Secure Information Hiding System in Image Steganography

Zo Nun Khuma
Department of Information Technology,
West Yangon Technological University, Myanmar

Dr. Khaing Myat Mon
Department of Information Technology,
West Yangon Technological University, Myanmar

Dr. Cho Cho Myint
Department of Information Technology,
West Yangon Technological University, Myanmar

Abstract: Today's real transmission environment, the two ways for securing messages and data are cryptography and steganography. Steganography is used for hiding messages in innocuous media (carriers) such as text, image, audio, video and protocol. Amongst these different carriers, digital images are the most popular because of their frequency on the internet. To be more robust in security, steganography can be combined with cryptographic techniques. In this paper, we propose LSB based image steganography combining with AES (Advanced Encryption Standard) cryptographic encryption algorithm in order to obtain a secure system that could be used in a real data communication environment. The system will be implemented by Java programming language.

Keywords: Cryptography, Advanced Encryption Standard, Hiding Information, Image Carriers, Steganography

1. INTRODUCTION
Since the rise of the Internet one of the most important factors of communication and information technology has been the security of information. It is necessary to protect this information while communicated over insecure channels. Thus, a need exists for developing technology that will help protect the integrity of digital content and secure the intellectual property rights of owners. This has resulted in an explosive growth of the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. To overcome this problem, some invisible information can be embedded in the digital media in such a way that it could not be easily extracted without a specialized technique [1]. One and most widely used for securing data is Steganography. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing" [2]. Today, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent. Research in information hiding has tremendous increased during the past decade with commercial interests driving the field [3].

For security enhancement, this system can be made by combining with another method for securing data, called Cryptography. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

2. RELATED WORKS
Recently, there is a growing interest in the information security to the problems in the current data communication domain. Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the ordinary.

The paper [4] pointed out that "some specific image based steganography techniques and show that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message." And the paper [5] also figures out that "given an image is believed to contain a secret message, identify where the message is hidden. We treat this problem as outlier detection". Moreover, the paper [6] pointed out that "The strength of steganography can be thus amplified by combining it with cryptography".

On the other hand, applying encryption algorithm on the message can enhance the security. And it is an important tool to protect information from attackers. To overcome this problem, the need is to add security mechanism in our system. To improve the performance of this proposed system, steganographic and cryptographic techniques are combined to implement the system.

3. STEGANOGRAPHY
3.1 Different Kinds of Steganography
Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Figure 1 shows the categories of steganography.

Hiding information in text is historically the most important method of steganography. Text steganography using digital files is not used very often since text files have a very small amount of redundant data. The large amount of redundant bits presents in the digital representation of an image, so images are the most popular cover objects for steganography.

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [3]. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images [7].

The protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [8]. In the layers of the OSI network model, there exist covert channels where steganography can be used [9].
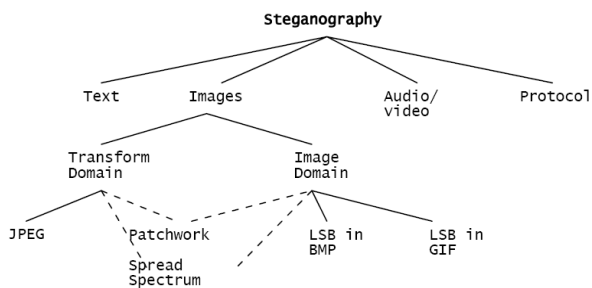

Figure 1 Categories of Steganography

3.2 Image Steganography

Images are the most popular cover objects used for steganography. For the different image file formats, different steganographic algorithms exist. For these different image file formats different steganography algorithm exist.

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [10]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [11]. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems". The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format.

Steganography in the transform domain involves the manipulation of the algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression.

3.3 Embedding data into an image

To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. In digital, images are represented with the numerical values of each pixel where the value represents the color and intensity of the pixel. These pixels make up the image's raster data. Digital images are typically stored in either 24-bit or 8-bit per pixel files. 24-bit images are known as true colour images. Obviously, a 24-bit image provides more space for hiding information as compared to 8 bit image [12].

3.4 Least significant bit insertion

The least significant bit insertion method is probably the most well-known image steganography technique. It is a common, simple approach to embed information in a graphical image file. This is the most common method used in this the data to be hidden is inserted into the least significant bits of the pixel information In digital, images are represented with the numerical values of each pixel where the value represents the color and intensity of the pixel. In 24 bit image we can embed 3 bits in each pixel while in 8-bit we can

embed only 1 bit in each pixel. To hide an image in the LSBs of each byte of the 24- bit image, one can store 3 bits in each pixel. A 1024 x 768 image has the potential to hide a total of 2,359,296 bits of information. For e.g., the letter A can be hidden in three pixels. The binary value of A is 10000011.
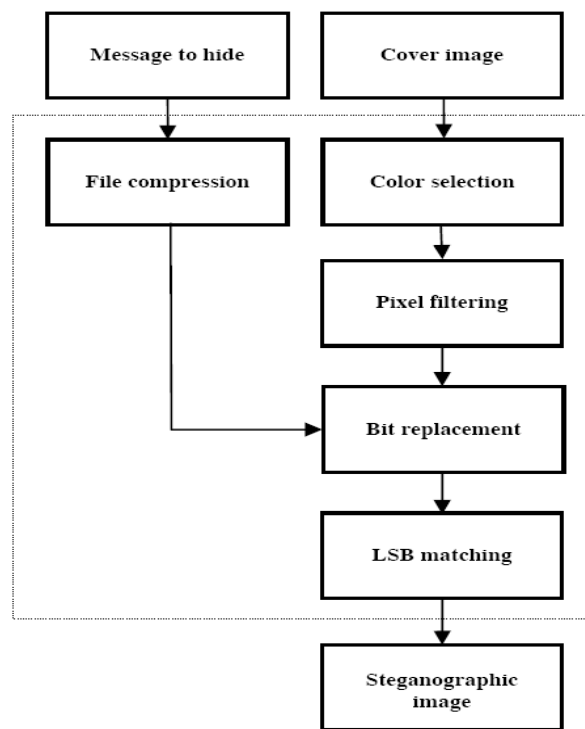

Figure 2 Structure of the algorithm SLSB

The original raster data of 3 pixels may be:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001).

After inserting the binary value for A.

(00100111 1110100**0** 11001000)

(0010011**0** 11001000 1110100**0**)

(11001000 00100111 11101001)

The highlighted bits are the only three actually changed in the 9 bytes of data. One can hide data in the least and second least significant bits and still the human eye would not be able to discern it. In this proposed algorithm we generate random number initialized with a stego-key and its output is combined with the input data, and this is embedded to a cover image. The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithm itself, instead of the choice of a secret key.

4. CRYPTOGRAPHY

Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be converted using a 'code' (in which case each character or group of characters is substituted by an

alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).Cryptology is the science underlying cryptography. Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are generically classified along three independent dimensions [13]. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver each use a different key, the system is referred to as asymmetric, two keys, or public-key encryption.

4.1 Advanced Encryption Standard (AES) Algorithm

This standard specifies the Rijndael algorithm and it is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits. Rihndael was designed to handle additional block sizes and key lengths; however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified herein will be referred to as "the AES algorithm." The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128","AES-192", and "AES-256".

4.2 Algorithm Specification

For the AES algorithm, the length of the input block, the output block and the State is 128 bits. This is represented by $Nb = 4$, which reflects the number of 32-bit words (number of columns) in the State.

For the AES algorithm, the length of the Cipher key, K, is 128, 192 or 256 bits . The key length is represented by $Nk = 4$, 6, or 8, which reflects the number of 32-bit words (number of columns) in the Cipher Key.
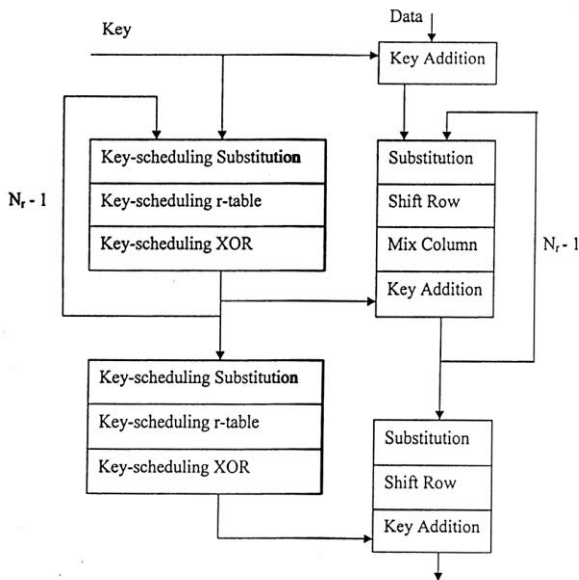

Figure 3 Advanced Encryption Standard

For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by Nr, where $Nr = 10$ when $Nk = 4$, $Nr =12$ when $Nk = 6$, and $Nr = 14$ when $Nk = 8$.

5. PROPOSED SYSTEM

As shown in Figure 4, two ways of securing method are used in this proposed system: Steganography and Cryptography.
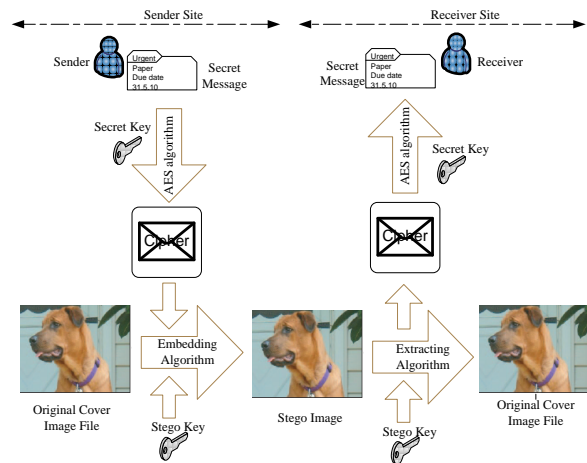

Figure 4 Proposed System Design

In the first step, at the sender site, the plaintext (secret message) is encrypted with the help of Advanced Encryption Standard (AES), popular and easy, algorithm and then the cipher text is produced as in Figure 5. Because it is a symmetric key algorithm, the same Secret Key is applied both for encryption and decryption.
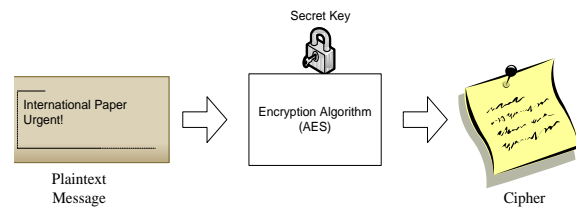

Figure 5 Encrypting the Message

Here we embed the message (Cipher) into the carrier image by using Least Significant Bit (LSB) insertion method. After embedding a secret message into the cover-image, a so-called stego image is obtained. The size of information to be hidden relatively depends on the size of the cover-image. Any image file can hide the message of size of one – eight the size of original cover file, e.g if cover image is 128 bytes then it hide 16 bytes of message without any distortion.

After this process, at the receiver site, the embedded message is extracted from the stego image file and obtained the cipher text again as depicted in Figure 6.
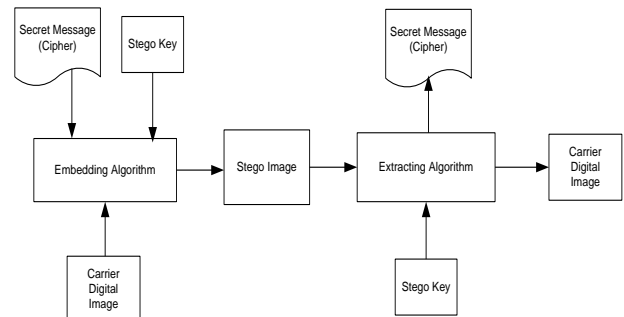

Figure 6 Embedding and Extracting the Message (Cipher)

The resulting cipher text is decrypted by using AES algorithm with the same Key as in encryption. Finally, the receiver obtains the sent message (plaintext) as shown in Figure 7.
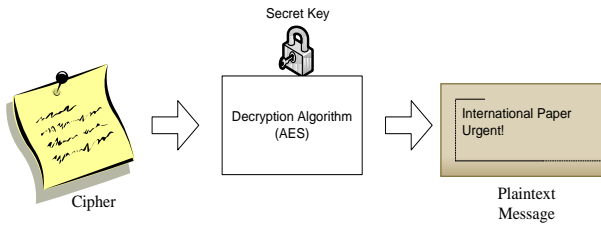

Figure 7 Decrypting the Message

6. PROS AND CONS

Table 1 Steganography Vs Cryptography

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithms are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

7. TEST AND RESULT

Firstly, the system is implemented by using StegoJava. Figure 8 shows the encryption process.
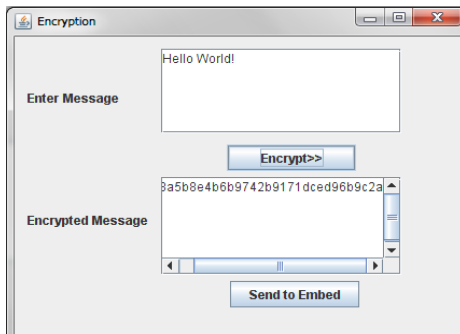

Figure 8 Encrypting the Message with AES Algorithm

The resulting cipher message is fetched to the embedding mode and is embedded the GIF image which is used as a cover image by the help of LSB. Then the resulting stego-image is obtained as shown in Figure 10.
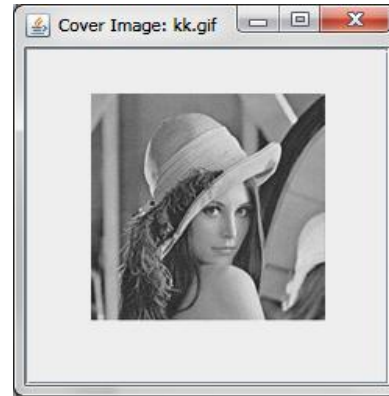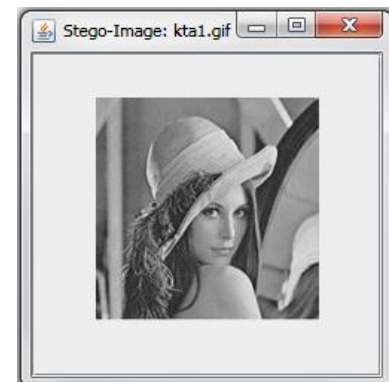

Figure 9 The Cover Image

Figure 10 The Stego-image

Finally, the resulting cipher message extracting from the stego-image is decrypted to get the original message as shown in Figure 11.
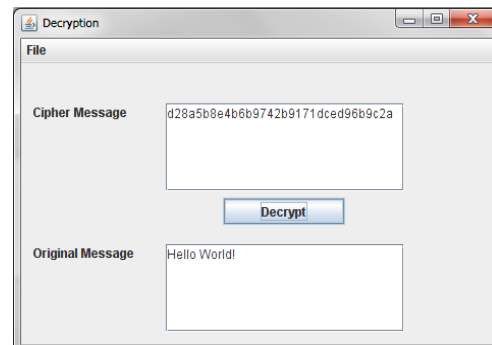

Figure 11 Decrypting the Cipher Message

8. CONCLUSION

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. In this paper we give an idea to enhance the security of system by combining the two techniques. It can enhance confidentiality of information and provides a means of communicating privately. Here message is first encrypted and then embed in image file with help of steganographic system. There are infinite number of steganography applications for digital image including copyright protection, feature tagging, and secret communication. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image.

9. ACKNOWLEDGMENTS

10. REFERENCES

[1] Dunbar, B. "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002

[2] Moerland, T. "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*,

www.liacs.nl/home/ tmoerl/privtech.pdf

[3] Silman, J. "Steganography and Steganalysis: An

Overview", *SANS Institute*, 2001

[4] Chandramouli, R. & Nasir Memon, "Analysis of LSB Based Image Steganography techniques", 2001 IEEE

[5] Ian Davidson & Goutam Paul, "Locating Secret Messages in Images", *KDD'04*, Seattle, Washington, USA, August 22-25, 2004

[6] Morkel, T., JHP Eloff and MS Olivier, "An Overview of Image Steganography," *in Proceeding of the fifth Annual Information Security South Africa Conference (ISSA 2005)*, Sandton, South Africa, June/July 2005 (Published electronically)

[7] Artz, D. "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

[8] Ahsan, K. & D Kundur, , "Practical Data hiding in TCP/IP", *Proceedings of the Workshop on Multimedia Security at ACM Multimedia*, 2002

[9] Handel, T. & M. Sandford, "Hiding data in the OSI network model", *Proceedings of the 1st International Workshop on Information Hiding*, June 1996

[10] Silman,J. "Steganography: and Steganalysis: An Overview", *SANS Institute, 2001*

[11] Lee, Y.K. & L.H. Chen, "High capacity image steganographic model", *Visual Image Signal Processing*, 147:03, June 2000

[12] Lin E.T. and E.J. Delp, "A Review of Data Hiding in Digital Images", JUNE 2001

[13] Stinsown, D. "Cryptography:Theory and Practice"