ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 7321–7330
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.79

IMAGE STEGANOGRAPHY ON COMPRESSED AND ENCRYPTED MESSAGE USING RSA, AES, 3DES,DES, AND BLOWFISH

MASUMEH DAMRUDI[1] AND KAMAL JADIDY AVAL

ABSTRACT. In today's world, Vulnerability of confidential information is growing due to insecure communication channel. Cryptography and steganography are common techniques of promoting security. A hybrid of these techniques enhances the security. In addition, compression of data before encryption leads to reducing the size of message. In this paper, Huffman code as the compression technique, RSA, AES, 3DES, DES, and Blowfish algorithms as cryptographic algorithms, and LSB (Least significant Bit) as the steganography algorithm are employed to encrypt the secret message. The experimental results in the form of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and the histogram of main and covered image indicates that the mentioned algorithms achieve appropriate quality of stego image. Huffman code made it possible to send greater messages than normal.

1. INTRODUCTION

Information security is becoming more important due to the increase of data transmission on insecure communication environment. In this era, cryptography and steganography are two common ways of transmitting secure information. Cryptography is one of the most important aspect of digital word [1]. Cryptography ensure that the encrypted message will be utilized by the authorized

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A08, 94A29, 94A60.

Key words and phrases. steganography, encryption, compression, Huffman, LSB, Blowfish, DES, 3DES, AES, RSA.

person. Symmetric key and asymmetric key (public key) are two main ways of cryptography. Symmetric key uses the same key for encryption and decryption while asymmetric key employs two different keys. Public key for encryption and private key for decryption.

Steganography is an effective way for hiding information. Steganography is categorized into three types including pure, secret key and public key steganography. Pure class has no key, secret key class has one key and public key class has a public and a private key [2].

Compression decrease the capacity of information. There are two kinds of compression including Lossless and Lossy. The main data and the decompressed data are exactly the same in lossless data compression while the main data is not exactly the same of decompressed data in lossy data compression [3].

Cryptography and steganography have more efficient in term of security and data protection while they are employed together [4]. Compression reduce the size of the data, therefore the amount of that will be placed in the same cover image will increases in steganography. Compression before encryption enhance the security in communication era [5]. Therefore, we employed compression, encryption, and steganography techniques altogether to achiever more security and capacity to transfer confidential information.

In this paper, five different encryption algorithms including RSA, AES, 3DES, DES, and BLOWFISH are employed. LSB as steganography and Huffman coding as compression techniques are utilized. The unauthorized person cannot realize the small changes in patterns visually whereas employing LSB as steganography algorithm [6]. Huffman coding is a lossless data compression algorithm which is based on the frequency of occurrence of a symbol in the text that is being compressed [3].

Different works on the mentioned cryptographic algorithms and LSB as steganography algorithm are performed. We presented a work that employs all these algorithms at the same time and we compared them on the same environment based on different factors such as encryption and decryption time, SNR (Signal to Noise Ratio), PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and the histogram [7]. In this paper, we employed the same cryptographic and steganography algorithms. in addition, Huffman code is used to increase the capacity of transmitted data and security. Abdelmged et. al. in [3] and Narayana in [5] employed Huffman code compression, an encryption algorithm and Lsb

as steganography algorithm. Abdelmged employed RC4 as cryptographic algorithm and Narayana used RSA as cryptographic algorithm and also Digital Watermark to help owner identification.

In this study, first the data is compressed by Huffman code. Then, encryption of data is performed employing RSA, AES, 3DES, DES, and Blowfish algorithms. Thence the compressed and encrypted message is hidden using LSB technique. This method leads to more layers of security. Therefore, the intruders cannot figure out the original message simply. Combination of steganography, cryptography, and compression promote the guarantee of protecting data. The Experimental and computational results reveals appropriate quality of stego image with more capability of sending encrypted message in the same cover image.

2. PROPOSED METHOD

Each of cryptography and steganography alone provide security to transfer a confidential message. However, combination of cryptography and steganography leads to more efficiency. In the proposed method, the confidential message first compressed using Huffman code, then the compressed message is encrypted employing RSA, AES, 3DES, DES, and BLOWFISH. The reason is to implement the method on different types of cryptographic algorithms. Afterwards, the cipher text is hidden inside a cover image utilizing LSB.

The process of the method is as following. First, the considered message is converted to ASCII code. Then the probability of symbols in the confidential message are computed to apply in compression algorithm which is Huffman coding. After compression using the Hoffman algorithm in MATLAB, compressed text is encrypted by the stated cryptographic algorithms separately. For this reason, the key is generated based on the algorithm that is mentioned. The process of key generation for RSA is different from AES, 3DES, DES, and Blowfish since RSA requires two different keys. Thence the message is encrypted with the mentioned algorithm that is based on java and is imported in MATLAB environment. The image which is selected for cover in steganography is converted to grayscale. Afterwards, the cipher text is fed into the LSB algorithm employing the image. This process is accomplished in MATLAB too. The output of procedure is the hidden of compressed encrypted message in the selected cover image. LSB stands for Least Significant Bit Which is the easiest way of image

steganography [8]. In the LSB algorithm, the least significant bit of each pixel which is the 8th bit is applied for the message encryption. Changes in the image are not visible to the human eye. The following procedure illustrates the proposed method.

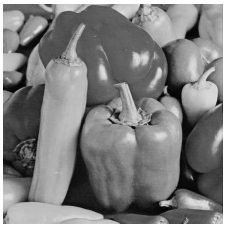
(1) Define the confidential message
(2) Convert the message to ASCII code
(3) Computation of symbols' probability in the message
(4) Message compression (Huffman coding)
(5) Key generation
(6) Encryption of message (RSA, AES, 3DES, DES, Blowfish)
(7) Calculate the length of encrypted message
(8) Define the cover image
(9) Convert the image to grayscale
(10) LSB algorithm (encrypted message, cover image)
(11) Convert the result to a visible image
(12) Calculate SNR, PSNR and MSE

The procedure of decompression and decryption are performed to ensure the correctness of algorithms and implementations. The execution of each cryptographic algorithm is implemented separately.

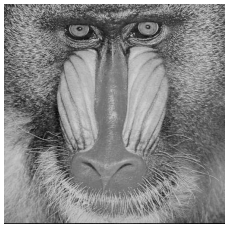
3. Experimental results

In this study, two images of size 512×512 are utilized as the cover images from USC-SIPI dataset (http://sipi.usc.edu/database/) for experiments. Figure 1 shows the selected images which researcher widely used for evaluating their results in steganography. MATLAB R2016a is employed as programming language and all parts of the method is implemented on the same environment which is MATLAB.

The confidential message is written in English alphabet including 1720 bits. This message first is compressed employing Huffman code. The length of compresses message become 919 bits for the selected message. Then the compressed message is encrypted with the five mentioned algorithms. The compressed plaintext is the same for all five encryptions. The size of key length for each encryption is illustrated in Table 1.



(A) Peppers



(B) Baboon

FIGURE 1. Cover images

TABLE 1. Key length of RSA, AES, 3DES, DES, and Blowfish

Algorithm	Key length bits	Message bits	Compressed message bits
RSA	2048	1720	919
AES	128		
3DES	168		
DES	56		
Blowfish	128		

The length of keys in bits for cryptographic algorithms which are illustrated in Table 1, are the most common key lengths that are still secure and utilized in various applications. In addition, the length of message and compressed message are represented in Table 1.

Three quality metrics to evaluate the steganography employing Huffman code compression, the five cryptographic algorithms and the LSB technique are the signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR) and Mean Square Error (MSE).

MSE depicts the degree of differences or similarity between main image and steganography image. The less the MSE value of an image is, the better the quality and distortion from the main image is [9],

$$MSE = \frac{\sum_{M,N}(T(r,c) - T'(r,c))^2}{M * N}, \tag{3.1}$$

where, M is the total number of rows, N is total number of columns. Furthermore, (r, c) are rows and columns respectively, T is original image, and T' is the changed image.

PSNR is the ratio between the original signal and the distortion signal on an image [5]. PSNR value defines the image quality. The image has more quality if the PSNR becomes greater. The PSNR value should be greater than 30dB in decibels [10],

$$PSNR = 10 * \log_{10} \left[\frac{R^2}{MSE} \right], \tag{3.2}$$

R imply the maximum fluctuation in the input image data type. Table 2 represents The SNR, PSNR and MSE values of employing Huffman code compression along with RSA, AES, 3DES, DES and Blowfish encryption algorithms on confidential message and peppers image as the cover image. The best results of five times execution applying different keys are illustrated on the mentioned tables.

TABLE 2. The SNR, PSNR and MSE values of employing Huffman code and RSA, AES, 3DES, and Blowfish on message and Peppers as cover image

Algorithm	SNR	PSNR	MSE
RSA	66.3389	72.0755	0.0040
AES	66.6585	72.3951	0.0.0037
3DES	66.8299	72.5665	0.0036
DES	66.7842	72.5207	0.0036
Blowfish	66.3389	72.5253	0.0036

The values in the form of PSNR which is high, SNR and MSE that is low, employing Huffman code compression along with RSA, AES, 3DES, DES and Blowfish encryption algorithms on confidential message and peppers image as the cover image indicates appropriate results.

Table 3 illustrates The SNR, PSNR and MSE values of employing Huffman code compression along with RSA, AES, 3DES, DES and Blowfish encryption algorithms on confidential message and Baboon image as the cover image. The best results of five times execution applying different keys are illustrated on the mentioned tables.

High PSNR and low MSE indicates the best results. The outcomes utilizing Huffman code as compression technique, RSA, AES, 3DES, DES, and Blowfish as cryptographic algorithms and LSB as steganography algorithm employing Peppers and Baboon images as cover images represent suitable method.

TABLE 3. The SNR, PSNR and MSE values of employing Huffman code and RSA, AES, 3DES, DES, Blowfish on message and Baboon as cover image

Algorithm	SNR	PSNR	MSE
RSA	66.8437	72.2816	0.0038
AES	67.0965	72.5344	0.0036
3DES	67.2546	72.6925	0.0035
DES	67.2357	72.6736	0.0035
Blowfish	67.2216	72.6595	0.0035

Figure 2 illustrates the stego images of using Peppers respectively.

Figure 1 indicates the cover images of size 512×512 as the input of the process including Peppers and Baboon images. Figure 2 illustrates the stego images where the confidential message are compressed, encrypted and embed ed into the mentioned cover images. Huffman code and RSA, AES, 3DES, DES, and Blowfish encryption algorithms applied as preprocess of steganography.

Measuring the robustness against common statistical attacks, histogram analysis between the cover image and stego image are employed. The histogram of stego images and the histogram of cover image considering peppers and Baboon images are compared in Figure 3 and Figure 4 respectively.

The outcome depicts that there is no significant difference in histograms of the cover image and stego image in both Peppers and Baboon. The most important part of this study compared to our previous work is the compression of the message before encryption and placement in the image, which makes it possible to send more confidential message in an image.

4. CONCLUSION

In this paper, compression along with cryptography and steganography are combined to achieve higher security. The compression algorithm is Huffman, the cryptographic algorithms are RSA, AES, 3DES, DES and Blowfish algorithms and the steganography technique is LSB. First, the message is compressed by Huffman code, then it is encrypted via the mentioned encryption algorithms.

(A) RSA

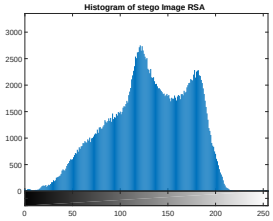
(B) AES

(C) 3DES

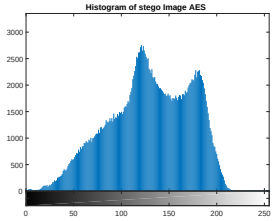
(D) DES

(E) Blowfish

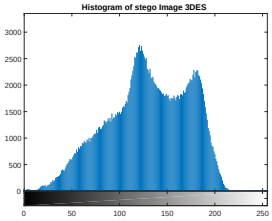
FIGURE 2. Stego images of applying (a)RSA (b) AES (c) 3DES (d) DES (e) Blowfish, and Peppers as cover image



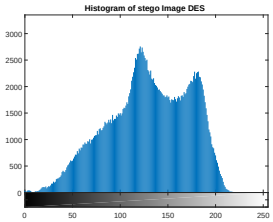
(A) RSA



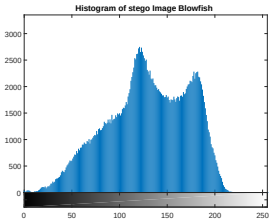
(B) AES



(C) 3DES

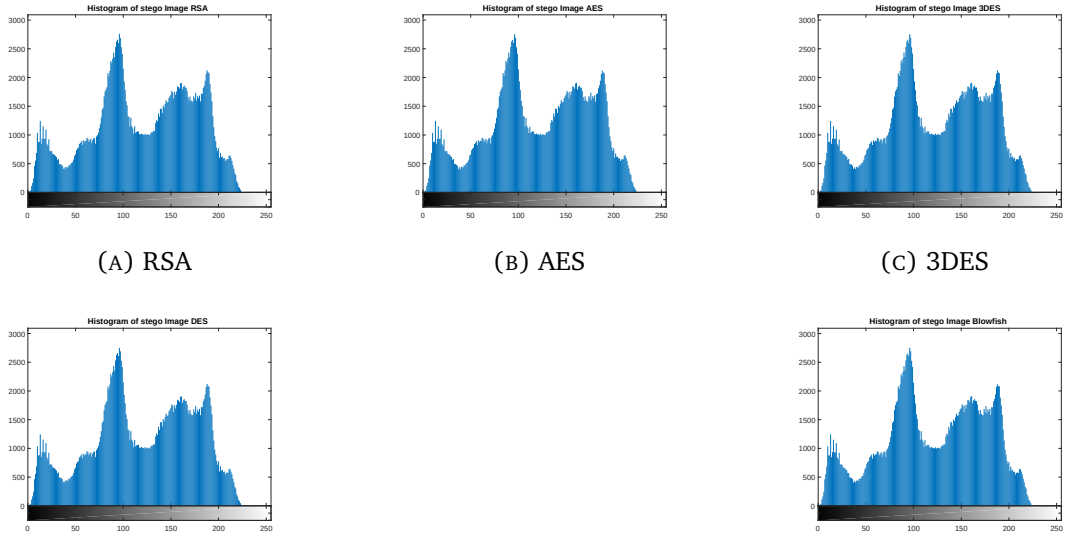


(D) DES



(E) Blowfish

FIGURE 3. Histogram of Baboon cover image applying (a)RSA (b) AES (c) 3DES (d) DES (e) Blowfish



(A) RSA (B) AES (C) 3DES

(D) DES (E) Blowfish

FIGURE 4. Histogram of Peppers stego image applying (a)RSA (b) AES (c) 3DES (d) DES (e) Blowfish

Thence the cipher text of confidential message is embedded into the cover image applying LSB algorithm. The proposed method is implemented in MATLAB R2016a. The strength of the proposed method is compared by calculating two error metrics including PSNR and MSE. The results indicate high PSNR and low MSE that represent the satisfaction of applying compression and encryption algorithms preprocess of the method. In addition, the confidential message is not easily figured out by the difference histogram analysis whereas using compression and encryption algorithms for the first step of steganography. Huffman coding algorithm not only change the appearance of the message, but also minimize the size of the main message and make it more difficult to detect the confidential message in the cover image after steganography.

REFERENCES

[1] M. DAMRUDI, MASUMEH, N. ITHNIN: *Parallel RSA encryption based on tree architecture*, Journal of the Chinese Institute of Engineers, **36**(5) (2013), 658–666.

[2] P. WAYNER: *Disappearing cryptography: information hiding: steganography and watermarking*, Morgan Kaufmann, ELSEVIER, 3rd Edition, 2009.

[3] A. A. ABDELMGED, AL-HUSSIEN SEDDIK SAAD, NADA HUSSIEN: *A Combined approach of steganography and cryptography technique based on parity checker and huffman encoding*, International Journal of Computer Applications, **148**(2) (2016).

[4] Z. S. YOUNUS, .G. T. YOUNUS: *Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data*, Journal of Intelligent Systems, **29**(1) (2019), 1216–1225.

[5] M. V. NARAYANA: *Compression, Encryption, Watermarking & Steganography (CEWS) Technique for Image Steganography*, International Journal of Latest Engineering and Management Research (IJLEMR), **3**(3) (2018), 20–27.

[6] U. M. E.ALI, M. SOHRAWORDI, M. P. UDDIN: *A Robust and secured image steganography using LSB and random bit substitution*, American Journal of Engineering Research (AJER), **8**(2) (2019), 39–44.

[7] M. DAMRUDI, K. JADIDY AVAL: *Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish*, International Journal of Engineering and Advanced Technology (IJEAT), **8**(6S3) (2019), 204–208.

[8] R. HALDER, S. SENGUPTA, S. GHOSH, D. KUNDU: *A secure image steganography based on RSA algorithm and hash-LSB technique*, IOSR Journal of Computer Engineering (IOSR-JCE), **18**(1) (2016), 39–43.

[9] A. PANDEY, P. BONDE: *Performance evaluation of various cryptography algorithms along with LSB substitution technique*, International Journal of Engineering Research & Technology (IJERT), **2**(6) (2013), 866–871.

[10] A. PANDEY, J. CHOPRA: *Steganography using AES and LSB techniques*, International Journal of Scientific Research Engineering & Technology (IJSRET), **6**(6) (2017), 620–623.

DEPARTMENT OF COMPUTER SCIENCE
FIROOZKOOH BRANCH, ISLAMIC AZAD UNIVERSITY
FIROOZKOOH, IRAN
Email address: m.damrudi@yahoo.com

DEPARTMENT OF COMPUTER SCIENCE
FIROOZKOOH BRANCH, ISLAMIC AZAD UNIVERSITY
FIROOZKOOH, IRAN
Email address: k.jadidy@yahoo.com