G407

A Robust Method of Encryption and Steganography Using ElGamal and Spread Spectrum Technique Based on MP3 Audio File

Priadhana Edi Kresnha
Department of Informatics Engineering
University of Muhammadiyah Jakarta
Central Jakarta 10510
priadhana.edi@informatika.ftumj.ac.id

Aini Mukaromah
Faculty of Computer Science
University of Mercu Buana
Kebon Jeruk, West Jakarta 11650
ainialmukaromah@yahoo.co.id

***Abstract*—Security is one of the most important things to be considered when exchanging message, particularly when the message exchanged is top secret message. In this research, a tool is developed to encrypt the message and hide it into a digital object. Encryption method used is ElGamal Encryption, and the object where the message hidden is mp3 audio file. The part in mp3 file used for attaching the message is homogenous frame. This process is enhanced with spread spectrum method and pseudo noise modulation to make the encrypted message more randomized and harder to decrypt. The result shows that the sound quality of the original file and stego-file are almost the same. The noise produced by the message is measured by calculating Error rate and PSNR (Peak Signal to Noise Ratio) between original file and stego-file.**

Keywords—Encryption; Mp3 file; Spread Spectrum; Steganography; Stego-Object;

I. INTRODUCTION

Security is one of the most important things to be considered when exchanging message, particularly when the message exchanged is top secret message. The importance of concealing the message has been considered since ancient age which makes the theory of cryptography becomes one of the oldest theories that human made.

One of the oldest cryptography methods which have ever been made is Caesar cipher. It is also known as shift cipher, Caesar's code, or Caesar shift. It is one of the simplest and most widely known encryption techniques. It works by shifting the order of the alphabet by some fixed number. Other advance shifting method was then discovered. The newer one uses key to shift the order of alphabet. The example of this one is vigenere encryption.

Along with encryption, steganography as a method to conceal the message has been emerged as well. Differ from encryption which converts the message into unreadable form, steganography tries to hide a message into an object. The oldest steganography method was hiding the message on a courier head. Before writing the message on the courier head, his hair had to be cut. The message was then written on his bald head. After writing the message, the courier had to be quarantined for approximately three months, while waiting until the hair grew up again. The courier would be sent to the field commander to convey the message from the supreme leader. Later on the courier had to be killed to prevent the message uncovered by unauthorized person.

In this research, both encryption and steganography are used to conceal the message. Encryption is used so that no unauthorized person can read the message, and steganography is used so that no unauthorized person realizes that the object being sent contains a message, thus an effort to break encryption codes or do cryptanalysis action can be avoided. This way, exchanging message can be more secure.

There are several studies on cryptography and steganography technique, particularly digital steganography. The most used digital steganography technique is Least Significant Bit (LSB). This technique manipulates bits which give insignificant changes when they are modified. It has been generally known that computer processes data in digital form which consists of bit 0 and 1 only. The bits are combined to represent a single value of data. I.e. a character is represented by the combination of 8 bits (1 byte). Therefore a character can be valued from 0 to 255.

In digital file, particularly multimedia file, a single value data can be represented by various numbers of bits. I.e.jpeg file, each pixel of every channel (Red, Green, and Blue) is represented by 8 bits. By changing the least significant bit, the modification cannot be seen clearly. For example, if the red value of the pixel is 255, after the least significant bit has been changed, it becomes 254. For human, this changed will not affect the sense of the picture. But if the modified bit is the most significant bit, the value will decrease into 128 and this will drastically change the sense of the picture. This kind of technique has been conducted by [1,2,3].

LSB is able to be implemented in audio file as well. In [1] MPEG formatted Audio becomes the cover file to conceal the message. It uses two-steps algorithm to embed watermark bits into higher LSB layers. However in that paper no encryption method is implemented to enhance message security. In [4] LSB is implemented to hide the message into uncompressed digital audio, but again, it is not enhanced by encryption technique to increase security level. In [3], LSB audio steganography and encryption techniques are implemented. The encryption process uses sum of all ASCII form of the key to create XOR modulation bits. These bits become the encryption key, and the encryption is done by doing XOR modulation between bits form of the message and XOR operator bits. The used key is symmetric key, so the sender and recipient share the same key. When decrypting the message, the recipient inserts the same key as the sender did when he encrypt the message.

In this research, combination of various encryption and steganography techniques are conducted to provide more powerful message concealing method. The file used for steganography is mp3 audio file. Audio file is chosen since the capacity is bigger than text or image file, and it is not as complicated as video file. Mp3 format is chosen since it is the most widely known and used compared to other audio formats. Another steganography studies using Mp3 file format have been conducted by [5,6,7,8]. Encryption method used in this research is ElGamal Encryption. The encrypted message is embedded in the homogenous frames of mp3 audio file. Before embedding the message into the file, the encrypted message is enhanced with spread spectrum method and XOR modulation to improve its randomness. This way, the security of the message can be improved without significantly affecting the quality of audio file.

This paper consists of several parts; Section 2 contains general information about encryption and steganography method. Detailed process of encryption is explained in section 3. Steganography process is explained in section 4 and its subsections. Quality measurement technique to assess stego-object is elaborated in section 5. Implementation of the method and its result is explained in section 6. The last section, section 7, contains conclusion and further development of the system.

II. METHODS

Generally, steganography process is described in Fig 1. First, cover object has to be prepared, and then the message is inserted into that cover object using some key. After the cover object has been inserted by the message and become stego-object, this stego-object is sent to the recipient. The recipient will open this stego-object using some key, and derive the message from the object.

In the proposed method, steganography is combined with other encryption technique to improve its security. The process of the proposed method is shown in Fig 2. First, cover object and message have to be prepared. The message is then encrypted using ElGamal Encryption. Encryption result is then converted into bits. In this bit form, the bits are spread using spread spectrum technique and modulated by pseudo noise signal. This noise signal is the XOR modulator which used to randomize the encrypted bits. The result of modulation is then inserted into mp3 file as noise. Mp3 file which has been inserted by the message is called stego-audio.

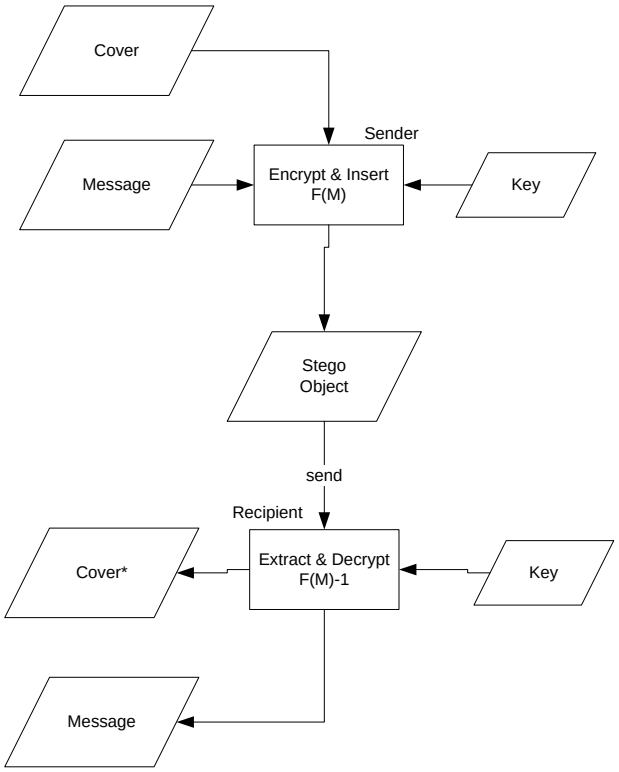

Fig. 1. General Steganography Process.

III. ENCRYPTION

Encryption method used in this research is ElGamal encryption. Elgamal Encryption is an asymmetric key encryption algorithm based on the Diffie-Hellman key exchange. Unlike [3], this research uses asymmetric key to encrypt the message. The sender and the recipient don't share the same key. The sender encrypts the message using recipient's public key, and the recipient decrypts the encrypted message using his own private key.

Elgamal encryption was originally used for digital signature, but was later modified so it can be used for encryption and decryption. Elgamal is currently used in security software developed by GNU Privacy Guard, recent versions of PGP. The security of this algorithm lies in the difficulties to solve discrete algorithm problem [9,10].

Discrete algorithm problem : *if p is prime number, g and y are random natural numbers, find x which satisfies following formula,*

$$g^x \equiv y(\mathrm{mod}\ p) \quad (1)$$

IV. STEGANOGRAPHY

There are several processes conducted before embedding the message into the file. First, converts the encrypted message

into bits form. Conversion is done for each character, and each encrypted character is not necessarily consists of 8 bits. It depends on the number of bits used in ElGamal encryption process. Normally, the number of bits used in encryption process is 64 bits. It means that a place consists of 64 bits must be prepared in stego-file for each character. This makes the length of the message become a major issue, since the capacity of stego-file to store the message is very limited, depends on the number of homogeneous frames provided by the stego-file. The more bits used for each character, the less number of characters can be inserted into the same file. Therefore the number of bits used in the encryption process is decided no more than 15 bits. This way, a longer message can be inserted into the file

After converting the message into bit form, spread spectrum process is done to the message, followed by XOR modulation and insertion into the file. Those processes are explained in the following subsections.

A. Spread Spectrum

In Spread Spectrum technique, secret message is encoded and spread to every available frequency spectrum. It transmits a narrow information signal band in a broad band channel [5,11].

In the steganography process, signal spreading is used to increase the level of redundancy. Redundancy magnitude is determined by a *cr* scalar multiplier. The length of the message bit after spreading is *cr* times of its initial length.

B. XOR Modulation

In this process, the enrypted message which has been converted into bits form and spread with some spreading coefficient (*cr*) is modulated by *pseudo-noise signal*. This *pseudo-noise signal* is generated randomly using *Linear Congruential Generation* (LCG) algorithm [12]. LCG is one of the oldest and best known pseudorandom generator algorithm. The generator is defined based on the following recurrence equation:

$$x_{n+1} = (ax_n + b)(\mathrm{mod}\, m) \qquad (2)$$

Where

$0 < m$, m is the modulus

$0 < a < m$ is the multiplier

$0 \le b < m$ is the increment

x_n is the current sequence of pseudo random value

x_{n+1} is the next sequence of pseudo random value

.

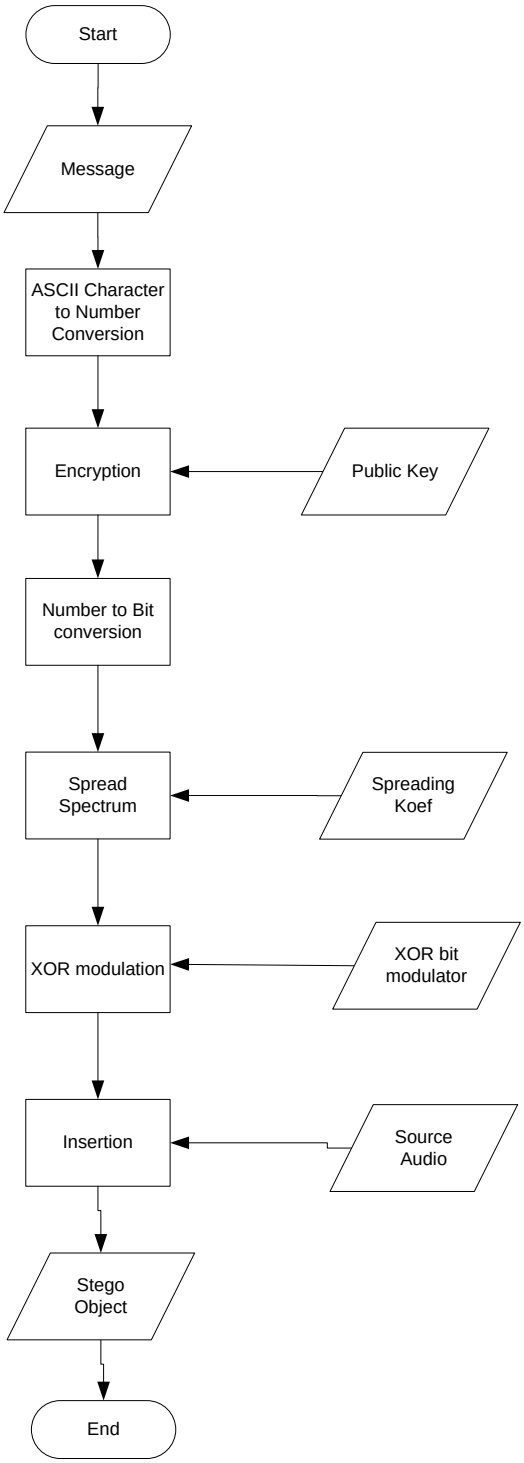

Fig. 2. Steganography Process in this study.

C. MP3 Homogenous Frame

The part of mp3 file which is used to embed the message is homogeneous frame. This frame consists of bit 1 only.If it is converted into the decimal,the value in this frame simply contains -1. Not every mp3 file has homogeneous frame. Therefore not all mp3 files can be inserted by the message.

Only files with homogeneous frames are able to be inserted by the message.

Homogenous frame can be seen as multiple '*ff*' character in some part of mp3 file. The example is shown in Fig.3.

Fig. 3. Homogenous Frame in an Mp3 File.

After inserting the message into the file, the homogenous frame in Fig.3 becomes Fig.4.

Fig. 4. Homogenous Frame After Inserted By Message.

The length of the message after encryption and steganography process, and ready to be inserted into the file can be computed using the following formula,

$$L = n * \omega * cr \tag{3}$$

Where L is message length (in bits), n is the number of characters in the message, ω is the number of bits used in encryption process, and cr is spread spectrum coefficient ratio.

On the other hand, The capacity provided in mp3 file to insert message can be calculated as follows,

$$SP = \tau * 8 * \varsigma - \left(2 * \left(\xi + \zeta\right)\right) \tag{4}$$

Where SP is the capacity provided, τ is the number of homogenous frame, ς is the number of byte provided in each frame, ξ is the number of header bit, and ζ is the number of footer bit.

To check whether the message can be inserted or not, the result of equation 3 and 4 are substracted using the following formula,

$$RS = SP - L \tag{5}$$

Where RS is remained message space. If $RS \geq 0$, then the message can be inserted.

V. Quality Audio Measurement

Two techniques are used to measure the quality of the audio, subjective and objective. Subjective measurement is done by listening to the stego-file and compare it with the initial file, while objective measurement is estimated by computing Error rate and PSNR (Peak Signal to Noise Ratio) of stego-file.

Error rate is calculated using this following formula,

$$ER = \frac{1}{m}\sum_{i=1}^{m}\left|x_1(i) - x_0(i)\right| \tag{6}$$

andPSNR is calculated using the following formula,

$$PSNR = 10 *^{10} \log\left(\frac{\sum_{i=1}^{m} x_1^2}{\sum_{i=1}^{m}\left(x_1 - x_0\right)^2}\right) \tag{7}$$

Where x_0 is the cover signal intensity and x_1 is the stego signal intensity.

A good audio quality is achieved when the error rate is low while the PSNR is high. Lower error rate and higher PSNR means better stego-object audio quality.

VI. Implementation and Result

Several mp3 files and messages are prepared to test the system. Mp3 files and their information are listed in Table I, while messages and their size after encryption and spread spectrum process are listed in Table II.

TABLE I. MP3 File with various size for testing

Name	File Size (bytes)	Capacity (bytes)
Mary.mp3	1423176	2576
Converstion.mp3	2152590	3976
Relaxing_instrumental_music.mp3	2357255	133288
Maid with the Flaxen Hair.mp3	4113874	1004065
Sleep Away.mp3	4842585	1436464

TABLE II. Message with various size for testing

Name	Size (bytes)
Coy knows pseudonoise codes	1620
Can you can a can as a canner can can a can?	2640
Send toast to ten tense stout saints' ten tall tents	3120
Six sick hicks nick six slick bricks with picks and sticks	3480
Peter Piper picked a peck of pickled peppers. A peck of pickled peppers Peter Piper picked. If Peter Piper picked a peck of pickled peppers, Where's the peck of pickled peppers Peter Piper picked?	11760

To simplify the writing, each mp3 file is represented from 1 (*mary.mp3*) to 5 (*Sleep Away.mp3*), and the message is

represented from A (*Coy knows pseudonoise codes*) to E (*Peter Piper picked a peck of pickled peppers. A peck of pickled peppers Peter Piper picked. If Peter Piper picked a peck of pickled peppers, Where's the peck of pickled peppers Peter Piper picked?*). Errorrate and PSNR of the combination between mp3 file and the message are shown in Table III and IV.

TABLE III. ERROR RATEMATRIX

Mp3\Msg	A	B	C	D	E
1	0.0016	-	-	-	-
2	$1.5x10^{-4}$	$2.2x10^{-4}$	$2.7x10^{-4}$	$2.8x10^{-4}$	-
3	$7.5x10^{-4}$	$9.5x10^{-4}$	$1.2x10^{-3}$	$1.5x10^{-3}$	$4.9x10^{-3}$
4	$3.3x10^{-6}$	$5.8x10^{-6}$	$7.2x10^{-6}$	$7.6x10^{-6}$	$3.1x10^{-5}$
5	$6.8x10^{-6}$	$9.0x10^{-6}$	$1.1x10^{-5}$	$1.2x10^{-5}$	$2.5x10^{-5}$

TABLE IV. PSNR MATRIX

Mp3\Msg	A	B	C	D	E
1	17.9851	-	-	-	-
2	26.5147	25.1752	24.4314	24.4003	-
3	19.8028	19.5011	18.0854	16.8738	11.2900
4	59.3997	56.0651	54.7537	54.4367	48.2227
5	58.1832	57.7936	57.1564	56.7710	53.5136

The result shows that there is a tendency more file size and capacity makes error rate lower and PSNR higher. On the other hand, more message size makes error rate higher and PSNR lower. The graphic of the result can be seen in Fig.5 and 6. To make it easy to see, the value in error rate graph is converted into log10 and added by 6.

In first mp3 file experiment, only first message can be inserted into the file. Other message cannot be inserted since the capacity for carrying the message is not big enough. Therefore neither error rate nor PSNR can be estimated. The same goes with second mp3 for last message.

The advantage of this steganography technique is that the size of stego-object does not change. It does not increase nor decrease, because it modifies the file in bit level, not byte nor signal magnitude.

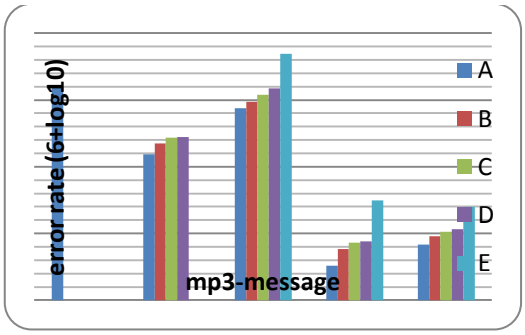

Fig. 5. Error Rate Graph

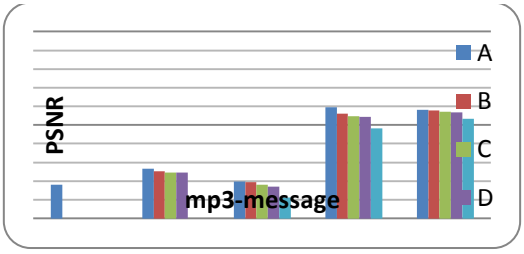

Fig. 6. PSNR Graph

VII. CONCLUSIONS

Elgamal Encryption and Steganography using spread spectrum and pseudonoise modulation have been successfully implemented in this research. The quality of stego-file is estimated using error rate and PSNR. The quality depends on file size and message length. The experiment shows there is a tendency that PSNR becomes lower and error rate becomes higher when the size of stego-file is smaller or the length of the message is larger. The less PSNR is, the lower quality stego-file will be obtained. The advantage of this technique is stego-file size does not change. It makes the quality of stego-file can be maintained and reduces the suspicion towards the stego-file.

ACKNOWLEDGMENT

The authors would like to thank Department's head and Faculty's Dean for the support to join the 1st AEMT conference. This research was funded in part by Faculty of Engineering University of Muhammadiyah Jakarta (http://ftumj.ac.id/).

REFERENCES

[1] Cvejic, N., and Seppanen, T, "Increasing Robustness of LSB Audio Steganography Using A Novel Embedding Method", in *The International Conference on Information Technology : Coding and Computing (ITCC'04)* IEEE, 2004.

[2] Pangaribuan, F, "Application Development of Encrypted Message Concealment Using Mars Method on Image with LSB Image Zang Method", B.S. thesis, Department of Informatics and Electro Engineering, Bandung Institute of Technology, Bandung, Indonesia, 2008.

[3] Sridevi, R., Damodaram, A., Narasimham, S, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhance Security", Journal of Theoretical and Applied Information Technology (www.jatit.org), 2009.

[4] Utami, E, "Steganography Application Based on Least Bit Modification Approach Using Uncompressed Digital Audio File", Journal of DASI, Vol. 10, No. 1, 2009.

[5] Baskara, T, "The Study and Implementation of Steganographic Based on MP3 Audio Using Spread Spectrum Technique", B.S. thesis, Department of Informatics and Electro Engineering, Bandung Institute of Technology, Bandung, Indonesia, 2008.

[6] Herianto, "Cryptography Software Development Based on MP3 Audio File Using Parity Coding Technique in Mobile Phone Device", B.S. thesis, Department of Informatics and Electro Engineering, Bandung Institute of Technology, Bandung, Indonesia, 2008.

[7] Atoum, M., S., Ibrahim, S., Sulong g., M-Ahmad., A. "MP3 Steganography: Review", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012.

[8] Pinardi, R., Garzia, F., Cusani, R. "Peak-Shaped-Based Steganographic Technique for MP3 Audio", Journal of Information Security, vol. 4, pp. 12-18, 2013.

[9] Munir, R, Cryptography, Bandung : Infomatika, 2006.

[10] Tsiounis, Y., Yung, M. “On the Security of ElGamal Based Encryption”, Springer-Verlag Berlin Heidelberg, LNCS 1431, pp. 117-134, 1998.

[11] Winanti, W, "Message Concealment Based on JPEG Compressed Image Using Spread Spectrum Method", B.S. thesis, Department of Informatics and Electro Engineering, Bandung Institute of Technology, Bandung, Indonesia, 2008.

[12] Hallgren, S. "Linear Congruential Generators over Elliptic Curves". CS94 -143 , Dept. of Comp. Sci., Cornegie Mellon Univ, 1994.