International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.03,Issue.10
May-2014,
Pages:1917-1921

www.semargroup.org,
www.ijsetr.com

Image Steganography Based Audio Security System

AUNG TINT PHYO[1], SU WAI PHYO [2]

[1]Dept of IT, Mandalay Technological University, Mandalay, Myanmar, Email: aungtintphyo@gmail.com.
[2]Dept of IT, Mandalay Technological University, Mandalay, Myanmar, Email: suwaiphyo@gmail.com.

Abstract: Information security became main concern because information and communication technology is developing dynamically today. Many problems can occur if there is no information security issue. At the same time, security for multimedia data is also important criteria. Cryptographic techniques are used to overcome these security problems. Meanwhile, steganographic techniques are developed to enhance the information security systems. Steganography is the method to hide secret information into another carrier file such as text, image, audio, and video. If the more robust information security system is needed than the ordinary information security system, cryptographic algorithm can be combined with steganographic technique. This paper proposes the combination of a cryptographic algorithm and a steganographic method to obtain the high level of information security. In this proposed system, secret audio message is encrypted with the help of AES encryption algorithm and then the encrypted audio message is embedded into a cover image by using LSB technique. This system is implemented by C# programming language.

Keywords: Advanced Encryption Standard (AES), Cryptography, Least Significant Bit (LSB), Steganography.

I. INTRODUCTION

Today, information is vital in all areas such as business, military and social affairs. Therefore, the security of information is also important to fulfill the information security requirements of above areas. Cryptography and steganography are the branches of information security field. In the cryptography point of view, symmetric and public key algorithms are available. Symmetric encryption is called conventional cryptography. In conventional cryptography, the same secret key is shared by the sender and receiver. In public key algorithms or asymmetric encryption, private and public keys are used to encrypt and decrypt data. Both approaches have not only advantages but also disadvantages. Symmetric algorithms are widely used to encrypt the vast amount of data than public key algorithms. Steganography is a technique in which secret data is embedded into the cover file such as text, image, audio, video, etc. There are many steganographic techniques to embed data into the cover file. Cryptographic techniques can be combined with steganographic techniques to be the information security system stronger. By combining these two techniques, confidential information can be secretly sent to the desired recipient. The proposed system is focused on the combination of symmetric key encryption and image steganography to send confidential audio message secretly.

II. RELATED WORKS

In the research areas, combination of different steganographic techniques and cryptographic techniques are used for hiding information secretly according to their security requirements. In 2013, Manoj Ramaiya and his fellows [1] presented an exclusive technique for image steganography based on the Advanced Encryption Standard (AES) using 128 bit block size of plaintext and 128 bits of secrete key. They believed that their system gives high level of security using cryptography which is not visible to unauthorized access and low level of security using steganography. In the previous research, Ankur Agarwal and Amit Asthana [2] presented an adaptive security scheme for secret data using cryptography and steganography. They presented a new generalized model by combining cryptographic and steganographic techniques so that the security of secret data increases to two tiers and a high quality of stego-image is obtained. Moreover, Domenico Bloisi and Luca Iocchi [3] presented image based steganography and cryptography. In their paper, they described a method for integrating together cryptography and steganography through image processing. In particular, they presented a system that is able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography. According to the concepts and knowledge pointed out from the previous research works, this work proposes image steganography based audio security system. Moreover, image steganography is effectively combined with cryptographic algorithm in order to enhance the security.

III. TWO WAYS OF INFORMATION SECURITY

In this work, it is considered at two concepts for information security in order to transmit the information secretly over open networks. These points are cryptography and steganography.

A. Cryptography

Cryptography is the art of achieving security by encoding message to make them non-readable and the science of using mathematics to encrypt and decrypt data. It enables to store sensitive information or transmit it across insecure networks (like the internet) so that it cannot be read by anyone except the intended recipient [4]. The security goals to meet the security requirements are: Confidentiality means that unauthorized parties cannot access information. Authenticity refers to validating the source of the message to ensure the sender is properly identified. Integrity provides assurance that the message was not modified during transmission, accidentally or intentionally. Non-repudiation means that a sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it [5]. In cryptography, encryption algorithms can be categorized into symmetric key (private) and asymmetric (public) key [6].

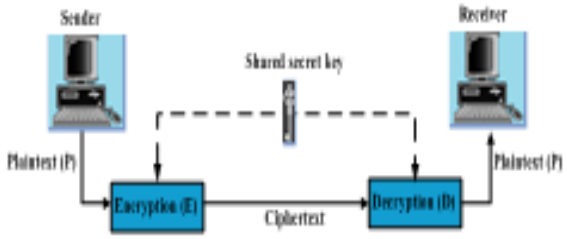

Figure 1. Schematic diagram of symmetric cryptosystem.

With symmetric encryption, confidentiality is guaranteed by the use of a secret key as shown in Figure 1. To achieve confidentiality, symmetric cryptographic algorithms are used.

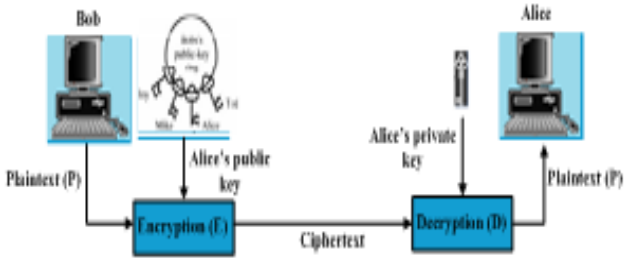

Figure2. Schematic diagram of asymmetric cryptosystem.

Public-key cryptography solves the key-distribution problem by making a scheme that uses two keys, public key and private key, rather than one [7]. It uses a pair of keys: one that encrypts the data and one that decrypts the data as shown in Figure 2. It is also called public key cryptosystems. In these two types of encryption techniques, symmetric cryptographic systems are popular for high speed encryption and low cipher expansion rate, comparing to asymmetric cryptosystems. The proposed system uses Advanced Encryption Standard (AES), the symmetric encryption algorithm.

B. Steganography

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information [8]. The term steganography is derived from the Greek word "stegano" means "covered" and "graphy" means "writing". The goal of steganography is to hide message inside other harmless message in a way that does not allow any enemy to even detect that there is a second secret message present [8]. It includes a vast array of secret communications methods that conceal the message's existence. Most of steganography works have been carried out on image, video, audio and text as shown in Figure 3.

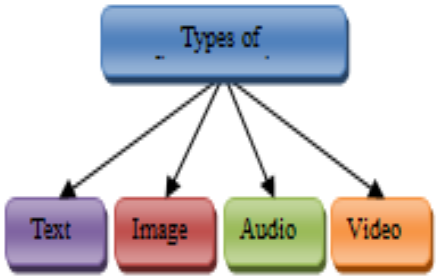

Figure 3. Types of steganography.

Among those various carrier media, image steganography is very popular to hide information in it. In this proposed system, image steganography is used to hide secret audio file. LSB (Least Significant Bit) algorithm is used in this proposed system.

IV.BACKGROUND THEORIES OF PROPOSED SYSTEM

To develop the proposed system, cryptographic symmetric encryption algorithm; Advanced Encryption Standard (AES) is used for data encryption. To create image steganography, Least Significant Bit (LSB) method is used to hide the encrypted data into the cover image file.

A. Advanced Encryption Standard (AES)

AES is Advanced Encryption Standard, a United States government standard algorithm for encryption and decryption data. AES is a symmetric block cipher with a block size of 128 bits. This means that it uses the same key for both encryption and decryption. AES Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192 and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds and AES-256 uses 14 rounds. The rounds operate on two 128-bit inputs: "State" and "Round key" [9]. These operate on a 4x4 arrays of bytes, termed the state. The proposed system used 128 bits and 128 bits key size. For complete encryption, the data is passed through 10 rounds. The algorithm begins with AddRoundKey stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the expansion that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

- SubBytes()
- ShiftRows()
- MixColumns()

- AddRoundKey()

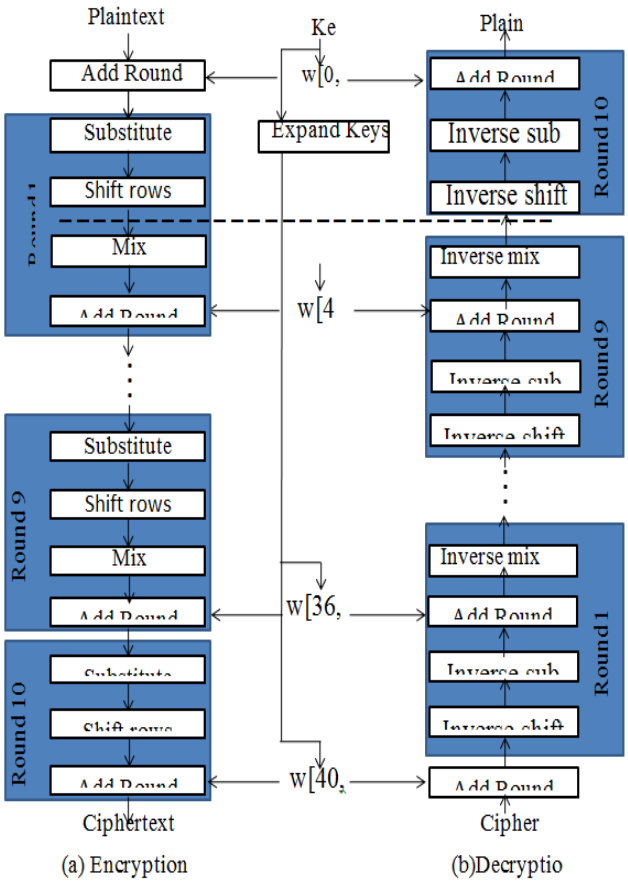

Figure 4. The overall structure of the AES algorithm

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

- Inverse ShiftRows( )
- Inverse SubBytes( )
- Inverse AddRoundKey( )
- Inverse MixColumns( )

Again, the tenth round simply leaves out the Inverse MixColumns stage [10]. Each of these stages is in more detail as shown in Figure 4. SubBytes( ) adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substitution algorithm. ShiftRows( ) provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is 1 byte, row 2 is shifted 2 bytes and row 3 is shifted 3 bytes. MixColumns( ) also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics. AddRoundKey( ) performs the actual 'encryption', when each bytes in the State is XORed with the sub key. The subkey is derived from the key according to a key expansion schedule. AES key Expansion( ) The AES key expansion algorithm takes input a 4-word (16-bytes) key and produces a linear array of 44 words, providing a 4-word round key for initial AddRoundKey stage and each of the 10 rounds of the cipher [1].

B. Least Significant Bit (LSB)

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover image. Image is composed of bits of RGB values. R stands for red, G stand for green and B stands for blue. After that, the least significant bit of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue color components so that they can be used, since they are each represented by a byte. In other words one can store 3 bit in each pixel. An 800*600 pixel image can store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24 bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the letter A, which binary representation is 01000001 and is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101100 00011101 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

Although the letter was embedded into the first 8 bytes of the grid, only the two highlighted bits need to be changed according to the embedded message. On average only half of the bit in an image will need to be modified to hide a secret message using the maximum cover size. The proposed system is designed to embed the data (encrypted audio) into an image. The least significant bit of each byte of image is substituted by the binary bit of data and then the stego-image is produced [11].

V. PROPOSED SYSTEM DESIGN

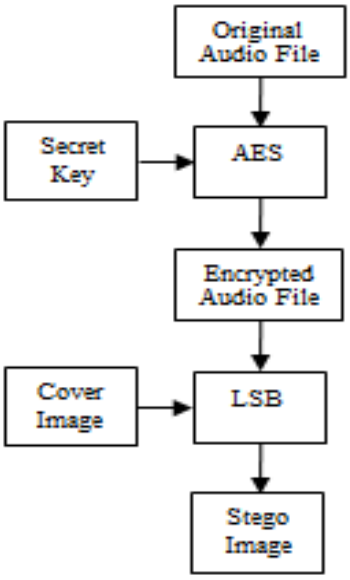

Figure 5. Block diagram from the sender's view.

The proposed system can be categorized into two portions: the sender's view and the receiver's view as shown in Figure 5 and Figure 6. The secret audio file is encrypted by AES encryption algorithm with the help of secret key at the sender's side. Then the encrypted audio file is embedded into a cover image by LSB algorithm and it can produce the stego-image.

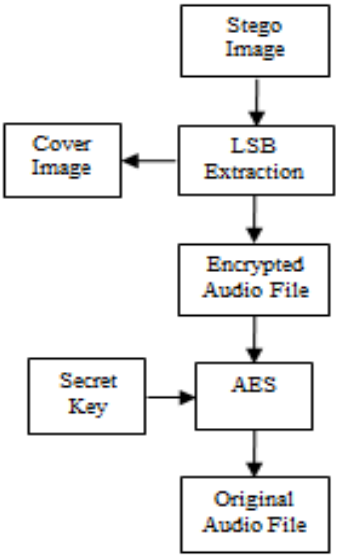

Figure 6. Block diagram from the receiver's view.

The encrypted audio file is extracted from the stego-image by using LSB extraction algorithm at the receiver's side. The extracted secret audio file is decrypted by the AES algorithm with the shared secret key and the original audio file is then produced.

VI. IMPLEMENTATION OF PROPOSED SYSTEM

Implementation results are described in this section and these are presented as a series of interfaces. The 'Home' interface is illustrated in Figure 7. The original audio file is encrypted first at the sender's side, which is illustrated in Figure 8. In this stage, the user is needed to load the original audio file and needed to point the location for the encrypted file. Then the user has to fill the secret key to encrypt the original file with the help of AES algorithm. The interface for encryption process is shown in Figure 8.

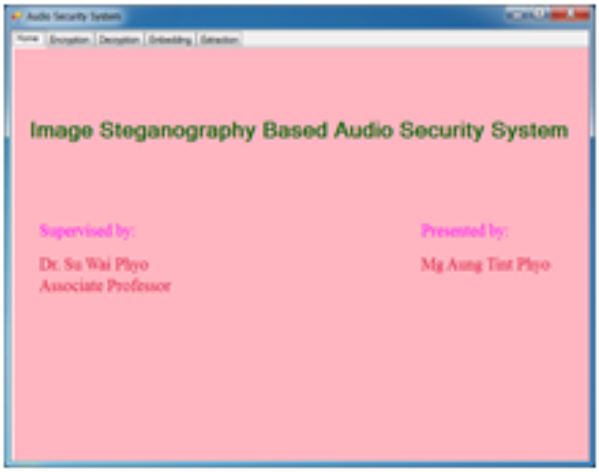

Figure 7. Home interface.

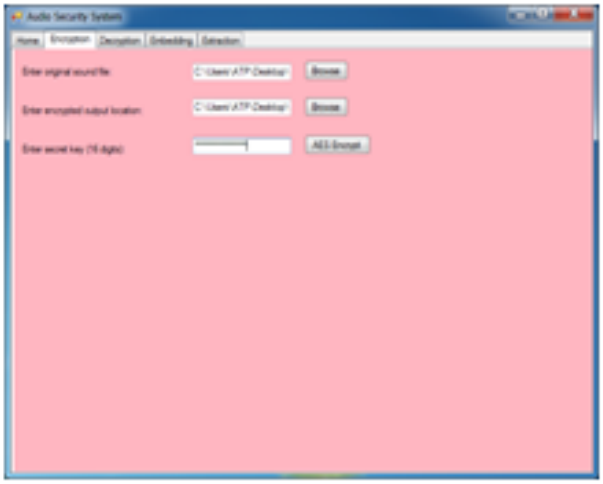

Figure 8. Encryption interface.

The next phase is embedding phase. To do that, encrypted file has to be embedded into a cover image. The user has to load the encrypted file and open the cover image. The user can embed the encrypted file into the cover file by using LSB algorithm. Then the stego-image is got and the user can save that image at the desired location. The embedding interface is shown in Figure 9.

Figure 9. Embedding interface.

The user must extract the encrypted file first from the stego-image at the receiver's side. At the extraction interface, the user has to load the stego-image and has to choose the location to save extracted file. Then, the user can extract the encrypted file from the stego-image as illustrated in Figure 10. The user at the receiver's side must decrypt the extracted file as illustrated in Figure 11. The user has to load the extracted file and needs to type the correct 16 digits secret key.

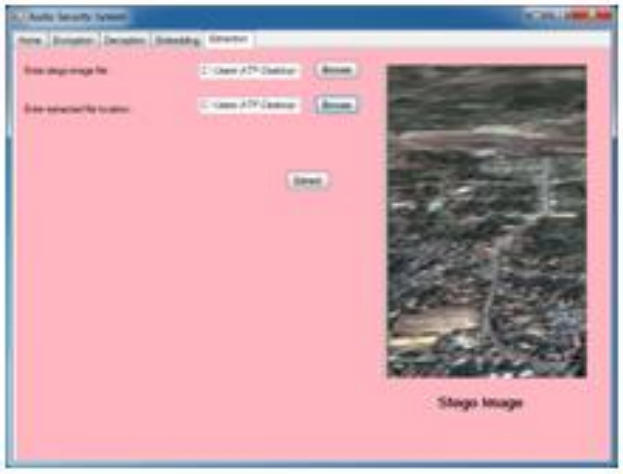

Figure 10. Extraction interface.

Figure 11. Decryption interface.

VII. CONCLUSION

The proposed system uses Advanced Encryption Standard (AES) algorithm for cryptographic portion and Least Significant Bit (LSB) algorithm for steganographic portion. Therefore, the proposed system can support two layers of security. But the weak point of this proposed system is that it can be allowed for small size of audio file (only .amr file format) to embed into an image (.bmp). The proposed system can be modified and combined with other cryptographic algorithms and steganographic techniques to extend more robust security system as further extension.

VIII. ACKNOWLEDGMENT

The author would like to thank Dr. Myint Thein, Rector of Mandalay Technological University, for his motivation, supports and guidance. The author is particularly grateful to Dr. Aung Myint Aye, Associate Professor and Head of Department of Information Technology, Mandalay Technological University, for his supports and guidance. The author would like to express his heartfelt gratitude to his supervisor Dr. Su Wai Phyo, Associate Professor, Department of Information Technology, Mandalay Technological University, for her kind advice, permission and supervision. Finally, the author would like to thank to his parents and family members for their supports and encouragements.

IX. REFERENCES

[1] Manoj Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Secured Steranography Approach Using AES", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831, Vol.3, Issue 3, Aug 2013, 185-192 © TJPRC Pvt.Ltd.

[2] Ankur Agarwal and Amit Asthana, "An Adaptive Security Scheme for Secret Data Using Cryptography and Steganography", 2nd International Conference on Role of Technology in Nation Building (ICRTNB-2013), ISBN: 97881925922-1-3, pp. 113-122.

[3] Domenico Bloisi, and Luca Iocchi, "Image Based Steganography and Cryptography", IJNCAA, 2009.

[4] Ayushi Lecturer, Sonipat, Haryana, "A Symmetric Key Cryptographic Algorithm", ©2010 International Journal of Computer Applications (0975-8887) Volume 1-No.15.

[5] Chapter 8, Cryptography – CCCure.org, Available Online: http://www.cccure.org/Documents/Cryptograpgy/cisspallinone.pdf.

[6] Shashi Mehrotra Seth and Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", MERI College of Engg. & Tech, India, 2011, ISSN: 0976-8491.

[7] Jon Callas, "An Introduction to Cryptography", 2009.

[8] K.Yugala, K.Venkata Rao."Steganography", International Journal of Engineering Trends and Technology (IJETT) Vollume4Issue5-May 20.

[9] Israel Shay Gueron, "Advanced Encryption Standard (AES) Instructions Set", White Paper, Intel Mobility Israel Development Center, Israel Shay Gueron.

[10] Chapter 7, The Advanced Encryption Standard (AES), Available Online: www.facweb.iitkgp.ernet.in./~sourav/AES.pdf.

[11] Mritha Ramalingam, "Stegomachine–Video Steganography using Modified LSB Algorithm", 2011.