TELKOMNIKA, Vol.17, No.5, October 2019, pp.2400~2409
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i5.9570

An improved security and message capacity using AES and Huffman coding on image steganography

Christy Atika Sari[1], Giovani Ardiansyah[2], De Rosal Ignatius Moses Setiadi*[3], Eko Hari Rachmawanto[4]
Department of Informatics Engineering, Dian Nuswantoro University,
207 Imam Bonjol St., Semarang 50131 Indonesia, tel: (+6224)3517261/(+6224)3569684
*Corresponding author, e-mail: atika.sari@dsn.dinus.ac.id[1], gvn.ardiansyah@gmail.com[2], moses@dsn.dinus.ac.id[3], eko.hari@dsn.dinus.ac.id[4]

Abstract

Information security is very important and has been widely implemented. Cryptography and steganography are two common methods that can be implemented to secure and conceal the information. In this research, the proposed AES algorithm for cryptography and DWT for steganography. However, in case of implementing DWT as steganography, there is a weakness which is a lower capacity. Based on DWT's problem, proposed Huffman Coding to reduce the total of the message's bit and increase the capacity. In the implementation, a message will be processed by using AES and compressed by using Huffman Coding then conceal in a cover using DWT. After doing several experiments using a 128x128 pixel message image and a 512x512 pixel of the cover image, achieved the average of MSE is 1.5676 and the average of PSNR result is above 40 db which is 46.1878.

Keywords*: AES, DWT, Huffman coding, image compression, image steganography*

1. Introduction

Currently, information security is widely used to secure or protect the information. Several common aspects that exist in information security has been implemented such as cryptography and steganography. According to [1], cryptography is a technique that aims to transform the message becomes the random message by encrypting it. On the other hand, steganography is a branch of information hiding method that aims to conceal the message in a medium, such as an image, video, audio, file [2-4]. Steganography has two different kinds of domains that are mostly used, such as spatial domain and frequency domain [4, 5].

The spatial domain is a message concealment technique that directly deals with the original pixel or data in a medium [6]. On the other hand, the frequency domain is a message concealment technique that transformed the original pixel or data in a medium becomes the frequency [7]. According to [8], the frequency domain is a better concealment technique than spatial domain because it spreads the pixel area to conceal the message. Discrete Wavelet Transform (DWT) is the algorithm that mostly used to implement the frequency domain because it has the advantage which is closed to the Human Visual System (HVS) [9, 10].

According to [11, 12], there are several aspects that should be concerned to achieve a good steganography result, such as robustness, capacity, and imperceptibility. Imperceptibility is very important because the steganography quality level will be tested by using PSNR [13]. A good imperceptibility should achieve more than 40 dB [14]. However, DWT for steganography has a weakness which is has a lower capacity to conceal a bigger message [15]. The weakness can affect the imperceptibility level will be lower when the message size that will be concealed is bigger, so needs a method that can minimize the DWT weakness.

According to [16], image compression is a technique that can be utilized to decrease the image size. There are several algorithms that can be implemented, including Run-Length Encoding (RLE), Lempel-Ziv (LZ), Discrete Cosine Transform (DCT), and Huffman Coding. According to [17], Huffman Coding is a lossless image compression (do not remove or change the original information) and easy to implement. In the implementation of steganography, the message integrity should be considered [18], so that Huffman Coding can be a suited

Received April 11, 2018; Revised November 6, 2018; Accepted March 12, 2019

algorithm for compressing the message because of its advantage. Utilizing an image compression, hopefully, can minimize the DWT weakness and increase the capacity. To secure the message authenticity, a cryptography method can be implemented in the message before concealing the message. Many popular algorithms that can be applied in cryptography, such as Data Encryption Standard (DES), 3-DES, Blowfish, Rivest–Shamir–Adleman (RSA), RC4, and Advanced Encryption Standard (AES) [19, 20]. Comparing to the other algorithms, AES has a good cryptographic algorithm based on its security and time to process [21]. In this research, a combination of cryptography and steganography which are using AES and DWT can protect the message. On the other hand, utilizing Huffman Coding in the message before doing steganography, hopefully, can increase the payload by decreasing the message bit.

2. Research Method

2.1. Basic Theory

2.1.1. Discrete Wavelet Transform (DWT)

In DWT there are several filters that can be implemented to process the signal and Haar is the simplest filter that mostly used. The implementation of DWT in the 2D image is by dividing the image into four subbands, such as LL–LH–HL–HH [10, 22], can be seen in Figure 1.

Figure 1. DWT subbands

To gain the coefficient of every subband can be used the Haar filter calculation below [22, 23] :

$$LL(x,y) = \frac{p(x,y)+p(x,y+1)+p(x+1,y)+p(x+1,y+1)}{2} \quad (1)$$

$$LH(x,y) = \frac{p(x,y)+p(x,y+1)-p(x+1,y)-p(x+1,y+1)}{2} \quad (2)$$

$$HL(x,y) = \frac{p(x,y)-p(x,y+1)+p(x+1,y)-p(x+1,y+1)}{2} \quad (3)$$

$$HH(x,y) = \frac{p(x,y)-p(x,y+1)-p(x+1,y)+p(x+1,y+1)}{2} \quad (4)$$

where, x = number of row, y = number of column, and p = the image pixel.

2.1.2. Advanced Encryption Standard (AES)

AES is the most popular cryptography algorithm that has a good security level and the fastest encryption [21, 24]. Generally, AES has four actual steps, such as SubBytes–ShiftRows–MixColumns–AddRoundKey [25, 26]. Visualization of the encryption and decryption process at AES can be seen in Figure 2 and Figure 3. To understand each process in AES, the explanation are given as below :

a. AddRoundKey

Implementing the XOR operation between each component of the block message and each component of the block key, as shown in Figure 4.

b. SubBytes & InvSubBytes

In the SubBytes and InvSubBytes process, it can be performed by looking up in the SubBytes Box (S-Box) as shown in Figure 5 for the SubBytes Process and Figure 6 for InvSubBytes.

c. ShiftRows & InvShiftRows

In this process, it is used to shift or move each message component as shown in Figure 7 for the shifting process and Figure 8 for inverse

d. MixColumns & InvMixColumns

Apply the XOR operation between the message block and the MixColumns box for the MixColumns process shown in Figure 9 and InvMixColumns Box for the InvMixColumns process that can be displayed in Figure 10.

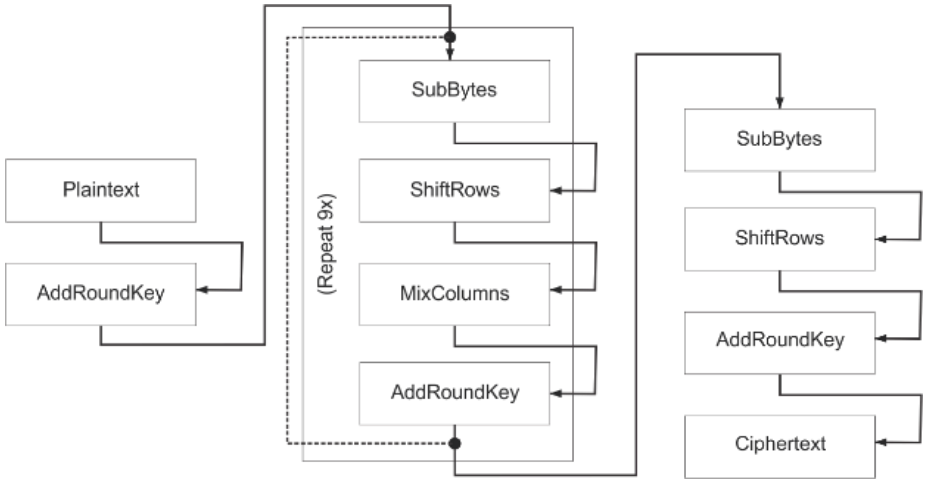


Figure 2. AES encryption

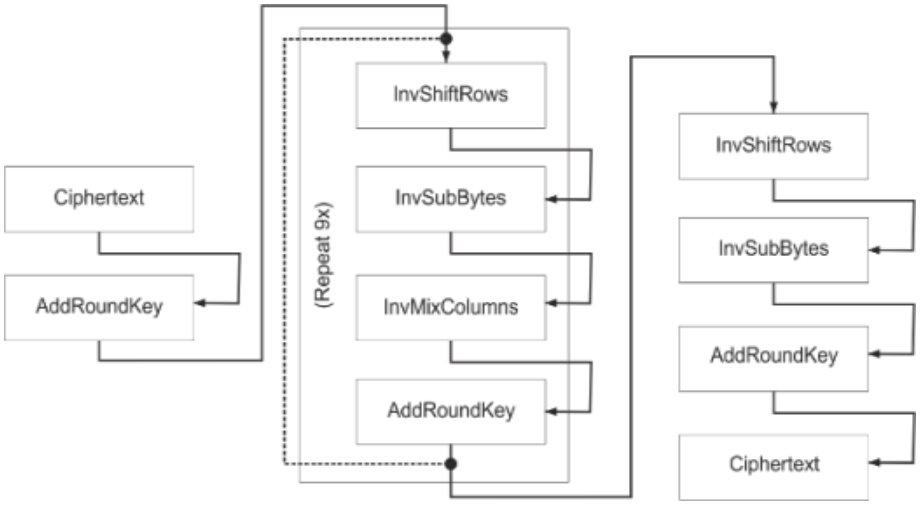


Figure 3. AES decryption

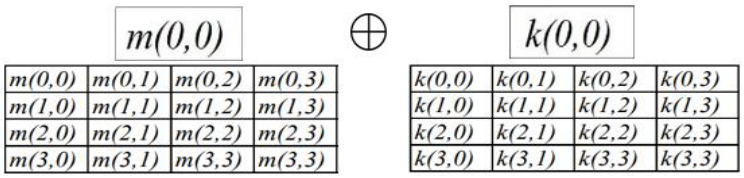


Figure 4. AddRoundKey process

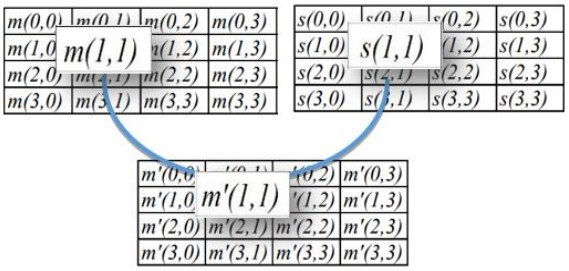


Figure 5. SubBytes process

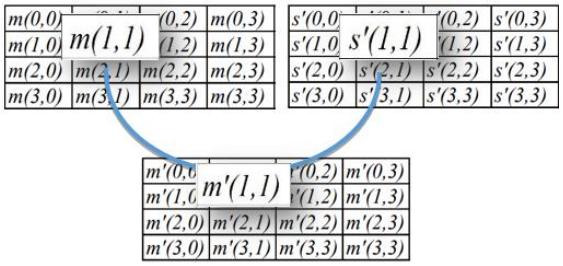


Figure 6. InvSubBytes process

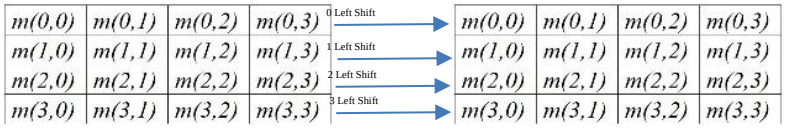


Figure 7. ShiftRows process

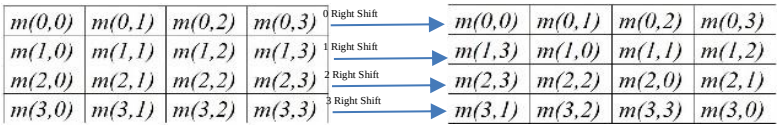


Figure 8. InvShiftRows process

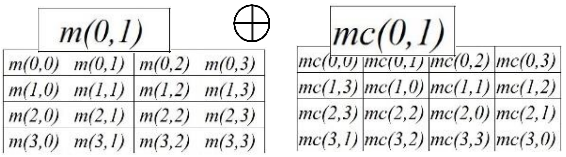


Figure 9. MixColumns process

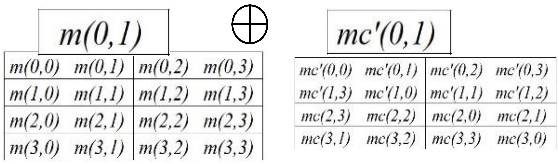


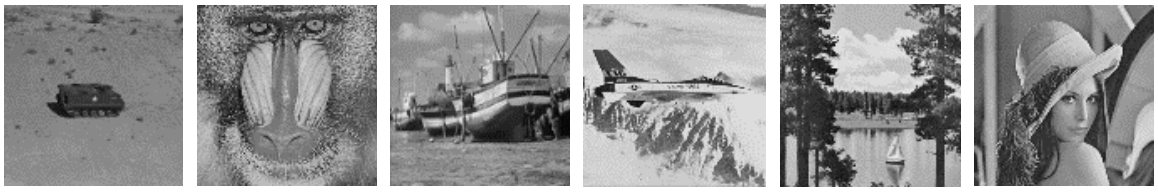
Figure 10. InvMixColumns process

2.1.3. Huffman Coding

Huffman Coding has several advantages, such as lossless image compression and easy to implement [27]. In the implementation, Huffman Coding used the occurrence of each data, then it will be sorted by ascending. Huffman Coding produced Huffman Tree that should be used to restore the data becomes the original data after being compressed.

2.2. Data Resource

Six images were downloaded from the sipi.usc.edu site used in this experiment, the image is shown in Figure 11.



(a) (b) (c) (d) (e) (f)

Figure 11. (a) apc.png, (b) baboon.png, (c) boat.png, (d) f16.png, (e) lake.png, (f) lena.png

2.3. Proposed Method

A combination of AES, Huffman Coding, and Haar DWT which aims to reduce the total of message's bit in steganography. There are two main processes, which are: embedding the message process and extracting the message process. The scheme can in Figure 12 for embedding and Figure 13 for extracting.

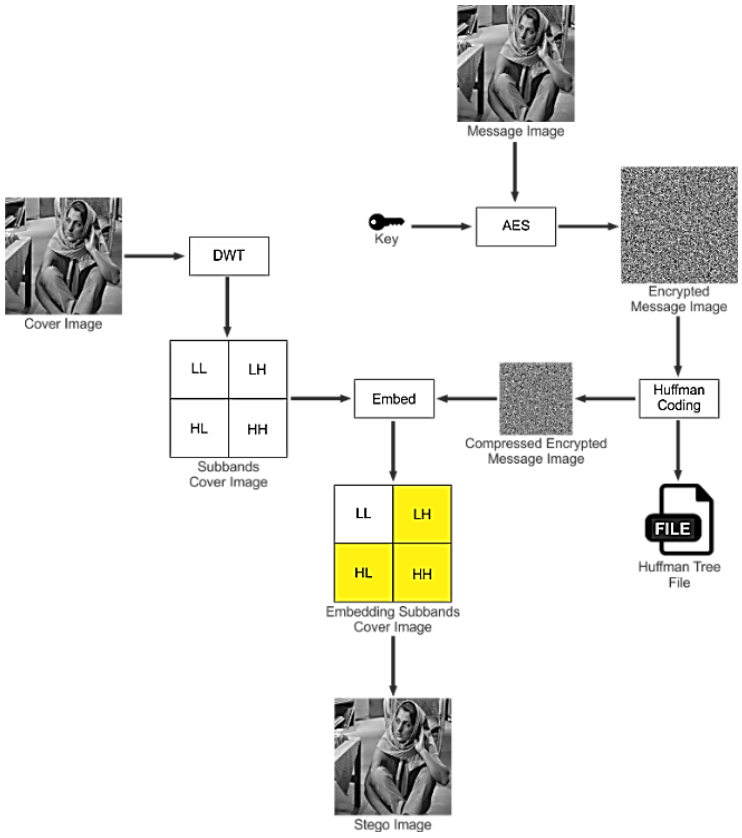


Figure 12. Embedding scheme

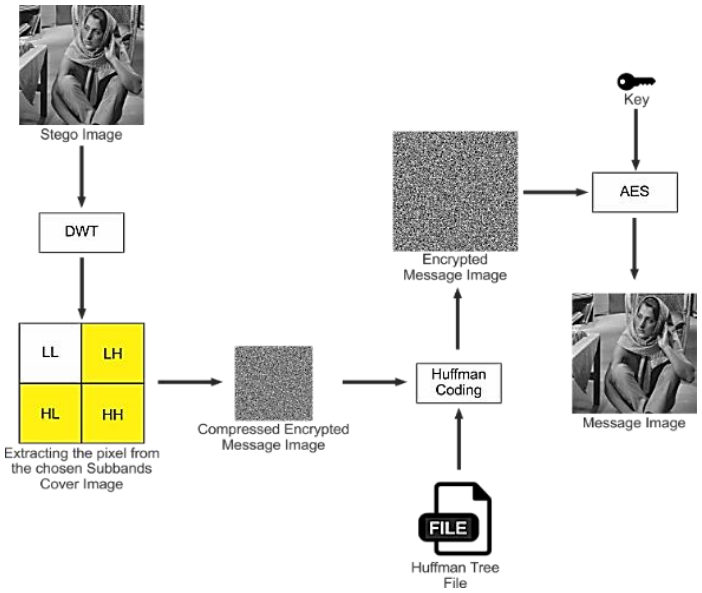


Figure 13. Extracting scheme

2.3.1. Embedding The Message Process

In the embedding process, there are several steps that should be done as follow :

- Firstly, a 128x128 pixel message image will be processed by using AES with a key and turns into an encrypted message image.
- Implementing Huffman Coding in an encrypted message image and producing two different results which are a compressed encrypted message image and Huffman tree file.
- Next step is decomposing a 512x512 pixel cover image by using DWT to get four subbands which are LL, LH, HL, and HH.
- From a compressed encrypted message image that already got, embed into the chosen subbands (LH, HL, and HH) and produce an embedding subbands of the cover image.
- The final step is composing embedding subbands of the cover image by using Inverse DWT and producing a stego image.

2.3.2. Extracting The Message Process

For the extracting process to gain a message, several steps should be followed :

- A stego image will be processed by using DWT to produce four subbands of stego image.
- Extract a message from the chosen subbands (LH, HL, and HH) and produce a compressed encrypted message image.
- Next step is by using the Huffman tree file and implementing Huffman Coding, decompress a compressed encrypted message image and producing an encrypted message image.
- Finally, decrypting an encrypted message image by using AES with a key and producing a message image.

3. Results and Analysis

3.1. Method Testing

In this research, to test and to measure the quality of stego image will be done the calculation using MSE and PSNR between an original cover image and a stego image. The details as follow :

3.1.1. Mean Square Error (MSE)

$$MSE = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(p(i,j) - q(i,j)\right)^2}{r * c} \quad (5)$$

From (5), according to [28], achieved the smaller value indicated that a stego image is more closely to be the same as an original cover image.

3.1.2. Peak Signal to Noise Ratio (PSNR)

$$PSNR = 10\, log10\left(\frac{255^2}{\sqrt{MSE}}\right) \quad (6)$$

According to [14], the higher the PSNR result and achieved more than 40 dB indicated that a stego image has a good imperceptibility.

3.2. Experiment

In this experiment, used all ten images and divided into two different sections, one image will be a cover image, and the rest which is nine images will be a message image. Here is the result of several experiments that have been done as shown in Figure 14.

After implementing Huffman Coding in each message, based on Figure 14, the total of bits are reducing and achieved the average of the total of bit reached up to 29,255 bits from 131,072 bits or it is about 22.319%. After doing several experiments achieved the average of MSE result is 1.5711 and the average of PSNR result is 46.1788. As shown in Table 1, the PSNR value means that image quality is in an excellent category.

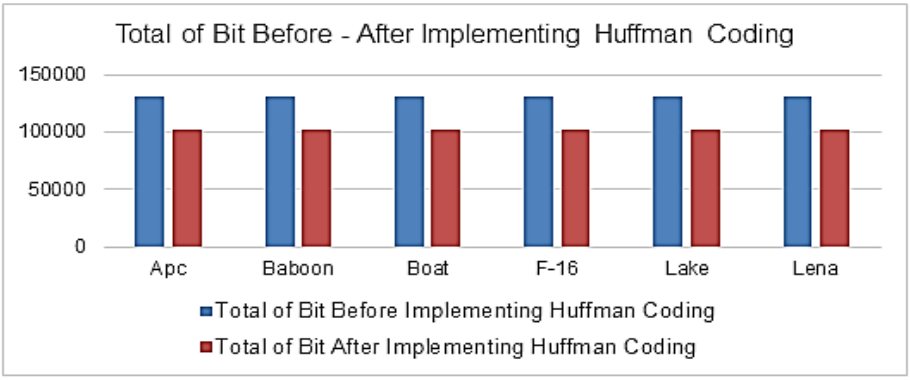


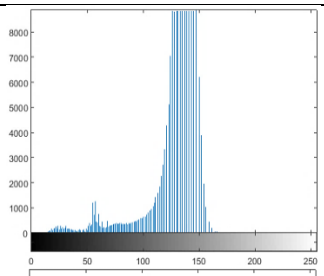
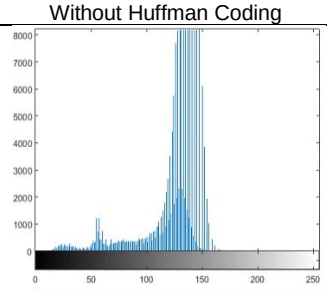
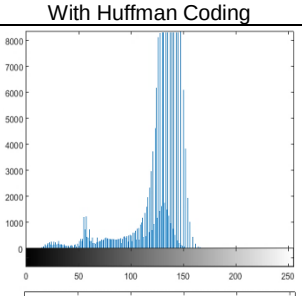
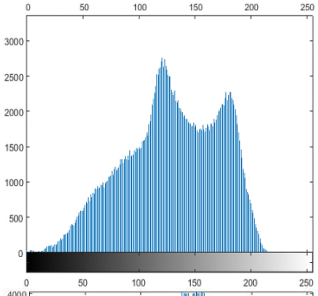
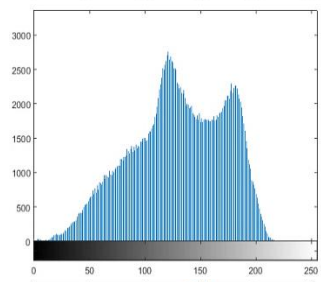
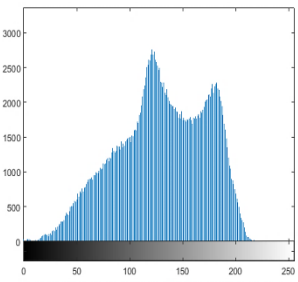
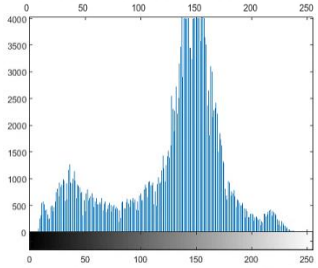
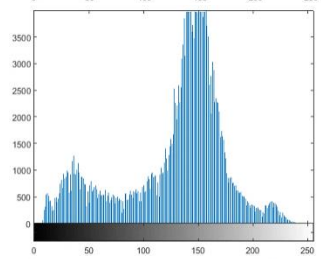
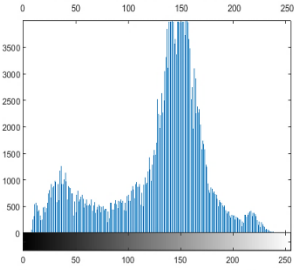
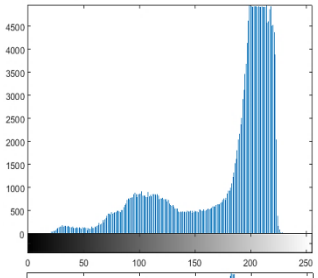
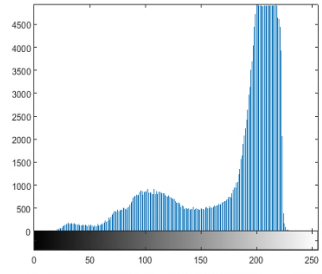
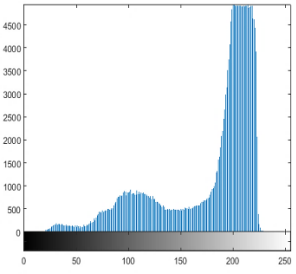
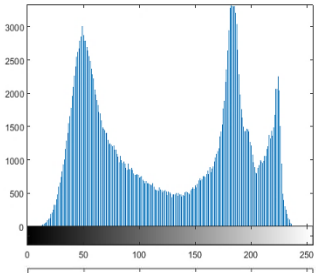
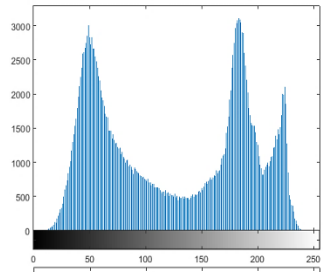
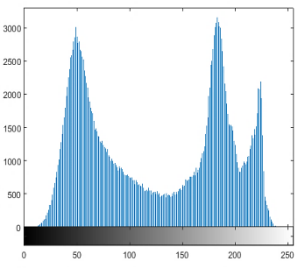
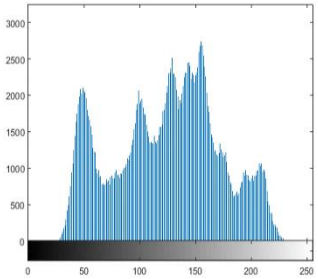
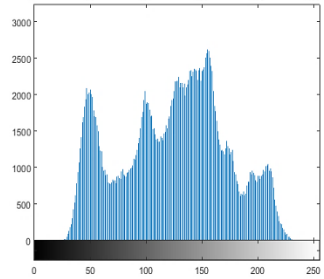
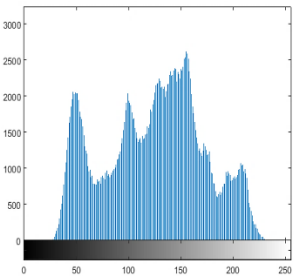
Figure 14. Total of bits before–after implementing Huffman Coding

Table 1. MSE and PSNR results of implementing the proposed method

Data		Result			
		With Huffman Coding		Without Huffman Coding	
Cover	Message	MSE	PSNR	MSE	PSNR
Apc	Baboon	1.4656	46.4708	1.8775	45.3949
	Boat	1.4708	46.4553	1.9052	45.3314
	F-16	1.4673	46.4655	1.8833	45.3816
	Lake	1.4777	46.4349	1.9035	45.3352
	Lena	1.4761	46.4396	1.9050	45.3319
Baboon	Apc	1.4535	46.5066	1.8418	45.4784
	Boat	1.4486	46.5213	1.8406	45.4813
	F-16	1.4410	46.5442	1.8385	45.4862
	Lake	1.4429	46.5385	1.8458	45.469
	Lena	1.4361	46.5589	1.8456	45.4694
Boat	Apc	1.5305	46.2825	1.9774	45.1699
	Baboon	1.5267	46.2932	1.9502	45.2300
	F-16	1.5385	46.2600	1.9744	45.1764
	Lake	1.5237	46.3018	1.9558	45.2176
	Lena	1.5373	46.2631	1.9643	45.1988
F-16	Apc	1.7460	45.7103	2.2362	44.6358
	Baboon	1.7434	45.7167	2.2565	44.5964
	Boat	1.7547	45.6888	2.2603	44.5891
	Lake	1.7408	45.7233	2.2316	44.6446
	Lena	1.7416	45.7214	2.2659	44.5784
Lake	Apc	1.5497	46.2282	2.0239	45.0688
	Baboon	1.5702	46.1712	2.0273	45.0616
	Boat	1.5684	46.1763	2.0052	45.1091
	F-16	1.5476	46.2343	2.0137	45.0909
	Lena	1.5640	46.1884	2.0162	45.0854
Lena	Apc	1.6876	45.8582	2.1354	44.8360
	Baboon	1.6720	45.8984	2.1312	44.8446
	Boat	1.6601	45.9296	2.1320	44.8429
	F-16	1.6665	45.9127	2.1025	44.9034
	Lake	1.6828	45.8704	2.1243	44.8586
Average		1.5711	46.1788	2.0157	45.0966

Based on Table 2, can be concluded that a few pixel difference that has been achieved between an original cover image and a stego image. The stego image with Huffman Coding also gave the effect in decreasing the pixel difference than the stego image without Huffman Coding, so that in a human visualization, a stego image still looks like an original cover image. This proposed method that concealed a 128x128 pixel message image into a 512x512 pixel of the cover image is produced a good quality of stego image.

Table 2. Histogram Difference

Original Cover Image	Original Cover Histogram	Message	Stego Image Histogram	
			Without Huffman Coding	With Huffman Coding
Apc		Baboon		
Baboon		Boat		
Boat		F-16		
F-16		Lake		
Lake		Lena		
Lena		Apc		

4. Conclusion

In this research, a combination of AES–Huffman Coding–DWT to secure a message image and conceal into a cover image, produced a good stego image quality. Provided a higher capacity in DWT for steganography by reducing the total of message's bit up to 22.319% from the original message's bit. A good stego image quality is proven by achieving the average of PSNR result is more than 40db which is 46.1788.

References

[1] Stallings W. Cryptography and network security: principles and practice. 6th ed. Pearson. 2013.
[2] Damara Ardy R, Indriani OR, Sari CA, Setiadi DRIM, Rachmawanto EH. *Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)*. In: Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems. IEEE. 2018.
[3] Setiadi DRIM. Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation. *Intl J Electron Telecommun*. 2019; 65(2): 295–300.
[4] Nain S, Kumar S. Steganography and Its Various Techniques. *Int J Enhanc Res Sci Technol Eng*. 2014; 3(6): 241–245
[5] Siper A, Farley R, Lombardo C. The Rise of Steganography. 2005.
[6] Chandran S, Bhattacharyya K. *Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography*. In: 2015 International Conference on Electrical, Electronics, Signals, Communication, and Optimization (EESCO). IEEE. 2015
[7] Bhattacharyya S, Sanyal G. Computer Network and Information Security. *Comput Netw Inf Secur*. 2012: 7: 27–40.
[8] Sari WS, Rachmawanto EH, Setiadi DRIM, Sari CA. A Good Performance OTP encryption image based on DCT-DWT steganography. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2017: 14(4): 1982-1989
[9] Baby D, Thomas J, Augustine G, George E, Michael NR. A Novel DWT Based Image Securing Method Using Steganography. *Procedia Comput Sci*. 2015; 46: 612–618.
[10] Setyono A, Setiadi DRIM, Muljono M. *StegoCrypt method using wavelet transform and one-time pad for secret image delivery*. In: 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE). IEEE. 2017: 203–207.
[11] Budiman G, Novamizanti L, Iwut I. *Genetics algorithm optimization of DWT-DCT based image Watermarking*. J Phys Conf Ser. 2017; 795(1): 012039.
[12] Wahab OFA, Hussein AI, Hamed HFA, Kelash HM, Khalaf AAM, Ali HM. Hiding data in images using steganography techniques with compression algorithms. *TELKOMNIKA Telecommunication Computing Electronics and Control*. 2019; 17(3): 1168.
[13] Cheddad A. Steganoflage: A New Image Steganography Algorithm. 2009.
[14] Setiadi DRIM, Jumanto J. An enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel edge detection. *Cybern Inf Technol*. 2018; 18(2): 74–88.
[15] Tushara M, Navas KA. Image Steganography Using Discrete Wavelet Transform-A Review. *Int J Innov Res Electr Electron Instrum Control Eng nCORETech*. LBS Coll Eng Kasaragod. 2016; 3(1): 2321–5526.
[16] Patel R, Kumar V, Tyagi V, Asthana V. *A fast and improved Image Compression technique using Huffman coding*. In: 2016 International Conference on Wireless Communications, Signal Processing, and Networking. IEEE. 2016: 2283–2286.
[17] Sarkar SJ, Sarkar NK, Banerjee A. *A novel Huffman coding based approach to reduce the size of large data array*. In: 2016 International Conference on Circuit, Power and Computing Technologies. IEEE. 2016: 1–5.
[18] Atoum MS, Ibrahim S, Sulong G, Zamani M. A New Method for Audio Steganography Using Message Integrity. *J Converg Inf Technol*. 2013; 8(September): 35–44.
[19] Chandra S, Paira S, Alam SS, Sanyal G. *A comparative survey of Symmetric and Asymmetric Key Cryptography*. In: 2014 International Conference on Electronics, Communication and Computational Engineering. IEEE. 2014: 83–93.
[20] Setiadi DRIM, Rachmawanto EH, Sari CA, Susanto A, Doheir M. A *Comparative Study of Image Cryptographic Method*. In: 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE). IEEE. 2018: 336–41.
[21] Rao SK, Mahto D, Khan DA. A Survey on Advanced Encryption Standard. *Int J Sci Res*. 2017; 6(1): 711–724.
[22] Ardiansyah G, Sari CA, Setiadi DRIM, Rachmawanto EH. *Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm*. In: 2017 2nd International conferences on Information Technology, Information Systems, and Electrical Engineering. IEEE. 2017: 249–54.

[23] Yasin A, Shehab MN, Sabha M, Yasin M. An Enhanced Steganographic Model Based on DWT Combined with Encryption and Error Correction Techniques. *International Journal of Advanced Computer Science and Applications*. 2015; 6(12).
[24] Rachmawanto EH, Amin RS, Setiadi DRIM, Sari CA. *A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size*. In: Proceedings-2017 International Seminar on Application for Technology of Information and Communication: Empowering Technology for a Better Human Life, iSemantic 2017. 2018.
[25] Saraf KR, Jagtap VP, Mishra AK. Text and Image Encryption Decryption Using Advanced Encryption Standard. *Int J Emerg Trends Technol Comput Sci*. 2014; 3(3): 118–126.
[26] Prasetyadi G, Refianti R, Mutiara AB. File Encryption and Hiding Application Based on AES and Append Insertion Steganography. TELKOMNIKA. 2018 Feb 1; 16(1):361.
[27] Dhawale N. *Implementation of Huffman algorithm and study for optimization*. In: 2014 International Conference on Advances in Communication and Computing Technologies. IEEE. 2014: 1–6.
[28] Farahani MRD, Pourmohammad A. *A DWT Based Perfect Secure and High Capacity Image Steganography Method*. In: 2013 International Conference on Parallel and Distributed Computing, Applications and Technologies. IEEE. 2013: 314–317.