ICITACEE

by Andik Setyono

Submission date: 16-May-2019 12:49PM (UTC+0700)

Submission ID: 1131309097

File name: International_Conference_1_ICITACEE.pdf (517.91K)

Word count: 2999

Character count: 15344

Proc. of 2017 4th Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE), Oct 18-19, 2017, Semarang, Indonesia

StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery

Andik Setyono, De Rosal Ignatius Moses Setiadi, Muljono
Faculty of Computer Science, Dian Nuswantoro University
Semarang, Indonesia
Email: andik.setyono@dsn.dinus.ac.id, moses@dsn.dinus.ac.id, muljono@dsn.dinus.ac.id

***Abstract*— In this study, the StegoCrypt technique is proposed using a combination of Discrete Wavelet Transform (DWT) and One-Time Pad (OTP). Cover image with size 512 * 512 transformed with Wavelet transformation of four levels. For the first level to the third level, the subband LL is selected to obtain LL3 subband. At fourth level, the LL3 is then transformed into HH4 subband with help of wavelet transformation. This is done to gain strength and imperceptibility to the stego image. The secret message that is used is a binary image with a size of 32 * 32. Secret image is encrypted with OTP before it is inserted in the host image. To test the quality of imperceptibility, stego images were measured using PSNR and MSE. While the quality of secret image reconstruction of extraction and decryption results are measured by using NCC. Robustness of stego image is also tested with JPEG compression attacks. From the test results can be concluded that the proposed method works well and get a better quality stego image. The secret image reconstruction results are also perfect as well as robust to JPEG compression attacks.**

Keywords—Discrete Wavelet Transform; One-Time Pad; Image Steganography; Image Encryption; Image Cryptography

I. Introduction

Currently messaging via the Internet network is a favorite thing because it is fast and practical. Not infrequently the secret message is also sent via the Internet. But the Internet is a public network that is accessible to all people in the world. This may cause an interruption in the messaging process. The dangerous thing is when the message is stolen by an unauthorized person [1]. Therefore it is necessary to safeguard the sending of messages, so messages sent from the sender can be safe to the recipient.

There are two techniques that have been popular and widely used in message security process, i.e., steganography and cryptography [2]. Steganography is the technique of hiding messages on an object in order to fool the human visual sense [3]. Steganography can be solved in two ways, namely spatial domain, and frequency domain. Pixel Value Differencing (PVD) and Least Significant Bit (LSB) is a widely used technique in the spatial domain of steganography [4]. Fourier, Tschebischev, Cosine, and Wavelet have widely used transformation in domain frequency steganography [1] [5] [6]. Frequency domains are mostly chosen on steganography as it is stronger against manipulation and distortion in the image [2] [7].

Cryptography is a technique for converting the form of a message into another form that has a different meaning to the message itself, possibly even tampering like a corrupted file. There are two main processes in cryptography, namely encryption, and decryption [8]. Both of these processes always use the key. In the key encryption process serves to change the plaintext into ciphertext, while the decryption key functions to return the cipher text to plain text. There are two kinds of cryptographic techniques, namely symmetrical and asymmetric. Asymmetric cryptography is a cryptographic technique that uses different keys when performing encryption and decryption. While symmetric cryptography uses the same key while doing the process of encryption and decryption. One-Time Pad (OTP) is one of symmetric cryptography techniques that is very safe and difficult to solve [9]. Currently, the combination of steganography and cryptography is becoming more popular, this is due to the layered security of the message so that the message more difficult to be stolen and solved. The combination of steganography and cryptography here is often referred to as StegoCrypt.

II. Related Work

E. H. Houssein et. al. [1] proposed a combination of Haar Discrete Wavelet Transform (HDWT) to insert data and AES to encrypt messages. The cover image used is a grayscale image with size 512 * 512. Embedded message on the image in the form of text with a message length of 1 to 500 characters. Stego image quality is measured by Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Mean Absolute Error (MAE).

D. R. I. M. Setiadi et. al. [1] proposed the use of 16 * 16 sub-block based DCT for insertion of messages that have been encrypted with OTP algorithm. The insertion is done on the DC part coefficient, the message is inserted in the form of a binary image with size 32 * 32 and cover image with size 512 * 512. Stego image quality is measured by PSNR and MSE. The decrypted and extracted message is compared with the original message to get the value of Normalize Cross Correlation (NCC). In this study also performed resistance test with JPEG and Median filtering compression.

S. Singh and T. J. Siddiqui [10] proposed using 8 * 8 DCT sub-blocks in which messages were inserted in the mid-coefficient section. Where messages are inserted in the form of

978-1-5386-3947-4/17/$31.00 ©2017 IEEE

a binary image with size 64 * 64. The message is encrypted with an Arnold transformation before it is inserted. While the cover image is a grayscale image with size 512 * 512. Stego image quality is measured by PSNR and MSE, while extracted and decrypted messages are measured by Normalize Correlation (NC) and Bit Error Ratio (BER). In this study also performed robustness test with JPEG compression, low-pass filtering, noise addition, and cropping.

M. Jain dan S. K. Lenka [11] in his research proposed the use of LSB and One-Time Pad (OTP) for the StegoCrypt scheme. The message insertion technique uses LSB with master variables, where messages can be inserted in 6th, 7th, or 8th bits. The cover image used is a color image. Messages inserted in the form of text that consists of only characters with the size of 8 to 128 bytes. Before this message is embedded, encrypt with OTP. Stego image quality is measured by PSNR and MSE.

S. N. Gowda [12] proposed the LSB technique for message insertion, while encryption was performed in two stages, with AES and RSA. The cover image used is a color image with a size of 1280 * 780 with text messages that embed with the size of 1kB to 512kB. The quality of stego images is measured by PSNR and MSE.

III. Basic Theory of Discrete Wavelet Transform and One-Time Pads

A. *Discrete Wavelet Transform (DWT)*

DWT is widely used in hiding message because it can perform spatial localization well and has multi-resolution characteristics in accordance with the model theory of human visual system (HVS) [13]. The image transformed with DWT will be divided into four subbands, namely LL, LH, HL, HH. LL is a subband that contains low frequency or contains the value of approximation of the image. LH is a subband that contains a low-high frequency or horizontal index value in the image. HL is a subband that contains high-low frequency or vertical index image value. While HH is a subband that contains high frequency or diagonal image index value [14]. The LL coefficients have some advantages compared to other coefficients that have an optimal approach for the original image because most of the image energy concentrates on this frequency [13], [15], [16]. Fig. 1 shows image decomposition on DWT.

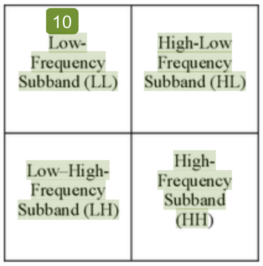
Low-Frequency Subband (LL)
High-Low Frequency Subband (HL)
Low–High-Frequency Subband (LH)
High-Frequency Subband (HH)

Fig. 1. DWT Composition Subband

B. *One-Time Pad (OTP)*

OTP is asymmetric cryptography technique, which uses randomly generated keys. This key is used to perform the encryption and decryption process. OTP technique was first created by G. Vernam in 1917. The process of encryption and decryption using XOR operators on key and secret messages [14]. This technique is very powerful and is resistant to brute force attacks if the key is truly random and only once used [1] [14].

IV. Proposed Method

In this section, the StegoCrypt technique is proposed with four levels of DWT and OTP encryption. This technique is used for securing the secret image delivery. The process is divided into two sides: the sender and the receiver.

A. *Sender Side Method*

On the sender side of the secret image will be done the process of encryption and insertion of secret images on the cover image. Here are the details of the steps in the algorithm on the sender side:

Step 1: Open and read the cover image, then save into variable (C_i).

Step 2: Perform three-level DWT and get LL3 subband, see Fig.2.

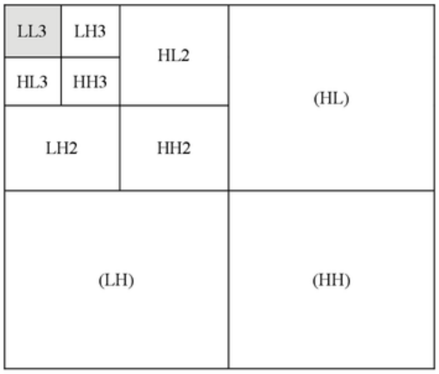

Fig. 2. 3-Level DWT Composition

Step 3: Perform DWT on LL3 subband and get HH4 subband. Save subband HH4 for key extraction process (K_e). See Fig. 3.

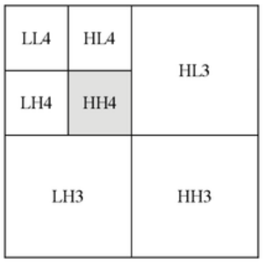

Fig. 3. 4th Level DWT Composition

Step 4: Open and read secret image, the save into variable (S_i).

Step 5: Generate random key (K_r) with the same size as the secret image.

Step 6 : Use Eq .1 to perform OTP on secret image (S_i) with random key (K_r) to get chipertext of secret image (CT_i).

$$CT_i = (S_i + K_r) \bmod i \qquad (1)$$

Where i is 2.

Step 7: Embed (CT_i) into HH4 subband to get stego HH4, use Eq. 2.

$$HH4_s = HH4 + (CT_i * Z) \qquad (2)$$

Where Z is embedding strength value

Step 8: Perform inverse transformation using four levels of IDWT, then stego image is generated

B. Receiver Side Method

On the receiver side requires input stego image and key. The output is the recover secret image obtained from the extraction and decryption process of the stego image. Here are the details of the steps in the algorithm on the receiver side:

Step 1: Open and read stego image, then save into variable (St_i).

Step 2: Perform three-level DWT, then take LL3 subband.

Step 3: Perform DWT on LL3 subband and get HH4 subband.

Step 4: Extract encrypted secret image (Es_i) on HH4 of stego image using (K_e), with Eq. 3.

$$Es_i = (HH4 - K_e)/Z) \qquad (3)$$

Step 5: Decrypt encrypted secret image using Eq. 4. then get decrypted secret image(DS_i)

$$DS_i = (Es_i - K_r) \bmod i \qquad (4)$$

IV. Experimental Result and Comparative Study

In this paper, we used a grayscale image with size 512*512 for the cover image. The number of cover images tested there are six, namely barbara.bmp, peppers.bmp, cameraman.bmp, women.bmp, lena.bmp, f16.bmp. The six images can be seen in Fig. 4. Whereas, for the secret image used is a binary image with a size of 32 * 32. The OTP key is generated by a random generator. All of our experiments work with MATLAB.

Fig. 4. Cover Image Used {(a) barbara.bmp, (b) peppers.bmp, (c) cameraman.bmp, (d) women.bmp, (e) lena.bmp, (f) f16.bmp}

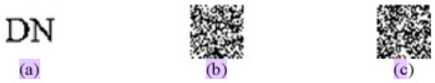

Fig. 5. {(a) secret image used, (b) sample OTP key, (c) encrypted secret image}

Fig 5. shows the encryption process occurring in the secret image. Once encrypted the secret image is inserted into the cover image so as to produce stego image. To measure stego image quality used PSNR and MSE. Where PSNR and MSE are obtained by comparing stego image with cover image. MSE is used to measure errors in the stego image, the higher the MSE value the poorer the quality of the image. Eq 5 and Eq.6 are formulas to compute MSE.

$$diff = St_i(a,s,d) - C_i(a,s,d) \qquad (5)$$

$$MSE = \sum_{a=0}^{A-1} \sum_{s=0}^{S-1} \sum_{d=0}^{D-1} \| diff \|^2 \qquad (6)$$

Where: a,s, and d is size of image.

While PSNR serves to measure the quality of stego image. The higher the PSNR value the stego image becomes more identical to the cover image. Eq. 7 is the PSNR formula we use.

$$PSNR_{dB} = 10 \log 10 \left(\frac{255^2}{\sqrt{MSE}} \right) \qquad (7)$$

Fig. 6 shows the PSNR value graph of the results of this study. Can be seen in the picture that the average value of stego image PSNR is 54.213dB. This value proves that the stego image quality is good because everything is above 40dB [11]. This value is also comparable with the results of the research [1].

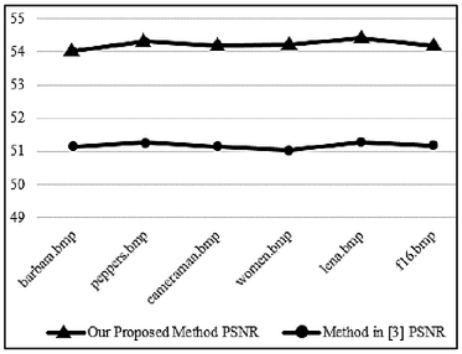

Fig. 6. Comparative PSNR Value for Different Stego Image

While Fig. 7 shows the MSE value of each stego image. The average value of MSE stego image is 0.247. This value is quite good when compared with research [1].

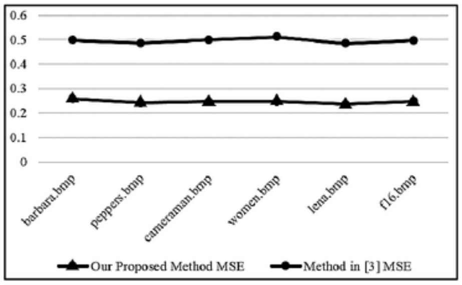

Fig. 7. Comparative MSE Value for Different Stego Image

At the end of the experiment was done the measurement of the quality of extraction and decryption of the secret image with NCC. The value of NCC ranges from 0 to 1, the better the value of NCC then the value will be close to 1. Eq. 8 is the formula for calculating the NCC.

$$ncc = \frac{S_i \times DS_i}{S_i \times S_i} \qquad (8)$$

where:

$\sum_a \sum_s$ = sum of pixel value with size a*s
S_i = secret image
DS_i = Decrypted secret image

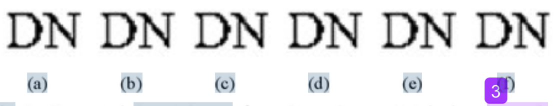

Fig. 8. Decrypted Secret Image from Stego Image {(a) barbara.bmp, (b) peppers.bmp, (c) cameraman.bmp, (d) women.bmp, (e) lena.bmp, (f) f16.bmp}

Fig. 8 shows the extraction and decryption of the secret image of each stego image. From the measurement of NCC formula obtained value 1 on all decryption of secret image. This shows that the results of extraction and decryption on the image can be done perfectly. For more details can be seen in Table I.

TABLE I. NCC VALUE EXTRACTED AND DECRYPTED SECRET IMAGE WITHOUT ATTACK

Image File	NCC
barbara.bmp	1
peppers.bmp	1
cameraman.bmp	1
women.bmp	1
lena.bmp	1
f16.bmp	1

Stego image is also resistant to JPEG attacks, this is evidenced by the high value of NCC which can be seen in Table II. Testing against JPEG attacks is done because in sending data via the internet is often done compression, and the standard compression image is JPEG.

TABLE II. NCC VALUE EXTRACTED AND DECRYPTED SECRET IMAGE WITH JPEG ATTACK

Image File	50% Quality	75% Quality
barbara.bmp	0.9143	1
peppers.bmp	0.9011	0.9989
cameraman.bmp	0.8993	1
women.bmp	0.8769	0.9957
lena.bmp	0.9065	1
f16.bmp	0.8813	0.9988

VI. CONCLUSION

This research proposes new methods on steganography and cryptography techniques (StegoCrypt) using four DWT levels and OTP encryption. The selection of LL subband on the first three DWT levels aims to make the image more robust. This can be proved by the NCC value of JPEG compression attacks. While the HH subband selected at the fourth level of DWT aims to improve imperceptibility. Based on the experimental results found in section V, it can be seen that the method proposed in the study works well. Evidenced by the results of PSNR and MSE on stego image and the perfect value of NCC on the extraction of secret image. The use of a very simple and powerful OTP algorithm provides a powerful protection against secret image messages. This method can be used to provide double security of secret image sent via the Internet, by combination steganography and cryptography.

REFERENCES

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Secure Image Steganography Algorithm Based on DCT," Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1-11, 2017.

[2] E. H. Houssein, M. A. S. Ali and A. E. Hassanien, "An image steganography algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System," in Federated Conference on Computer Science and Information Systems (FedCSIS), Gdansk, 2016.

[3] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.

[4] S. A. Thanekar and S. S. Pawar, "OCTA (STAR) PVD: A different approach of image steganography," in IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Enathi, 2013.

[5] A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari, and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (ISemantic), Semarang, 2017.

[6] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto, and C. A. Sari, "Fast and Efficient Image Watermarking Algorithm using Discrete Tchebichef Transform," in International Conference on Information Technology for Cyber and IT Service Management (CITSM), Denpasar, 2017.

[7] C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Robust and Imperceptible Image Watermarking by DC Coefficients Using Singular Value Decomposition," in International Conference on Electrical Engineering, Computer Science, and Informatics (EECSI), Yogyakarta, 2017.

[8] H. A. Elsayed, Y. K. Jadaan and S. K. Guirguis, "Image Security Using Quantum Rivest-Shamir-Adleman Cryptosystem Algorithm and Digital Watermarking," in Progress in Electromagnetic Research Symposium (PIERS), Shanghai, 2016.

[9] B. J. Saha, Arun, K. K. Kabi, and C. Pradhan, "Non blind watermarking technique using enhanced one time pad in DWT domain," in International Conference onComputing, Communication and Networking Technologies (ICCCNT), Hefei, 2014.

[10] S. Singh and T. J. Siddiqui, "A Security Enhanced Robust Steganography Algorithm for Data Hiding," International Journal of Computer Science Issues, (IJCSI), vol. 9, no. 1, pp. 131-139, 2012.

[11] M. Jain and S. K. Lenka, "Secret Data Transmission using Vital Image Steganography over Transposition Cipher," in International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015.

[12] S. N. Gowda, "Advanced Dual Layered Encryption for Block Based Approach to Image Steganography," in International Conference on Computing, Analytics and Security Trends (CAST), Pune, 2016.

[13] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science, vol. 3, pp. 740-746, September 2007.

[14] B. J. Saha, Arun, K. K. Kabi, and C. Pradhan, "Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain," in International Conference on Computing, Communication and Networking Technologies (ICCCNT), Hefei, 2014.

[15] W. Na, W. Yunjin and L. Xia, "A Novel Robust Watermarking Algorithm Based on DWT and DCT," in International Conference on Computational Intelligence and Security, 2009.

[16] A. Susanto, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," in International Conference on Information Technology for Cyber and IT Service Management (CITSM), Denpasar, 2017.

ICITACEE

ORIGINALITY REPORT

15%	7%	5%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Dian Nuswantoro Student Paper	2%
2	Submitted to Brunel University Student Paper	2%
3	media.neliti.com Internet Source	1%
4	Submitted to Universitas Jember Student Paper	1%
5	Submitted to University of Liverpool Student Paper	1%
6	"Table of contents", 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 2017 Publication	1%
7	eprints.undip.ac.id Internet Source	1%
8	www.csroc.org.tw Internet Source	1%

9	Muljono, Askarya Qaulan Syadida, De Rosal Ignatius Moses Setiadi, Andik Setyono. "Sphinx4 for Indonesian continuous speech recognition system", 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), 2017 Publication	1%
10	Der-Chyuan Lou. "Highly robust watermarking scheme based on surrounding mean value relationship", Optical Engineering, 2005 Publication	1%
11	ijsetr.org Internet Source	1%
12	archive.org Internet Source	<1%
13	edlib.asdf.res.in Internet Source	<1%
14	Kaur, L., R. C. Chauhan, and S. C. Saxena. "Wavelet based compression of medical ultrasound images using vector quantization", Journal of Medical Engineering & Technology, 2006. Publication	<1%
15	Submitted to Pacific University Student Paper	<1%

16	Submitted to University of Nottingham Student Paper	<1%
17	pnrsolution.org Internet Source	<1%
18	paper.ijcsns.org Internet Source	<1%
19	www.irjet.net Internet Source	<1%
20	Submitted to University of East London Student Paper	<1%
21	Submitted to iGroup Student Paper	<1%
22	"International Conference on Computer Networks and Communication Technologies", Springer Nature America, Inc, 2019 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		