International Journal of Engineering & Technology, 7 (2.5) (2018) 119-121

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Increase the PSNR Of Image Using LZW and AES Algorithm With MLSB on Steganography

Erick Fitra Wijayanto[1]*, Muhammad Zarlis[1], Zakarias Situmorang[2]

[1]Faculty of Computer Science, Universitas Sumatera Utara, Medan, Indonesia
[2]Faculty of Computer Science, Universitas Katolik Santo Thomas Sumatera Utara, Medan, Indonesia
**Corresponding author E-mail: efiraw@gmail.com*

Abstract

There are many research has done a hybridization approach of text message insertion that has been compressed with Lempel-Ziv-Welch (LZW) algorithm and has also been encrypted. The text messages in ciphertext form are inserted into the image file using LSB (Least Significant Bit) method. The results of this study indicate that the value of Peak Signal to Noise Ratio (PSNR) lower than the LSB method of 0.94 times with a ratio of 20.33%, with Kekre's method of 10.04%. To improve the value of PSNR stego image of insertion, in this research is inserted audio samples using 5 bits to reduce the amount of data insertion, so it can get the value of MSE stego image low. Prior to insertion, the text file is compressed with the Lempel-Ziv-Welch (LZW) algorithm and encrypted with the Advanced Encryption Standard (AES) algorithm. Then, the insertion of compression and encrypted text files is done with the Modified Least Significant Bit (MLSB) algorithm. To performa test reliability of steganography, the image stego image is done by calculating Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). At extraction process with MLSB algorithm, decryption with AES algorithm and decompression with LZW algorithm. The experimental results show that the MSE values obtained are lower and the proposed PSNR method is better with (α) 1,044 times than the Kaur method, et al. The result of embed text file extraction from the stego image works well resulting in encrypted and uncompressed text files.

Keywords: *file compression, advanced encryption standard cryptography, steganography modified least significant bit*

1. Introduction

This research was conducted on the quality of the imagery of his guardian research by kaur[1]is found the result increasingly low PSNR[2] values along with increasing the size of the insertion[3]. To keep the quality of the image insertion, then the results do hybridization compression algorithm[4]–[7], encryption as well as the insertion of text messages into digital image files[8]–[11]. Hybridization performed on process image steganography is Lempel-Ziv compression algorithm-Welch (LZW)[1], [4], [12], encrypted with the algorithm Advanced Encryption Standard (AES)[13] algorithm with the modified insertion as well as the most significant Bit (MLSB). In this research was conducted, the results text file compression of compressed text file encryption is performed into a text file in the form Ciphertext[14]–[17], then the Ciphertext text file pasted into the image file and retrieved stego images[18], [19]. To find out the quality of the stego images, then performed the calculation value of the Mean Squared Error (MSE) [20]–[23] and Peak Signal to Noise Ratio (PSNR)[2], [24], [25] stego file from the image. Next do the extraction of text files in the files of the form Ciphertext stego images and is done in order to obtain decryption Plaintext as well as do decompression in order to return to the text[26]–[28]. To know the reliability of the algorithm, then performed the calculation value of DRR (Data Recovery Rate) of intruder, namely, a comparison of the amount of data that insert into the media cover with data extraction results back.

2. Methodology

Description in general step inserts the message into the image. The first step that is doing compression LZW algorithm with a message, and then encrypted with the AES algorithm is done to get Ciphertext[10], [29], [30]. After obtained Ciphertext message, then the insertion is done with the MLSB algorithm to obtain the stego images results insertion. The image has been insert then calculated the value of PSNR and MSE. To know the reliability of the insertion algorithm, then performed the extraction of messages from the stego file image and calculated the value of the Data Recovery Rate (DRR).

A. Compression LZW algorithm of text files

This algorithm uses a dictionary in its techniques. Where the string of characters is replaced by a code table made any string entered. The table is created to reference the input string. The size of the chart on the original LZW algorithm dictionary is 4096 samples or 12 bit, where the first sample of 256 is used for single character table (Extended ASCII), and the rest is used to couple the character or string in the input data. LZW algorithm performs compression by using code table 256 up to 4095 to encode the byte pair or string. With this method a lot of strings that can be coded with reference to the string that had appeared previously in the text[4].

B. LZW Algorithm File Decompression

LZW algorithm in doing a compressed text file[12] decompression with LZW algorithm are as follows, that is, for example, from the results of the previous compression code output taken decimal resulting to "77-65-256-32-256-83-65-75-32-78-65-83-73" and compressed with LZW algorithm. Bit dictionary used is 8 bits. Stages of the process of decompression if known input code: 77-65-256-32-256-83-65-75-32-78-65-83-73. i.e. "MA-MA_MASAK_NASI".

C. AES encryption

The AES algorithm[31], [32] in encryption takes place in the sequence of the four function Builder (primitive) that has been described, namely: SubBytes, ShiftRows (), (), (), and MixColumns AddRoundKey (). The sequence run as much as the Nr-1 as the main loops, each loop is called round (Nr = 10 round for AES-128). AddRoundKey () was executed as a loop round the initials before the primary. After the main loop terminates (a nine-round), SubBytes, ShiftRows (), (), and AddRoundKey (), executed in succession as the final round.

The AES algorithm in the Encrypt message text that has been compressed to get the ciphertext which will be inserted into the image file. For example the encryption is done with:
PLAINTEXT: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
KEY: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

D. Decryption Ciphertext

The AES algorithm in the decrypt text messages that have been compressed to obtain the plaintext that will be inserted into the image file. For example the decryption is done by Ciphertext:
CIPHER KEY = 2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
KEY : 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

3. Results and Discussion

A. Insertion Algorithm MLSB

The algorithm MLSB bit-bit message modified into 5 bits will then be inserted into the image file with the technique of LSB. The process is as follows:

1. Image Files and message input and read.
2. The message and its size is converted into ASCII form (hexadecimal).
3. The message is modified in accordance with the provisions and MLSB algorithm combined with control of his symbol.
4. When a message is modified then the message is converted into binary form.
5. Does random numbers as much as the number of bits of the message.
6. Insertion is done on a byte correspond to random numbers using the algorithm LSB.
7. If the bit-bit messages have not been exhausted then repeated step 5 until all the bit-bit message timeout is inserted (j = "null").

$$MSE = \frac{1}{XY}\sum_x\sum_x[I(x,y) - I'(x,y)]^2$$

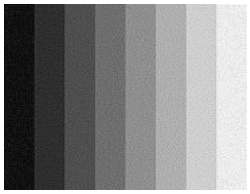
8. Embedded Image File that has been saved with messages requiring image file information.
9. Calculate the value of the MSE measurement as PSNR & quality.

B. Peak signal-to-noise rasio (PSNR)

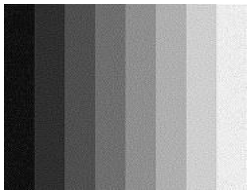
$$PSNR = 10 \log \frac{m^2}{MSE}$$

Where MSE = Mean Square Error
XY = image dimension
I = the pixel value of the cover image
I ' = pixel value of the stego images
m = maximum value of the pixel

Experiment conducted on some of the pictures below gray_img, lena_gray, lena_rgb, rgb_img. Implementation of coding in programming language visual basic 2010.



(a) gray_img (Cover-image)



(b) gray_img (Stego-image)

(c) lena_gray (Cover-image

(d) lena_gray (Stego-image)

(e) lena_rgb (Cover-image)

(f) lena_rgb (Stego-image)

(g) rgb_img (Cover-image)

(h) rgb_img (Stego-image)

Table.1: PSNR (db)

No	Cover Image	Size (byte)	Kaur (HAIS)	Proposed
1	gray_img	14,643.2	46.6492	48.66
2	lena_gray	12,390.4	44.9326	47.24
3	lena_rgb	12,697.6	43.7429	47.45
4	rgb_img	12,492.8	46.3205	46.45
	Average	13,056	45.4113	47.45

According to experimental result can be seen the proposed method of PSNR values better with (α) 1,044 times of Kaur (HAIS).

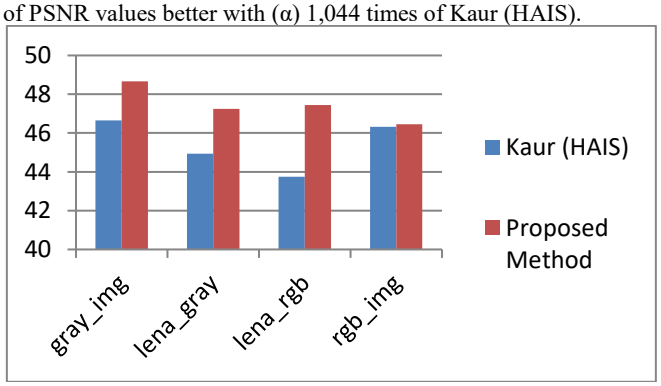


Fig.1: Graph the value of PSNR Results text File Encrypted Insertion into the Image

4. Conclusion

From the results of the experiment software Image Steganography Algorithm Using Lempel-Ziv-Welch (LZW), Advanced Encryption Standard (AES) and Modified Least Significant Bit (MLSB) that obtained results that suggested PSNR value method is better with (α) 1,044 times from Kaur method.

References

[1] D. Kaur, H. K. Verma, and R. K. Singh, "A hybrid approach of image steganography," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017.

[2] U. Khair, H. Fahmi, S. Al Hakim, and R. Rahim, "Forecasting Error Calculation with Mean Absolute Deviation and Mean Absolute Percentage Error," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012002, Dec. 2017.

[3] J. Fridrich, *Steganography in digital media: Principles, algorithms, and applications*. 2012.

[4] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, "Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression," *World Trans. Eng. Technol. Educ.*, vol. 15, no. 3, pp. 292–297, 2017.

[5] D. Rachmawati, A. Amalia, and J. Surya, "Combination of Huffman Coding Compression Algorithm and Least Significant Bit Method for Image Hiding," in *Journal of Physics: Conference Series*, 2017, vol. 801, no. 1.

[6] P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 395–403, 2000.

[7] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, and M. M. Rahman, "Tiny encryption algorithm and pixel value differencing for enhancement security message," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 82–85, 2018.

[8] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.

[9] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012005, Dec. 2017.

[10] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, p. 012003, Apr. 2018.

[11] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, pp. 366–371.

[12] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, and A. Hidayat, "An application data security with lempel - ziv welch and blowfish," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 71–73, 2018.

[13] A. Putera, U. Siahaan, and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016.

[14] Q. Kester, "A Visual Cryptographic Encryption Technique for Securing Medical Images," *arXiv Prepr. arXiv1307.7791*, vol. 3, no. 6, pp. 3–7, 2013.

[15] Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)," *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.

[16] R. Rahim *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.

[17] E. Kartikadarma, T. Listyorini, and R. Rahim, "An Android mobile RC4 simulation for education," *World Trans. Eng. Technol. Educ.*, vol. 16, no. 1, pp. 75–79, 2018.

[18] T. Zhang, W. Li, Y. Zhang, and P. Xijian, "Detection of LSB matching steganography based on distribution of pixel differences in natural images," in *IASP 10 - 2010 International Conference on Image Analysis and Signal Processing*, 2010, pp. 548–552.

[19] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3. pp. 727–752, 2010.

[20] A. Rahman and A. S. Ahmar, "Forecasting of primary energy consumption data in the United States: A comparison between ARIMA and Holter-Winters models," in *AIP Conference Proceedings*, 2017, vol. 1885.

[21] A. S. Ahmar, "A comparison of α-Sutte Indicator and ARIMA methods in renewable energy forecasting in Indonesia," *Int. J. Eng. Technol.*, vol. 7, 2018.

[22] D. U. Sutiksno, A. S. Ahmar, N. Kurniasih, E. Susanto, and A. Leiwakabessy, "Forecasting Historical Data of Bitcoin using ARIMA and α-Sutte Indicator," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, p. 012194, 2018.

[23] N. Kurniasih, A. S. Ahmar, D. R. Hidayat, H. Agustin, and E. Rizal, "Forecasting Infant Mortality Rate for China: A Comparison Between α-Sutte Indicator, ARIMA, and Holt-Winters," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, p. 012195, 2018.

[24] A. S. Ahmar, A. Rahman, A. N. M. Arifin, and A. A. Ahmar, "Predicting movement of stock of 'Y' using sutte indicator," *Cogent Econ. Financ.*, vol. 5, no. 1, 2017.

[25] A. S. Ahmar *et al.*, "Modeling Data Containing Outliers using ARIMA Additive Outlier (ARIMA-AO)," *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018.

[26] A. A. J. Altaay, S. Bin Sahib, and M. Zamani, "An Introduction to Image Steganography Techniques," in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 2012, pp. 122–126.

[27] M. Liśkiewicz, R. Reischuk, and U. Wölfel, "Security levels in steganography – Insecurity does not imply detectability," *Theor. Comput. Sci.*, vol. 692, pp. 25–45, 2017.

[28] H. Wang and S. Wang, "Cyber Warfare: Steganography vs. Steganalysis," *Commun. ACM*, vol. 47, no. 10, pp. 76–82, 2004.

[29] R. Ratnadewi, R. P. Adhie, Y. Hutama, J. Christian, and D. Wijaya, "Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system," *World Trans. Eng. Technol. Educ.*, vol. 15, no. 2, pp. 178–183, 2017.

[30] J. Hoffstein, J. Pipher, and J. H. Silverman, "Diffie–Hellman key exchange," *An Introd. to Math. Cryptogr.*, pp. 65–67, 2014.

[31] A. Widarma, "Kombinasi Algoritma AES, RC4, dan Elgamal dalam Skema Hybrid untuk Keamanan Data," *J. Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 1–8, 2016.

[32] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 6, no. 19, pp. 33–38, 2013.