INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2021.15.54 Volume 15, 2021

Two Stage Steganography on Compressed and Encrypted Message

Kamal Jadidy Aval[2], Masumeh Damrudi[1,2]
[1]Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran
[2]Department of Computer Science, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran

Received: October 29, 2020. Revised: April 25, 2021. Accepted: May 17, 2021. Published: May 24, 2021.

Abstract— Security of confidential information in the insecure era of information transmission (Internet) is still one of the most important challenges of the day. The combination of cryptography and steganography increases the security of embedded data to avoid from unauthorized access. Furthermore, compression of secret data reduces the size of transmitted message. In addition to compression and encryption, in this paper, two stage steganography is employed to enhance the security. In the proposed approach, the Huffman coding as lossless compression, the Blowfish, DES, 3DES, AES, and RSA as cryptography algorithms and LSB (Least significant Bit) as steganography technique are employed with enhancement of security by two stage steganography. The results are analyzed through quality parameters including MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio), and histogram of images.

Keywords— Compression, Encryption, Huffman, LSB, Steganography.

I. Introduction

Information security is one of the common issues among all members of a society. Confidential information is spreading around the world, and unauthorized people are eager to obtain it for a variety of reasons.

Cryptography, a Greek word meaning "secret writing"[1], is one of the most important aspect of digital word [2]. Cryptography is utilized to ensure that the main message cannot be figured out. Cryptography is classified into asymmetric key (public key) and symmetric key (private key). Public key employs two different keys for encryption and decryption whereas symmetric key applies identical key for encryption and decryption.

Steganography, a Greek word meaning "covered writing", ensures that there is not a secret message. Steganography hides the existence of data by covering with another media [3]. Pure, secret key and public key steganography represent three classification of steganography. Pure steganography has no key while secret key use one key and public key steganography employs two keys [4].

Compression reduces data in size. Lossless and Lossy compressions are two types of compressions. Huffman coding which is employed in the approach of this paper is a lossless compression. The decompressed data is exactly the same as main data in lossless technique [5].

Each of Cryptography and steganography has a problem [6] however they can be employed together to provide more data protection [7]. In steganography process, employing compression decreases the data capacity and increases the amount of data to be embedded in the cover image. Compression before cryptography leads to enhancement in communication security [8].

In the proposed approach, the benefits of combining cryptography and steganography increases along with employing compression to achieve enhancement in security during transmission of confidential information and reduction in size of data. In addition, compression before cryptography improve the security [8]. The approach gains multilayer security while the approach employs two stages of steganography. In this paper RSA from asymmetric cryptography and AES, 3DES, DES, and BLOWFISH from symmetric cryptographic algorithms are selected.

RSA is still the most widely used asymmetric algorithm [6]. The best known economical and comparatively secure symmetric algorithms are AES, DES and 3DES [3]. Blowfish provides appropriate encryption rate and there has been found no effective cryptanalysis of it till now [9]. The LSB (Least Significant Bit) algorithm is most popular and general method used in steganography [6]. Unauthorized person cannot realize the small changes in patterns visually whenever LSB steganography algorithm is utilized [10]. Huffman coding compression relies on frequency of occurrence of a symbol in a message [5]. Huffman algorithms entails increase in security and capacity of embedding data.

Researchers are worked on various cryptographic algorithms and LSB steganography algorithm as a combination technique for more security. Some researchers employed compression in their studies too. Narayana in [8] and Abdelmged et. al. in [5] utilized Huffman code compression, one encryption algorithm and LSB steganography. Narayana

and Abdelmged employed RSA and RC4 respectively as cryptographic algorithm. In addition, Narayana used Digital Watermark to help owner identification.

In the proposed approach, first of all, the message is compressed by Huffman algorithm. Second, different encryption algorithms are employed in next step including Blowfish, DES, 3DES, AES, and RSA to encrypt the message in separately. Third, the cipher text is hidden in an image using LSB steganography. Furthermore, the result of previous step which is an image, is hidden in another cover image employing LSB algorithm. The approach with different cryptographic algorithms are performed and compared based on factors including MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), SNR (Signal to Noise Ratio) and the histogram.

We have issued a work that employs all these encryption algorithms along with LSB and compared them on the same environment based on various factors including MSE (Mean Square Error), SNR (Signal to Noise Ratio), encryption and decryption execution time, PSNR (Peak Signal to Noise Ratio) and the histogram [11]. Furthermore, in our next research, we append compression to the work and the results are depicted in [12]. The approach of this paper using two stage steganography leads to multilayer security. Therefore, it is not simple for intruders to find out the original message. The results of research execution represent more security via second stage of steganography.

II. Proposed Approach

Cryptography and steganography are two well-known methods to hide confidential data. The combination of these methods will promote the security of the secret message.

The process of the proposed approach is detailed as following. First of all, some preprocessing i.e. converting message to ASCII code, computation the probability of symbols in the message, is performed to apply Huffman code on the secret message. Then the message is compressed via Huffman algorithm employing MATLAB environment. Next, compressed text is encrypted by the mentioned cryptographic algorithms. Although, the key generation process take place for cryptographic algorithms in advance. The encryption algorithms performed in java and is imported to MATLAB environment. After that, the compressed and encrypted message is embedded into a cover image via LSB algorithm. The images are converted to grayscale. Finally, the image is embedded into another cover image to achieve more security. All procedures are performed in MATLAB.

The output of procedure is the hidden of compressed encrypted message in the selected cover image one and embedded into cover image two. LSB is employed in this approach due to being the easiest way of image steganography [13] which presents high security []. The least significant bit of each pixel (the 8th bit) is utilized to embed the message in LSB. Therefore, the changes in the image are not visible to the human eye. In this study, the processes of decompression and decryptions are executed to certify the accuracy of procedures and implementations.

III. Experimental Results

Two images of size 512×512 are employed as the cover images from USC-SIPI dataset [15]. Fig. 1 shows the selected images while Fig.1 (a) is the first cover image and Fig.1(b) is the second cover image. MATLAB R2016a is used as programming language environment.

The secret message is in English alphabet including 1728 bits is compressed using Huffman code. The length of compressed message is decreased to 923 bits. Then, the encryption algorithm is performed. The key length for cryptographic is as following: RSA:2048 bits, AES: 128 bits, 3DES: 168 bits, DES: 56 bits, and Blowfish: 128 bits. These key lengths are still secure and utilized in various applications. After that, the encrypted message is embedded into cover image 1 which is Fig. 1(a) using LSB. At last, the image of previous step is hidden in the second cover image that is Fig. 1(b).

Evaluating the results of this approach, we considered following quality metrics including signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), Mean Square Error (MSE), and execution time.

The degree of difference or similarity between the main image and the steganography image is MSE [16]. The more the quality and distortion from the original image is, the less the MSE value of an image would be [17].

$$MSE = \frac{\sum_{M,N}(T(r,c)-T'(r,c))^2}{M*N} \quad (1)$$

Where, M and N are total number of rows and columns. Also, (r,c) are rows and columns respectively, T is primary image, and T' is the altered image.

The ratio between the primary signal and the distortion signal on an image depicts PSNR [8] which demonstrates the quality of image. The more the quality of image is, the greater the PSNR would be. The value for PSNR should be greater than 30dB in decibels [18].

$$PSNR = 10*\log_{10}\left[\frac{R^2}{MSE}\right] \quad (2)$$

(a) (b)

Figure 1: (a) Baboon (b) Peppers cover images

The maximum fluctuation in the input image data type is demonstrated by R. Table 1 shows the SNR, PSNR, MSE, and the execution time of LSB steganography of stage one with Baboon cover image for three iterations. Table 2 illustrates the SNR, PSNR, MSE, and the execution time of LSB steganography of stage two with Peppers for three iterations. It

should be pointed out that the Huffman code compression is performed in advance before the encryption phase as explained in the proposed approach. In the rest of paper stego is employed as the abbreviation of steganography.

The results on Table 1 and Table 2 reveal that the PSNR is high enough and the MSE is low. The execution time part of the LSB steganography in stage one and stage two are low either. Therefore, the results are appropriate. Fig. 2 indicates the images of stego1 and stego2 while using RSA cryptographic algorithm. The difference value of results in three iterations depends on the key of cryptographic algorithms which is generated automatically in Table 1.

The values in Table 2 are almost equal. The point is that the LSB execution time in the second stage is almost more than twice of LSB execution time in first stage due to hide a large image in a cover image in second stage in comparison to hide a small text in a cover image. This execution time does not make delay in transmission of secret data because the process takes place in the source and destination.

Table 1: The SNR, PSNR, MSE, and LSB execution time for stego1 employing Huffman code compression and Baboon as cover image

Cryptographic algorithm	SNR	PSNR	MSE	ET (s)
RSA	66.8870	72.3249	0.0038	0.007412
	66.8179	72.2558	0.0039	0.004582
	66.7923	72.2302	0.0039	0.005226
AES	67.0420	72.4799	0.0037	0.005878
	67.1748	72.6127	0.0036	0.005527
	67.2075	72.6454	0.0035	0.006174
3DES	67.0465	72.4845	0.0037	0.005589
	67.1102	72.5481	0.0036	0.005501
	67.1424	72.5803	0.0036	0.006716
DES	67.2498	72.6878	0.0035	0.005571
	67.2357	72.6736	0.0035	0.005537
	67.0330	72.4709	0.0037	0.005844
Blowfish	67.1609	72.5988	0.0036	0.005390
	67.1841	72.6220	0.0036	0.005669
	67.0873	72.5253	0.0036	0.005437

Table 2: The SNR, PSNR, MSE, and LSB execution time for stego2 employing Huffman code compression and Peppers as cover image

Cryptographic algorithm	SNR	PSNR	MSE	ET (s)
RSA	56.4694	62.2060	0.0391	0.027145
	56.4699	62.2064	0.0391	0.018672
	56.4699	62.2064	0.0391	0.016031
AES	56.4699	62.2064	0.0391	0.023941
	56.4699	62.2064	0.0391	0.022279
	56.4699	62.2064	0.0391	0.022817
3DES	56.4699	62.2064	0.0391	0.020973
	56.4694	62.2060	0.0391	0.018120
	56.4699	62.2064	0.0391	0.017927
DES	56.4682	62.2047	0.0391	0.024189
	56.4699	62.2064	0.0391	0.014736
	56.4699	62.2064	0.0391	0.021061
Blowfish	56.4699	62.2064	0.0391	0.018753
	56.4699	62.2064	0.0391	0.018004

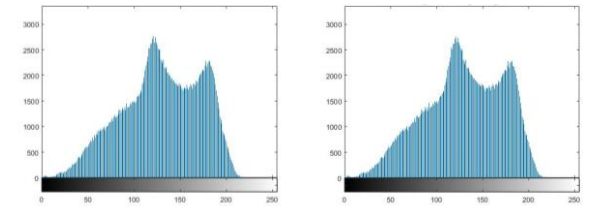
Fig. 1 reveals the color cover images of size 512 × 512 as the cover images of proposed approach for stage one and two. Fig. 2 shows the results of steganography algorithm on stage one and stage two. It must be considered that the compressed and encrypted message is embedded in Baboon in stage one and the results of this stego is hidden in peppers in stage two.

The histogram analysis between the stego image and the cover image demonstrates the robustness against common statistical attacks. Fig. 3 depicts the histogram of Baboon stego image whereas compression and AES cryptographic algorithm is utilized and the cover image.

Fig. 4 compares the histogram of Peppers cover image and the stego image in the second stage whereas the hidden image is the results of previous step (stego of Baboon). In this figure, the 3DES algorithm is performed on secret input text in the first stage.

(a) (b)

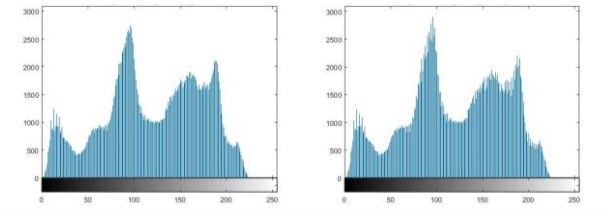
Figure 2: Stego images of applying RSA (a) Stego on stage one and Babbon as cover image (b) Stego on stage two and Peppers as cover image



(a) (b)

Figure 3: Histogram of (a) Baboon cover image (b) stego on stage one applying compression and AES on message

The histograms in Fig. 3 and Fig. 4 indicate that there is a slight difference between the histograms of the cover image and the stego images in stage one and stage two and there is no significant difference. What more, applying two phase steganography leads to more security.



(a) (b)

Figure 4: Histogram of (a) Peppers cover image (b) stego on stage two applying compression and 3DES on message in stage one

IV. Conclusion

Security is still an important part of our digital life today. The approach in this paper enhance the security of secret message due to two stage steganography. The steps are as following: compression with Huffman code, encryption via Blowfish, DES, 3DES, AES, and RSA separately in separate works, LSB steganography to hide cipher text in cover image one, LSB steganography to hide the stego image of previous step in cover image two. The whole process is implemented in MATLAB R2016a. The robustness of the proposed approach is calculated by two main error metrics including PSNR and MSE. The low MSE and high PSNR reveal the considerable results for the approach. Thence, the secret message is not found out using the difference histogram analysis easily.

References

[1] S. Panwar, S. Damani, and M. Kumar, "Digital image steganography using modified lsb and aes cryptography," International Journal of Recent Engineering Research and Development (IJRERD), ISSN: 2455-8761, vol. 3, no. 6, pp. 18-27, June 2018.

[2] M. Damrudi and N. Ithnin, "Parallel RSA encryption based on tree architecture," Journal of the Chinese Institute of Engineers, vol. 36, no. 5, pp. 658-666, 2013.

[3] Abdelkader Moumen and Hocine Sissaoui, "Images Encryption Method using Steganographic LSB Method," AES and RSA algorithm, Nonlinear Engineering, vol. 6, no. 1, pp. 53–59, 2017.

[4] P. Wayner, "Disappearing cryptography: information hiding: steganography and watermarking," Morgan Kaufmann, ELSEVIER, 3rd Edition, 2009.

[5] A. A. Abdelmged, Al-Hussien Seddik Saad, and Nada Hussien, "A Combined approach of steganography and cryptography technique based on parity checker and huffman encoding," International Journal of Computer Applications, vol. 148, no. 2, 2016.

[6] Jagdish Sharma and Ramesh Thapa, "Hybrid approach for data security using RSA and LSB Algorithm," Proceedings of IOE Graduate Conference, vol. 7,2019, pp. 1811-186.

[7] Zeyad Safaa Younus, and Ghada Thanoon Younus, "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data," Journal of Intelligent Systems, vol. 29, no. 1, pp. 1216-1225,2019.

[8] M V Narayana, "Compression, Encryption, Watermarking & Steganography (CEWS) Technique for Image Steganography," International Journal of Latest Engineering and Management Research (IJLEMR), vol. 3, no. 3, pp. 20-27, 2018.

[9] Diksha Singh, Indira Bhattacharya, and Manika Bhardwaj, "Analysis of Different Image Steganography with Encryption Techniques," International Research Journal of Engineering and Technology (IRJET), vol. 7, no. 4, 2020.

[10] U. M. E.Ali, M. Sohrawordi, and M. P. Uddin, "A Robust and secured image steganography using LSB and random bit substitution," American Journal of Engineering Research (AJER), E-ISSN: 2320-0847 p-ISSN: 2320-0936, vol. 8, no. 2, pp. 39-44, 2019.

[11] Masumeh Damrudi, Kamal Jadidy Aval, "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no. 6S3, 2019.

[12] Masumeh Damrudi, Kamal Jadidy Aval, "Image Steganography on compressed and encrypted message using RSA, AES, 3DES, DES, and Blowfish," Advances in Mathematics: Scientific Journal, vol. 9, no. 9, 2020.

[13] R. Halder, S. Sengupta, S. Ghosh, and D. Kundu, "A secure image steganography based on RSA algorithm and hash-LSB technique," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 1.

[14] Kusuma Priya B, L. P. Maguluri, T. Srinivasarao, T.E. Rao, "A Systematic Approach for Data Hiding Using Cryptography and Steganography," International Journal of Emerging Trends in Engineering Research, vol. 8, no. 4, pp. 1326-1332, April 2020.

[15] The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 6 July 2019).

[16] R. C. Gustilo, R. M. Castillo, N. A. Gonzales, J. Gerard Raz, T. J. Tejones, "Android-based Image and Video Steganography System," International Journal of Emerging Trends in Engineering Research, vol. 7, no. 9, pp. 346-352 September 2019.

[17] A. Pandey, and P. Bonde, "Performance evaluation of various cryptography algorithms along with LSB substitution technique," International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 6, pp. 866-871, 2013.

[18] A. Pandey, and J. Chopra, "Steganography using AES and LSB techniques," International Journal of Scientific Research Engineering & Technology (IJSRET), vol. 6, no. 6, pp. 620-623, 2017.

Sources of funding for research presented in a scientific article or scientific article itself
Report potential sources of funding if there is any