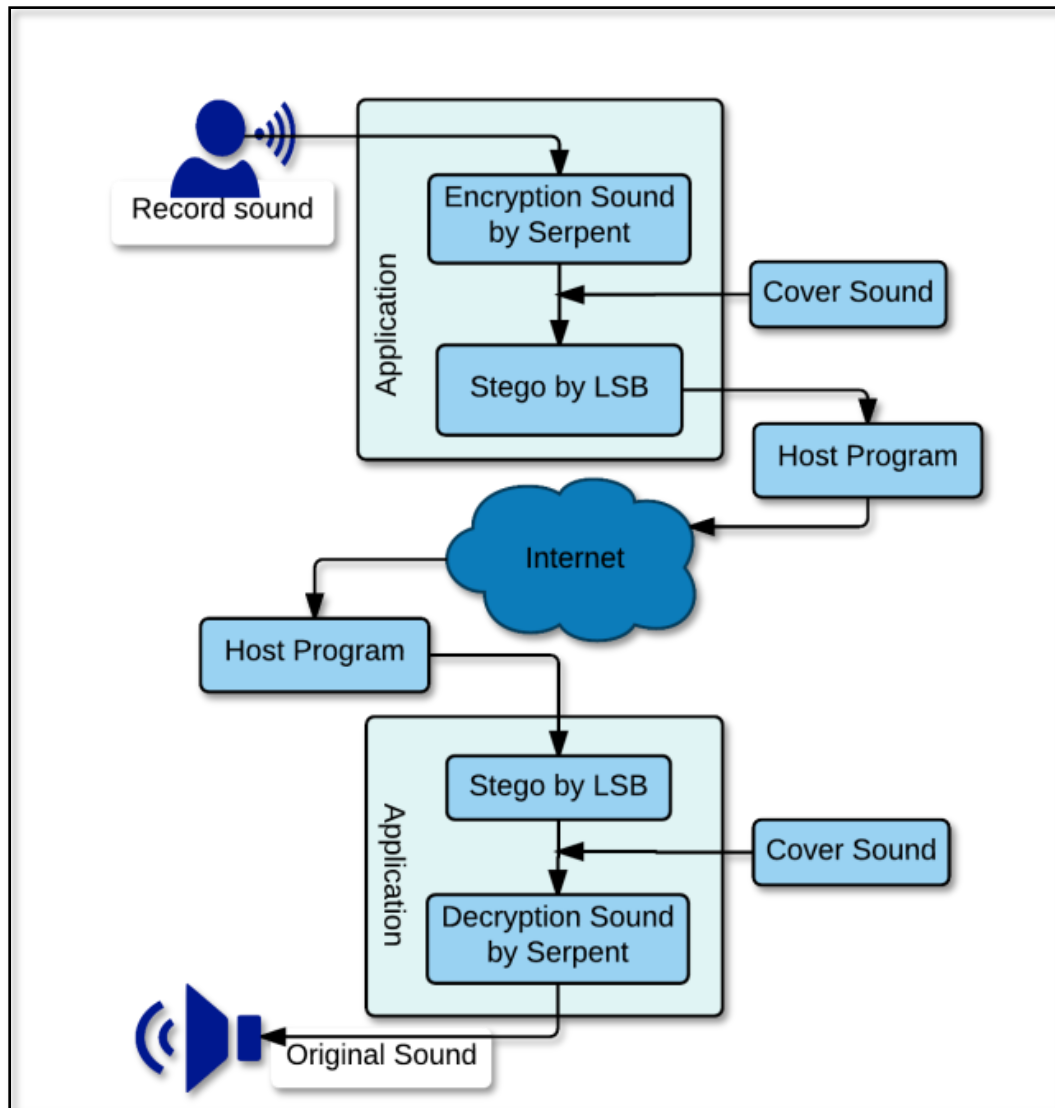


Figure 3.1: The proposed technique

The proposed technique consists of two phases, the sender side and the receiver side as listed below.

1. Sender side

This phase declares all the steps that occurred in the sender side, where it had a secret audio that would like to deliver the other party, by any way, without exposing for dangerous.

In this phase, the proposed solution is implemented through several steps. Firstly, it is selected cover of WAV type from the mobile library to hidden other audio inside it by steganography technique. Secondly, it recorded the desired audio then encrypts it by serpent method, because it has a strong encryption property represented in a key size. Finally, it used LSB technique to hide the encrypted audio in to cover audio to prepare the result for sending it to the receiver side by the host program; all the steps are shown in Figure 3.2.

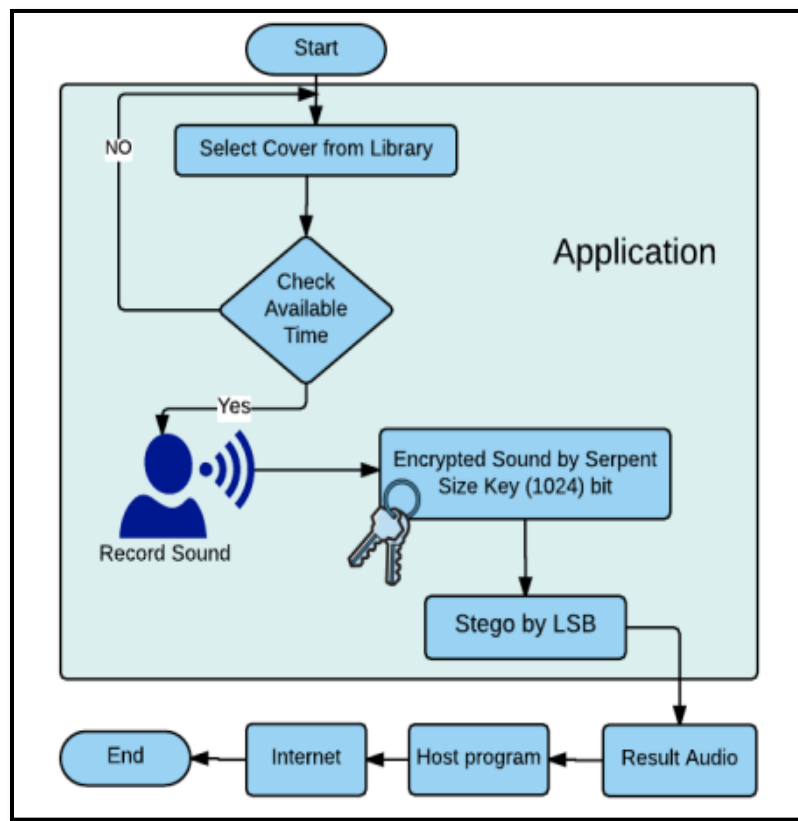


Figure 3.2: Sender side

2. Receiver side

This procedure declared all the steps that had occurred in the receiver side. The receiver side have received the unknown audio by the host program after that checking was done whether it had a stego audio or not.

The receiver procedure applied the proposed solution through several steps, beginning with removing the cover audio, and retrieving the encrypted secret audio, after that the receiver decrypts the hidden WAV sound; all the steps are shown in Figure 3.3.

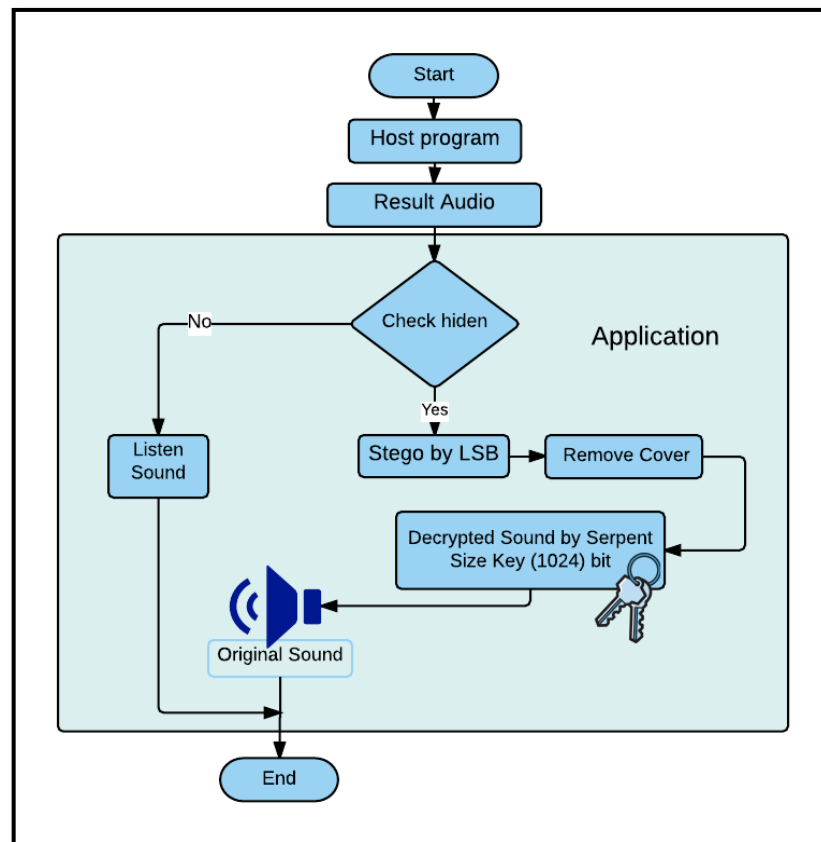


Figure 3.3: Receiver side

3.2 Proposed Methodology

The proposed model is implemented for protecting sensitive data or information from any attacks by combining between steganography and encryption techniques. This combining is running through encrypted secret data by the serpent method, then divides the cover audio into bytes to achieve the framework model when applied on 3 bytes together utilized LSB technique. This framework integrates between encryption and steganography techniques as explained below:

Step1: Audio.

Step2: Applying model for each three bytes

Step3: Dividing first byte into two sides:

The first side: contained 5 bits original audio.

The second side: contained 3 bits, but dividing to three bits:

The first bit empty.

The second bit included secret audio.

The third bit included key for serpent encryption.

Step4: finish first byte.

Step5: Dividing second byte to two sides:

The first side: contained 5 bits original audio.

The second side: contained 3 bits, but dividing to three bits:

The first bit included secret audio.

The second bit empty.

The third bit included key for serpent encryption.

Step6: finish second byte.

Step7: Dividing third byte to two sides:

The first side: contained 5 bits original audio.

The second side: contained 3 bits, but dividing to three bits:

The third bit included key for serpent encryption.

The second bit included secret audio.

The first bit included secret audio.

Step8: finish third byte.

Step9: if complete audio go to step10 then is not go to step2.

Step10: finished.

This step is applying through when divided into two algorithms (Sender algorithm and receiver algorithm).

GZIP: Is a file format and a software application used for file compression and decompression created by (Jean-Loup Gailly and Mark Adler), a free software for compression. Can be applied to any stream of bytes, achieving compression rates of as high as 70-90% for larger files, (James Hoo, 2015).

The proposed model is divided into two algorithms (Sender algorithm and receiver algorithm).

3.2.1 Sender Algorithm

Sender algorithm is implemented in the sender side; the algorithm hides a secret audio inside cover audio, the first point is checking the size of the cover, the cover size have to be 3.75 bits from 8 bits of the secret size, plus (88) bits, this algorithm is divided into four steps:

Step 1: Preparing the audio by choosing the cover audio from library and recording the secret audio by the user.

Step 2: generating random key ,then encrypting secret audio by serpent method after that come the compression encrypted audio by GZIP program.

Step 3: Embedding encrypted audio inside cover audio by LSB technique through a divided result audio per 3 bytes:

- First byte is divided into two parts, one for original audio, and the other is divided into three bits (third bit for serpent key, second bit for secret audio and first bit is empty).
- Second byte is divided into two parts, one for original audio, and the other is divided into three bits (third bit for serpent key, second bit is empty and first bit is for secret audio).
- Third byte is divided into two parts, one for original audio, and the other is divided into three bits (third bit for serpent key, second and first bits for secret audio).

Step 4: Sending the stego audio to the other party using the host program.

3.2.2 Receiver Algorithm

Receiver algorithm is implemented in the receiver side; it is retrieval secret audio from audio recipient. The first point is checking the presence of the "SECRET" word input audio to check whether the audio has a hidden text or not. This algorithm is divided into four steps:

Step 1: Checking the recipient audio from the sender, through the existence of the secret word that indicates to the hidden audio. If the recipient audio is stego then goes to step two, else exit.

Step 2: Retrieving encrypted audio from stego audio by LSB technique through a divided result audio per 3 bytes:

- first byte is divided into two parts, one retrieving in the original audio, and the other is divided into three bits and retrieving the second bit in the secret audio.
- second byte is divided into two parts, one retrieving in the original audio, and the other is divided into three bits, and retrieving the first bit in the secret audio.
- third byte is divided into two parts, one retrieving in the original audio, and the other is divided into three bits, , and retrieving the second and first bits in the secret audio.

Step 3: implementing de-compression of the encrypted audio by GZIP program, then decryption the result through the serpent method by key random.

Step 4: listening to the result audio (secret audio).

3.3 Summary

In this research, the model for transmitting audio is presented. It introduces a technique to protect a recorded audio transmitted over a network. The methodology summarized a process and applied solution to the intruder's problem, who works to access the sound transferred by mobile, listens them and discovers their content, where represented the applied solution process through beginning to encryption process after recording the original sound by the use of the serpent, then hiding sound the output of encryption by using LSB which used another Bit only.

The applied part of the model lies between two mobiles; each mobile contains android operating system, and choosing the Skype program as a host program to transfer audio between them.

The transfer process occurs between two parties, sender and receiver. The sender records audio to transfer it to the receiver, whether the other party is online or not, as long as the two parties have the same application used to hidden data.

Therefore our model includes two procedures:

- Sender procedure: this procedure, occurs in the party that has important audio to hide and send it to the other party.
- Receiver procedure: this procedure, occurs in the party that receives the stego audio and retrieves the original audio from it.

Chapter Four Experimental Results

4.1 Research Tools

Android is an operating system based on the Linux kernel with the user interface. Android's source code is released by Google under open source licenses.

Android 4.1 (Jelly Bean) is announced by Google at the conference on 27 June 2012. Jelly Bean was an incremental update with the primary aim of improving the functionality and performance of the user interface. There are many features as listed in the following, that updating the features from the previous versions:

- Lock/home screen rotation support for the Nexus 7.
- One-finger gestures to expand/collapse notifications.
- Bug fixes and performance enhancements.

In the study we have used the following devices:

- HTC Desire 600(operating system: Android, CPU: 1.2GHz and RAM: 8GB).
- HTC Desire 500 (operating system: Android, CPU: 1GHz and RAM: 4 GB).
- Samsung S5 (operating system: Android, CPU: 2.5 GHz and RAM: 2 GB).
- A router of 108 megabytes per second.
- A router of 54 megabytes per second.
- A router of 150 megabytes per second.

4.1.1 Host program

The experiment is implemented by using devices that support the android operating system, and then choosing a host program. The main goal of using the host program for transmitting the audio between two devices only, and each device is located on separate network.

The host program is two types, the first type is flexible in process sending and receiving the data on shape attached file such as the Skype or yahoo messenger program, while the second type is a fixed data type (do not support attach file) for using send and receive such as social media program.

In this research, applying on the first type where is choosing the Skype for many reasons:

- Transferring audio file without any concern about the size or type.
- Easily used.
- Using in any operating system.

4.2 Sender procedure

The user installs application in the smart phone mobile by using android operating system, this application is called “Sound Encrypt”, as shown in Figure 4.1 .



Figure 4.1: Icon Application Interface

When the user uses the Sound Encrypt application, the application interface that browses two choices to the user; encrypt icon and Decrypt icon. If the party that uses the application is the sender, his/her should choose the Encrypt into icon, as shown in Figure 4.2.



Figure 4.2: Main Interface

The user starts using the application by choosing Encrypt into the icon. The application browses different programs which exist in the smartphone. The user chooses “ES File Explorer” browser program to view the audios that exist in the mobile to the user, as shown in Figure 4.3.

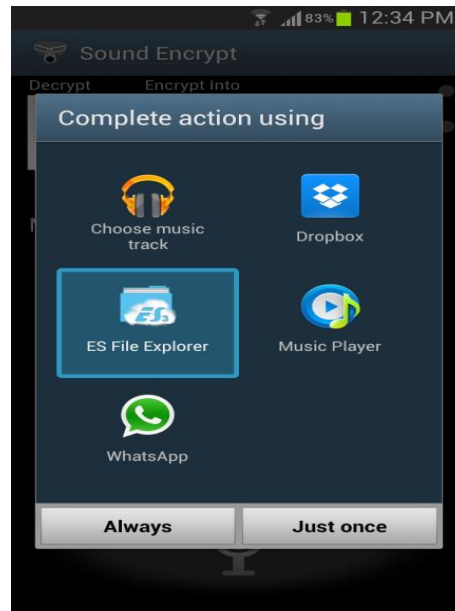


Figure 4.3: Browse File

The browser program views many audios that exist in the smartphone, and it is only WAV extenuation. The user chooses one of the audio to use it as a cover to embed the recorded audio, and to browse the path of this audio to the user, as shown in Figure 4.4 .

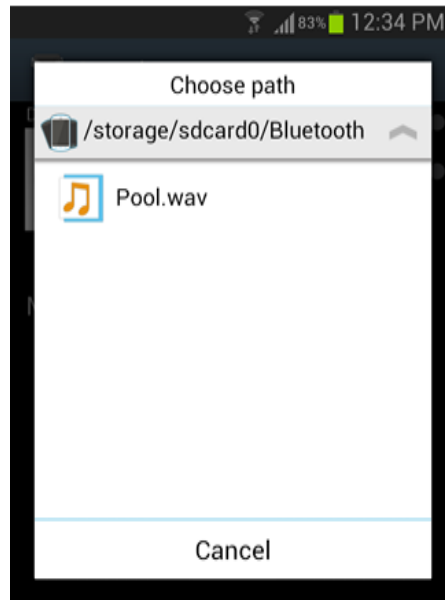


Figure 4.4: Path Cover File

Depending on the size of the cover, the application determines the maximum time which allows the user to record audio in it. The user begins recording the audio as a secret audio in the specified time, as shown in Figure 4.5 .

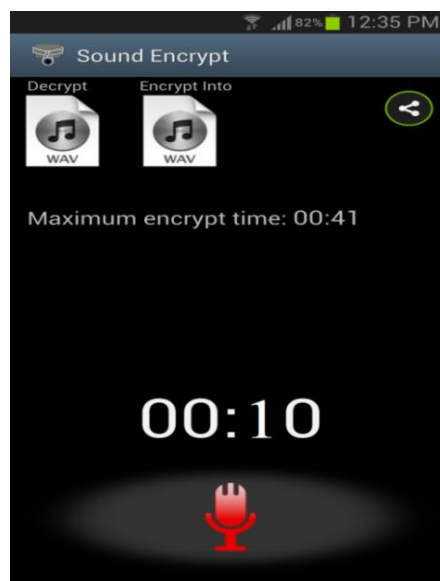


Figure 4.5: Recorded Audio

The application embeds a secret audio in the cover audio to produce the stego audio. The user chooses the Skype program as a host program to transfer audio to the second party, as shown in Figure 4.6 .

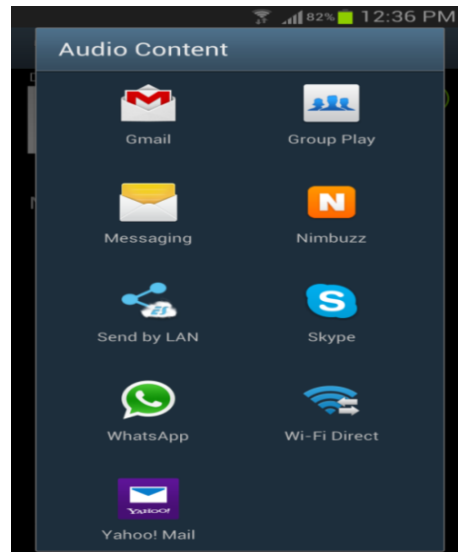


Figure 4.6: Chooses of Host Program

The user uses the Skype program and determines appropriate user-name to the second party, as shown in Figure 4.7 .

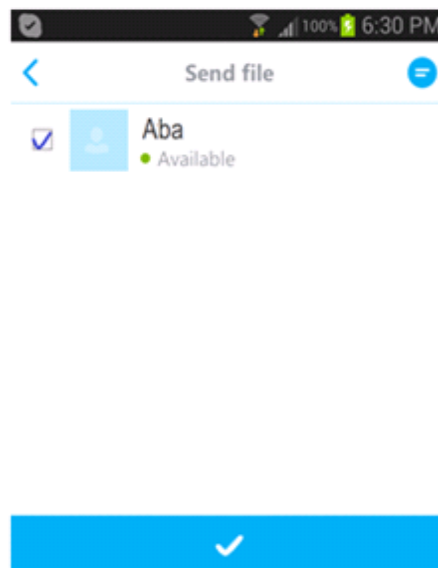


Figure 4.7: Choose Sender

The sender uploads the stego audio as an attachment to send it to another party, as shown in Figure 4.8 .

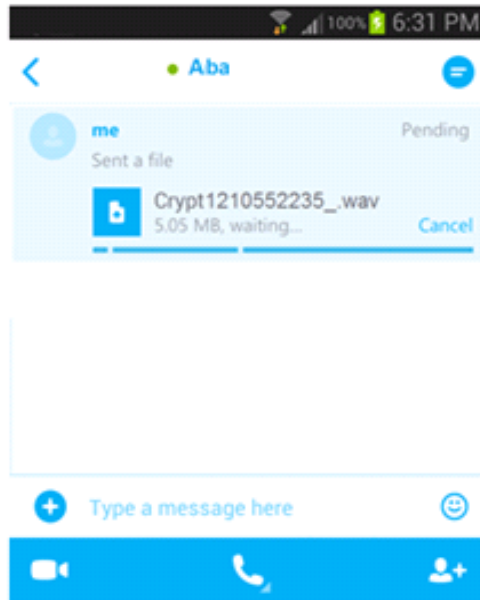


Figure 4.8: Send Stego Audio

4.3 Receiver procedure

The second party (receiver) uses the Skype program, as the sender, to receive and download the stego audio, as shown in Figure 4.9 .

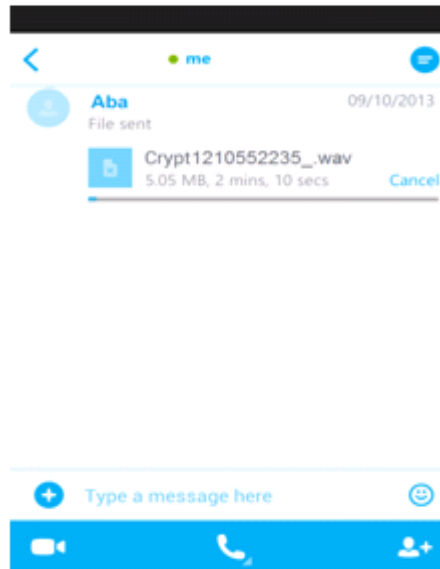


Figure 4.9: Receive Stego Audio

When the receiver uses the Skype program, the application will browse an alert to the user to check existence of a new stego audio and the path of it, as shown in Figure 4.10 .

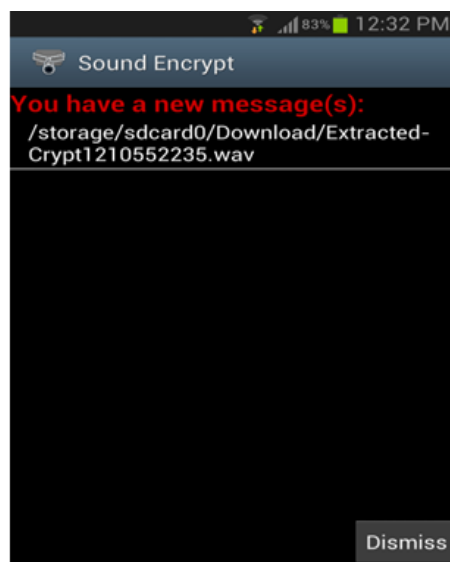


Figure 4.10: Notification of New Sound

The user uses the path of the new stego audio to download it in the smart phone, as shown in Figure 4.11 .

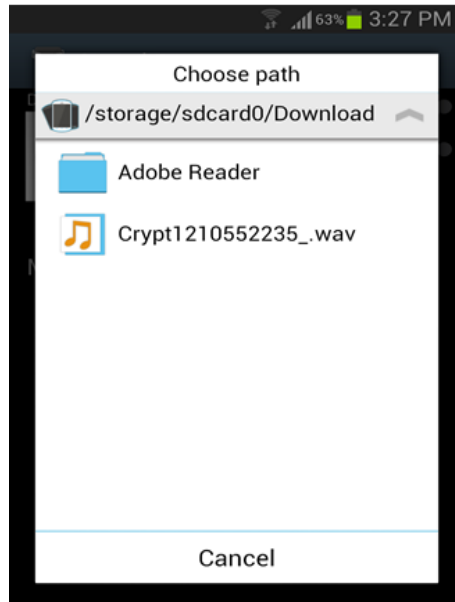


Figure 4.11: Path of Receive Audio

After downloading the new stego, the application decrypts stego audio, retrieves the original audio and appears views of media player programs to the user to determine which program is used to listen to the secret audio, as shown in Figure 4.12 .

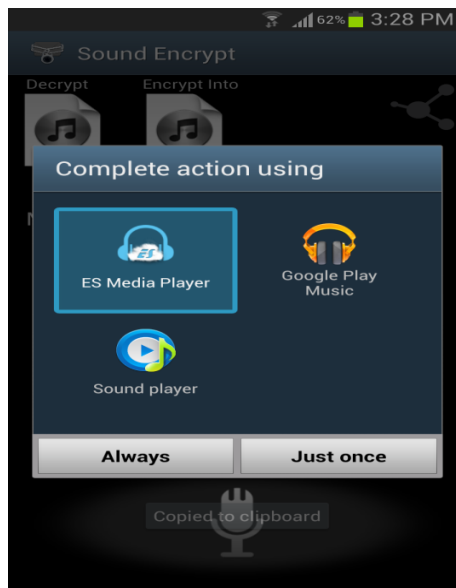


Figure 4.12: Media Player Programs

The application shows the secret audio that turned on as normal audio without noise, as shown in Figure 4.13.

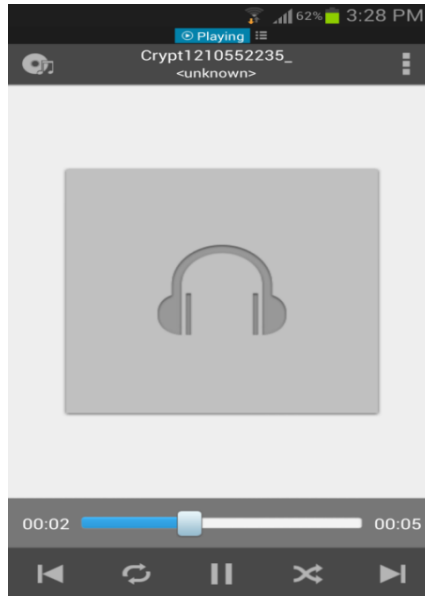


Figure 4.13: Listen Recode Audio

If the user wants to listen to the secret audio in any time, he/she should the user use the application and repeat all the steps on the receiver again, as shown in Figure 4.14.



Figure 4.14: Re-use Main Interface

The user uses the previous path of the required stego audio and downloads, it downloads as a folder through the application, as shown in Figure 4.15 .

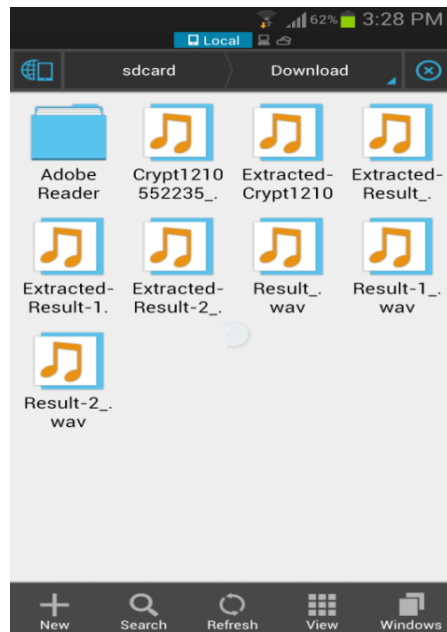


Figure 4.15: Path Stego through Application

The user can use the previous path of the required stego audio and listen to it directly without using the application, as shown in Figure 4.16 .

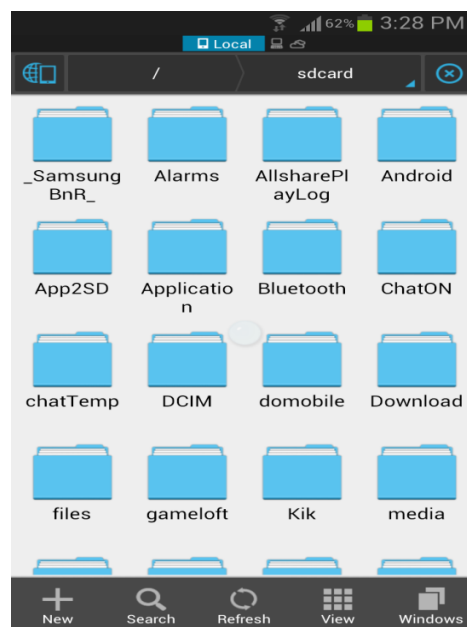


Figure 4.16: Path Stego Out Application

Then the user listens to the stego audio as it is received from the sender, as shown in Figure 4.17 .

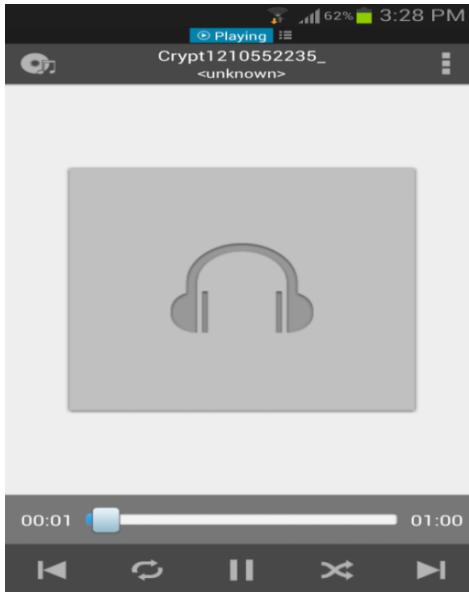


Figure 4.17: Listen Stego Audio

If the user chooses the audio that doesn't contain another audio, the application shows a message to the user as an alert that there is no secret audio in the selected audio, as shown in Figure 4.18 .

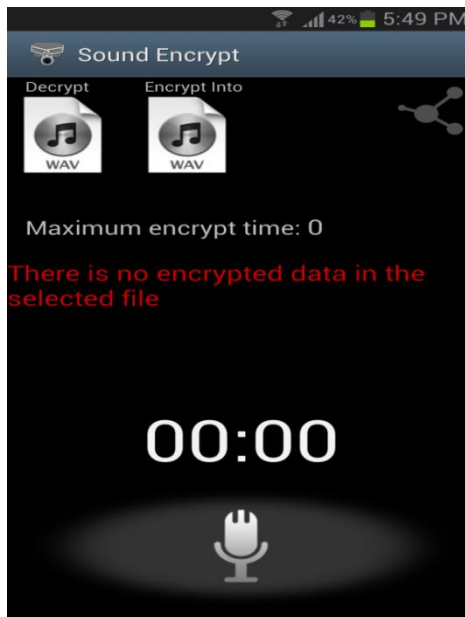


Figure 4.18: Notification file

4.4 Experimental Results

The proposed technique is evaluated of different mobile devices with different routers; Table 4.1, shows the results of both the encryption and decryption phases' interns of required time.

Table 4.1: experiment results

Secret Length(s)	Encryption side		Decryption side	
	Serpent Encryption Time (ms)	Stego Time (ms)	Decrypt Time (ms)	Extract Time(ms)
1	33	44	246	40
2	34	41	219	31
2	73	55	236	32
3	90	64	286	50
3	84	78	252	36
3	71	95	208	25
5	319	220	1908	70
5	247	137	1409	41
5	73	189	329	123
5	183	75	541	68
5	150	214	622	58
5	140	116	464	80
5	85	189	560	68
5	165	103	1155	39
5	156	138	476	42
5	106	107	316	35
10	429	260	2151	72
10	146	317	481	122
10	394	440	1458	278
10	311	274	1295	116
10	280	377	1192	234
10	170	150	1223	53
10	330	427	1054	181
10	237	231	789	189
10	637	378	2371	194
10	493	205	1774	78

Table 4.1: experiment results

20	291	550	1078	188
20	730	427	2190	244
20	600	520	1832	368
20	560	634	3397	511
20	340	602	1054	255
20	660	548	3999	190
20	621	753	2577	222
20	474	300	1788	94
20	858	880	4831	361
20	566	861	2503	388
30	1343	2415	4636	739
30	946	562	4392	268
30	510	1280	1765	400
30	990	691	6076	210
30	710	1134	3660	445
30	1910	928	12379	295
30	1478	877	10054	275
30	436	674	3086	242
30	1095	897	6598	761
30	900	756	3596	237

Previous results presented when the proposed model is implemented on the same audio in different time and device, and the experiment results applied into two procedures, the first procedure is encryption process that is representing a serpent encryption time and steganography time, other procedure is decryption process that is retrieving the secure audio.

These results is measured the steganography, encryption and decryption time and audio recorded time, in addition to, the proposed model using the audio frequency is 44100 Hz, bit rate is 16 bit and the audio type is WAV.

4.5 Performance Measures

Extensive study has been made on the audio used in this technique. After executing the steganography and encryption algorithm the quality of each output stego audio is examined using a different metrics.

1. Mean Square Error (MSE)

The mean square errors defined between stego audio signal and cover audio signal. The distortion in the audio signal can be measured as follows, (Sundar, A. 2015).

$$MSE = \frac{1}{n*m} \sum_{i=1}^n (\hat{Y}_i - Y_i)^2 \quad (1)$$

2. Signal to Noise Ratio (SNR)

It is a measure that compares the level of a desired signal to the level of noise. And it is defined as the ratio of signal power to the noise power. Mathematically represented as follows,(Sundar, A. 2015).

$$SNR = 10 \log_{10} \frac{signal}{noise} \quad (2)$$

3. Peak Signal to Noise Ratio(PSNR)

It is the measure of quality of audio signal by comparing cover audio with stego audio and it is calculated as follows, (Sundar A. 2015).

$$PSNR = 10 \log_{10} \frac{MAXVAL}{MSE} \quad (3)$$

In the previous equations, \hat{Y}_i is the stego signal, Y_i is the original signal, m and n are the numbers of rows and columns in the input signals and $MAXVAL$ is the maximum value of the signal.

This study gave us the ability to calculate the noise in the recorded sounds in the program by using the above-explained three equations Mean Square Error (MSE), Signal to Noise Ratio (SNR), and Peak Signal to Noise Ratio (PSNR). After recording the sounds by the program we measured the noise percentage before and after the recording.

Table 4.2: Results obtained for 3 bits/sample embedding of encrypt-stego

	Freq	Bit Rate	Size Cover	Size secret	Secret Time	MSE	SNR	PSNR
20 db	44100 Hz	16 bit	2.71 MB	132 KB	8 s	0.061195	35.3686	60.2855
40 db	44100 Hz	16 bit	2.71 MB	132 KB	8 s	0.061393	70.7372	95.571
60 db	44100 Hz	16 bit	2.71 MB	132 KB	8 s	0.061715	106.1057	130.2015

Commonly the value of SNR above 35dB guarantees a logical good audio quality. The proposed technique has approached this problem by obtaining necessary improvements for noise control during embedding and keeping the SNR value strong above 35dB. This reduces the effect of noise on the audio quality and the recipient receives obvious audio.

The tested audio signals are analyzed accurately during listening, Figure 4.19, shows the amplitude comparison of some of the source and stego audio.

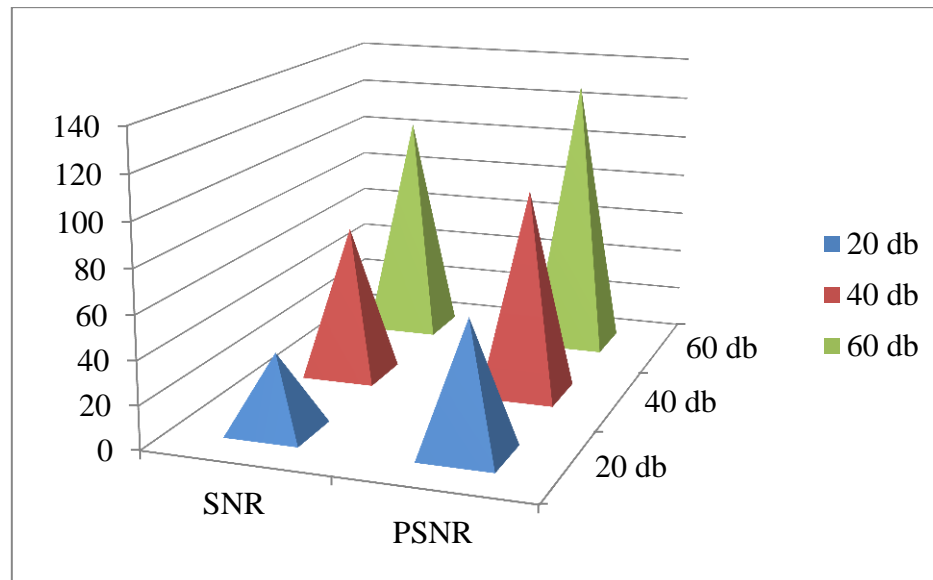


Figure 4.19: Graphical comparisons of SNR and PSNR

An experiment was done to hide the voice type (WAV) have frequency 44100 Hz at the bit rate 16 data transfer inside another voice. The hidden voice time was used 8 seconds inside its cover 41 seconds to purpose the get of results value MSE (0.061195), SNR (35.3686), PSNR (60.2855) and the signal decibel (20), which is acceptable as remarked previously.

The Table 4.3, is showing compared this study with another by PSNR, where the result from used the same number of bit as following is:

Table 4.3: Results compared

Researchers	LSB bit	PSNR
Jeswani, V., (2015)	3	42.9346
Fatin, E. M, (2015)	3	59
Proposed Methodology	3	60.2855

Chapter Five Conclusion and Future Work

In this thesis, focuses on one of these methods as shown in conclusion when summarize all of important points in this thesis, and future work when present some ideas about future.

5.1 Conclusion

The rise of the Internet and multimedia techniques in the recent years has prompted increasing interest in hiding data in digital media, various steganography tools have been developed to provide suitable security for multimedia techniques. The steganography technique means of storing information in a way that hides that information's existence, it is aimed to mask the important data of communication, making the true message is not discernible to the unauthorized user.

With the rapid proliferation of smartphones equipped with a lot of features, the mobile devices become an important part of our everyday lives since they enable us to access a large variety of services. This study presented an overview of smartphones, encryption method, with the uses and techniques of steganography for hiding the data.

In this study, the author provides appropriate security to the audio by encryption audio through serpent method. Then, they hiding the encryption audio in other audio based on LSB technique, The Merger between the encryption and Steganography is considered one of safer ways for text and multimedia, because there is no possibility to access the hidden content but only by the encryption private key. So by using 3 bits of each byte in the test

and get the results, Measures of noise (SNR, PSNR, and MSE) were used for the purpose of knowing whether the results were acceptable or not. An experiment was done to hide the voice type (WAV) with frequency 44100 Hz at the bit rate 16 data transfer inside another voice. The hidden voice time was used 8 seconds inside its cover 41 seconds to purpose the get of results value MSE (0.061195), SNR (35.3686), PSNR (60.2855) and the signal decibel (20), which is acceptable the accordance with the standards of Metrology.

5.2 Future work

At the end of the thesis, the author suggests some ideas for the future work to provide more security for the audio transmission.

- 1- Applying proposed model on another operating system such as IOS, Symbian and windows to study the effect of OS on the audio transmission speed.
- 2- Implemented other steganography techniques or encryption method then merge them, to study the effect of the changing on the security force.
- 3- The methods can be improved by applying mixed approaches, making the system more secure towards detection by using the combination of various techniques of data hiding in audio signals.

References

Aghajanzadeh, N., Aghajanzadeh, F., & Kargar, H. R. (2013) Developing a new Hybrid Cipher using AES, RC4 and Serpnt for Encryption and Decryption. *International Journal of Computer Applications*, **69** (8), 53-62.

Ahmed, S., & Hemachandran, k. (2012) Secure Data Transmission Using Steganography and Encryption Technique, *International Journal on Cryptography and Information Security*, **2**(3), 161-172.

Al-Hamami A., & Hamdi, A, S. (2015) Mobile Secure Transmission Method Based on Audio Steganography, *World of Computer Science and Information Technology Journal*, **5**(5). 87-91.

Al-Obaidi, F. E., & Ali, A. J. (2015) Which Bit Is Better in Least Significant Bit?. *Journal of Information Security*, **6** (03), 161.

Al-Omari, Z., and Al-Taani, A. T. (2015) A Survey on Digital Image Steganography. *International Conference on Information Technology*,**10** (15849),109-115.

Al-Taani, A. T., & Al-issa, A. M. (2009) A novel steganographic method for gray-level images. *International Journal of Computer and System Science and Engineering*,**3**(1),5-10.

Alwan, R. H., Kadhim, F. J., & Al-Taani, A. T. (2008) Data embedding based on better use of bits in image pixels. *International Journal of signal processing*, **2**(8), 2785-2788.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011) Mobile Security Catching up Revealing the nuts and bolts of the Security of Mobile Devices. *In Security and Privacy (SP), IEEE Symposium* ,96 -111.

Deepak D, Karthik M ,& Manjunath A. (2012) Efficient Method to Increase Robustness in Audio Steganography, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* , 1 (6), 531-536.

Fatin E. M. Al-Obaidi, & Ali Jassim, Mohamed Ali. (2015) Which Bit Is Better in Least Significant Bit. *Journal Scientific Research Publishing Inc*, (6), 161-165.

Gawande, M. S. V., & Deshmukh, P. R. (2015) Data Seclusion in Audio Wave File. *International Journal of Computer Science and Mobile Computing*, 4(4),221-228.

Gupta, S., Goyal, A., & Bhushan, B. (2012) Information hiding using Least Significant Bit steganography and cryptography. *International Journal of Modern Education and Computer Science*, 4(6), 21-27.

Hakeem, A., Amin, N. U., Shah, M., Khan, Z., & Qadi, A. (2014) Threshold Based LSB Audio Steganography. *Int'l Conf. on Chemical Engineering and Advanced Computational Technologies*,24(25), 88-92.

Jayaram, P., Ranganatha, H. R., & Anupama, H. S. (2011) Information Hiding Using Audio Steganography–A Survey. *International Journal of Multimedia and Its Applications* , 3(3), 86-96.

Jeswani, V. R., Kulkarni, S., & Ingle, M. (2015) Android Application Development for Secure Data Transmission using Steganography. *Transactions on Networks and Communications* ,3(3), 39-48.

Kieser, R., Reynisson, P., & Mulligan, T. J. (2005) Definition of signal-to-noise ratio and its critical role in split-beam measurements. *ICES Journal of Marine Science: Journal du Conseil*, **62**(1), 123-130.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013) A survey on security for mobile devices. *IEEE, Communications Surveys and Tutorials*, **15**(1), 446-471.

Liu, Y., Huang, D., Zhu, H., & Rau, P. P., (2011) Users Perception of Mobile Information Security. *International Conference for Internet Technology and Secured Transactions*, (11-14).

Mamatha, P. G., Naidu, T. & Prasad, G. (2014) A Multi-Level Approach of Audio-Steganography and Cryptography. *International Journal of Innovative Research in Computer and Communication Engineering*, **2**(4), 56-61.

Mandal, P. C. (2012) Modern Steganographic technique a survey. *International Journal of Computer Science and Engineering Technology*, **3**(9), 444-448.

Mane, A., Galshetwar, G., & Jeyakumar, A. (2012) Data Hiding Technique Audio Steganography Using LSB technique. *International Journal of Engineering Research and Applications*, **2**(3), 1123-1125.

Meligy, A. M., Nasef, M. M., & Eid, F. T. (2015) An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys. *International Journal of Computer Network and Information Security* , **7**(3), 24-29.

Mona, M. C., Chitra, S. B., & Gayathri, V., (2014) A Survey On Various Encryption And Decryption Algorithms. *Singaporean Journal of Scientific Research*, 6(6), 289-300.

Nagaraj, V., Vijayalakshmi, V., & Zayaraz, G. (2013) Overview of Digital Steganography Methods and Its Applications. *International Journal of Advanced Science and Technology*, (60), 45-58.

Pradhan, K., and Bhoi, C. (2014) Robust Audio Steganography Technique using AES algorithm and MD5 hash. *International Journal of Innovative Research in Advanced Engineering*, 1(10), 2349-2163.

Rad, R. M., Attar, A., & Atani, R. E. (2013) A Comprehensive Layer Based Encryption Method for Visual Data. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 6(1), 37-48.

Rakhi, Gawande, S., (2013) A Review on Steganography Methods. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2(10), 2278-8875.

Rana, M., and Tanwar, R. (2014) Genetic Algorithm in Audio Steganography. *International Journal of Engineering Trends and Technology*, 13(1), 29-34.

Saeed, M. J. (2013) A New Technique Based On Chaotic Steganography and Encryption Text InDCT Domain For Color Image. *Journal of Engineering Science and Technology*, 8(5), 508-520.

Saroha, K., and Singh, P. K. (2010) A Variant of LSB Steganography for Hiding Images in Audio. *International Journal of Computer Applications*, 11(6), 12-16.

Saxena, S. (2015) Secure Data Transfer through a Combination of Steganographic and Cryptographic Encryption Technique. *International Journal of Multidisciplinary and Current Research*, 3(12), 38-41.

Seleyrn A., and Darwish D.,(2012) Real-time Covert Communications Channel for Audio Signals. *International Journal of Computer Science Issues*, 9(3),279-292.

Sheth, R. K, and Sarika, P. (2015) Analysis of Cryptography Techniques. *International Journal of Research in Advance Engineering*, 1(2), 1-6.

Von Solms, R., and Van Niekerk, J. (2013) From information security to cyber security. *International Journal Computers and security*, 34(38), 97-102.

Wang, Z., and Bovik, A. C. (2009) Mean squared error: love it or leave it? A new look at signal fidelity measures. *Signal Processing Magazine, IEEE*, 26(1), 98-117.

Wolf, S., and Pinson, M. H. (2009) Reference algorithm for computing peak signal to noise ratio (psnr) of a video sequence with a constant delay. *International Telecommunication Union*, 9(6), 1-18.

Yugala, k., (2013) Steganography, *International Journal of Engineering Trends and Technology* , 4, (5).

Zhu, J., Wu, P., Wang, X., & Zhang, J. (2013) Sensec: Mobile security through passive sensing. *International Computing Networking and Communications* , 1128-1133. IEEE.

Aditya Sundar, http://it.mathworks.com/matlabcentral/fileexchange/52342-evaluating-performance-of-denoising-algorithms-using-metrics---mse-mae-snr-psnr--cross-correlation?s_tid=srchtitle, (22 Oct: 09:PM, 2015).

James Hoo, <http://www.e7z.org/open-gz-gzip.htm>, (23 Oct: 011:PM, 2015)

Appendix

1- SNR is checking by Matlab:

```
x_signal = wavread('Crypt1087239735.wav');
x_noise = wavread('Extracted-Crypt1087239735.wav');
P_x_signal = mean(x_signal.^2);
P_x_noise = mean(x_noise.^2);
SNR = 20* log10 (P_x_signal/P_x_noise)
```

2- PSNR is checking by Matlab

```
function [] = PSNR(clean,denoised)
temp=clean;
y=denoised;

%MSE %Mean squared error
mse=0;
for i=1:length(temp)
mse=mse+(y(i)-temp(i))^2;
end
mse=mse/length(temp);
fprintf('Mean Squared Error %f\n',mse);

%PSNR %signal to noise ratio %peak signal to noise ratio

den=0;
for i=1:length(temp)
den=den+(y(i)-temp(i))^2;
end

PSNR= 20*log10(max(temp)/sqrt(mse));
fprintf('Peak Signal to Noise Ratio %f db\n',PSNR);
end
```

3- Appling in Android studio:

```
public class SoundCrypAppActivity extends Activity implements
Chronometer.OnChronometerTickListener {
    private static final int RECORDER_SAMPLERATE = 8000;
    private static final int RECORDER_CHANNELS =
AudioFormat.CHANNEL_IN_MONO;
    private static final int RECORDER_AUDIO_ENCODING =
AudioFormat.ENCODING_PCM_16BIT;
    private static final int PICKFILE_RESULT_CODE = 1;
    static String Prefix = "Crypt";
    static String intoFilePath = "";
    private static String MaxTime = "00:00";
    byte[] AppendixInt;
```

```

        int iEncodeSize;
        pkg.PCM.WavAudioFormat.Builder bldr = new
pkg.PCM.WavAudioFormat.Builder();
        pkg.PCM.WavAudioFormat WF;
        SoundPool mSoundManager = new SoundPool(2,
AudioManager.STREAM_NOTIFICATION, 0);
        int soundIDopen = -1;
        int soundIDsuccess = -1;
        String NewName = "Result";
        Random Rand = new Random();
        Calendar c = Calendar.getInstance();
        int BufferElements2Rec = 1024; // want to play 2048 (2K)
since 2 bytes we
        int recorderFileSize = 0;
        private AudioRecord recorder = null;
        private Thread recordingThread = null;
        private boolean isRecording = false;
        private View.OnClickListener btnClick = new
View.OnClickListener() {
            public void onClick(View v) {
                switch (v.getId()) {
                    case R.id.btnUnlock: {
                        Intent intent = new
Intent(Intent.ACTION_GET_CONTENT);
                        intent.setType("audio/*");
                        startActivityForResult(intent,
PICKFILE_RESULT_CODE);
                        break;
                    }
                    case R.id.btnShare: {
                        String cFilePath =
Environment.getExternalStoragePublicDirectory(Environment.DIRECT
ORY_DOWNLOADS).getAbsolutePath() + "/" + NewName + ".wav";
                        Intent share = new
Intent(Intent.ACTION_SEND);
                        share.setType("audio/*");
                        share.putExtra(Intent.EXTRA_STREAM,
Uri.parse(cFilePath));
                        String shareBody = "Audio Content";
                        startActivity(Intent.createChooser(share,
shareBody));
                        break;
                    }
                    case R.id.btnEncrypt: {
                        ((ImageButton)
findViewById(R.id.btnShare)).setEnabled(false);
                        ((ImageButton)
findViewById(R.id.btnShare)).setImageResource(R.drawable.ishare)
;
                        Intent intent = new
Intent(Intent.ACTION_GET_CONTENT);

```

```

        intent.setType("audio/*");
        startActivityForResult(intent, 10);
        break;
    }
    case R.id.btnDismiss: {
        findViewById(R.id.listView1).setVisibility(4);
        findViewById(R.id.textView4).setVisibility(4);
        findViewById(R.id.btnDismiss).setVisibility(4);
        break;
    }
}
};

// use only 1024
// int BytesPerElement = 2; // 2 bytes in 16bit format

@Override
public void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.main);

    soundIDopen =
mSoundManager.load(getApplicationContext(), R.raw.open, 1);
    soundIDsuccess =
mSoundManager.load(getApplicationContext(), R.raw.success, 1);

    setButtonHandlers();
    bldr.sampleRate(RECORDER_SAMPLERATE);
    WF = bldr.build();

    byte[] Appendix = "SECRET".getBytes();
    AppendixInt = new byte[Appendix.length];
    for (int iAppendix = 0; iAppendix < Appendix.length;
iAppendix++)
        AppendixInt[iAppendix] = Appendix[iAppendix];
    iEncodeSize = AppendixInt.length;

    ((Chronometer)
findViewById(R.id.chronometer1)).setOnChronometerTickListener(t
his);

    GetFiles();
}

void GetFiles() {
    try {

```



```

        ArrayList<String> Files = new ArrayList<String>();
        String filePath =
Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_DOWNLOADS).getAbsolutePath();// + "/Download";

        File sd = new File(filePath);

        File[] sdDirList = sd.listFiles();
        if (sdDirList == null)
            return;
        for (int iFile = 0; iFile < sdDirList.length;
iFile++) {
            String item =
sdDirList[iFile].getAbsolutePath();
            if (item.contains("Extracted")) {
                if (!item.endsWith("_wav")) {
                    Files.add(item);
                }
            } else if (item.endsWith(".wav") &&
!item.endsWith("_wav")) {
                String Res = Decrypt(item);
                if (Res != "") {
                    File F = new File(item);
                    F.renameTo(new File(item.replace(".wav",
"_wav")));
                    Files.add(Res);
                }
            }
        }

        if (Files.size() > 0) {

            ArrayAdapter<String> adapter = new
ArrayAdapter<String>(this, android.R.layout.simple_list_item_1,
Files);

            ListView listView1 = (ListView)
findViewById(R.id.listView1);
            listView1.setVisibility(0);

            findViewById(R.id.textView4).setVisibility(0);
            findViewById(R.id.btnDismiss).setVisibility(0);

            listView1.setAdapter(adapter);

            listView1.setOnItemClickListener(new
OnItemClickListener() {

                public void onItemClick(AdapterView<?>
parent, View view, int position, long id) {

```

```

        String item = ((TextView)
view).getText().toString();

        // Toast.makeText(getApplicationContext(),
item,
        // Toast.LENGTH_LONG).show();
File F = new File(item);
F.renameTo(new File(item.replace(".wav",
"_.wav")));
        OpenWav(item.replace(".wav", "_.wav"));
    }
    });
}
} catch (Exception e) {
    e.printStackTrace();
}
}

public void onChronometerTick(Chronometer chronometer) {
    if (MaxTime.equals(((Chronometer)
findViewById(R.id.chronometer1)).getText())) {
        StopRec();
        // Create Intent and start the new Activity here
    }
}

private void setButtonHandlers() {
    ((ImageButton)
findViewById(R.id.btnRec)).setOnClickListener(btnClick);
    ((ImageButton)
findViewById(R.id.btnShare)).setOnClickListener(btnClick);
    ((ImageButton)
findViewById(R.id.btnUnlock)).setOnClickListener(btnClick);
    ((ImageButton)
findViewById(R.id.btnEncrypt)).setOnClickListener(btnClick);
    ((Button)
findViewById(R.id.btnDismiss)).setOnClickListener(btnClick);
    ((ImageButton)
findViewById(R.id.btnShare)).setEnabled(false);
    ((ImageButton)
findViewById(R.id.btnShare)).setImageResource(R.drawable.ishare)
;

    ((ImageButton)
findViewById(R.id.btnRec)).setTouchListener(new
TouchListener() {

        public boolean onTouch(View v, MotionEvent event) {
            if (event.getAction() ==
MotionEvent.ACTION_DOWN) {

```

```

        if (soundIDopen != -1)
            mSoundManager.play(soundIDopen, (float)
0.5, (float) 0.5, 1, 0, (float) 0.6);
            (((ImageButton)
findViewById(R.id.btnRec))).setImageResource(R.drawable.mic_wrec
);
            startRecording();
            (((Chronometer)
findViewById(R.id.chronometer1))).setBase(SystemClock.elapsedRea
ltime());
            (((Chronometer)
findViewById(R.id.chronometer1))).start();
        } else if (event.getAction() ==
MotionEvent.ACTION_UP) {
            StopRec();
        }
        return false;
    }
});
}

void StopRec() {
    NewName = Prefix + Rand.nextInt(Math.abs((int)
c.getTimeInMillis()));
    (((ImageButton)
findViewById(R.id.btnRec))).setImageResource(R.drawable.mic_w);
    if (soundIDsuccess != -1)
        mSoundManager.play(soundIDsuccess, (float) 0.5,
(float) 0.5, 1, 0, (float) 0.6);
    stopRecording();
    (((Chronometer)
findViewById(R.id.chronometer1))).stop();
    Encrypt(intoFilePath);
    (((ImageButton)
findViewById(R.id.btnShare))).setEnabled(true);
    (((ImageButton)
findViewById(R.id.btnShare))).setImageResource(R.drawable.shareic
on);
}

private void startRecording() {

    int bufferSize =
AudioRecord.getMinBufferSize(RECORDER_SAMPLERATE,
RECORDER_CHANNELS, RECORDER_AUDIO_ENCODING);
    BufferElements2Rec = bufferSize;

```