JOP_1

by Andik Setyono

Submission date: 16-May-2019 12:09PM (UTC+0700)

Submission ID: 1131293894

File name: International_Journal_4_JOP_1.pdf (646.79K)

Word count: 3057

Character count: 16229

Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Imperceptible Improvement of Secure Image Steganography based on Wavelet Transform and OTP Encryption using PN Generator

To cite this article: Andik Setyono and De Rosal Ignatius Moses Setiadi 2019 *J. Phys.: Conf. Ser*. **1196** 012031

View the article online for updates and enhancements.

IOP ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

This content was downloaded from IP address 36.72.218.208 on 16/04/2019 at 16:05

Imperceptible Improvement of Secure Image Steganography based on Wavelet Transform and OTP Encryption using PN Generator

Andik Setyono, De Rosal Ignatius Moses Setiadi

Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Indonesia

Email: andik.setyono@dsn.dinus.ac.id

Abstract. Digital data is widely transacted through internet media that can be accessed publicly, so this requires security of the data. This research proposes a combination of steganography and cryptography methods using wavelet transforms and OTP encryption based on PN generators. The PN generator is used as a tool to generate binary random numbers that are used to improve the quality of the embedding process and the encryption process. Messaging is carried out with four levels of wavelet transformation, the first three levels of the LL subband are selected to be transformed, while the fourth level wavelet transformation is selected for the HH subband to be embedded. This subband selection strategy is carried out with the aim of getting good imperceptibility and robust values. While OTP encryption is proposed because it has strong encryption results with a lightweight computing process. Based on the experimental results, binary random numbers generated by PN generators have been proven to successfully improve the quality of stego images and security. This has been measured by the PSNR and MSE, where there are remembrances on the two measuring instruments.

1. Introduction

The internet is a public network that can be used by all people in the world to conduct digital data transactions. Important digital data should be secured so that they cannot be misused by others [1] [2]. Some techniques that are widely used are by hiding or encoding the data before the data is sent. Data hiding techniques that are widely used are watermarking and steganography [3] [4]. Both of these techniques have similarities in how to hide data, which distinguishes these two techniques from their purpose. Watermarking is useful to protect ownership of data, while steganography is done with the aim of deceiving people so they do not know the hidden data [3] [5] [6].

Steganography techniques in many images are done with two kinds of domains, namely the transformation domain and spatial domain [7] [8] [9]. The transformation domain has a relatively more complex computation than the spatial domain so that the transformation domain has a higher security. The transformation domain is also relatively more resistant to some image manipulation [10] [11]. The steganography method that is widely used in the transformation domain is Wavelet, Cosine, and Fourier [8] [9] [10]. Wavelet transformation is a relatively new transformation compared to Fourier and Cosine transformations. Wavelet transformation also has a better imperceptibility aspect to human vision systems [9] [12]. At present steganography research has been developed and combined with cryptographic techniques to provide stronger protection [12] [13] [14]. Cryptography is

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

a different security technique from steganography, cryptography secures data by encoding data into forms that cannot be understood and even appear to be broken [1] [9] [15]. Some cryptographic techniques that are widely combined with steganography techniques in images are visual cryptography [12] [16], RSA [13], one-time pad (OTP) [5] [8] [17]. OTP is a simple but powerful symmetrical cryptographic technique against various attacks and fast in computing [17] [18]. In some steganography studies using the pseudo number (PN) generator is also applied to the message embedding process, this technique can be used to spread message embedding, it can even improve the imperceptibility and security aspect [8] [13]. In research [9]it has been proposed a combination of strong steganography and cryptography techniques, but this method can still be optimized by combining it with PN sequence techniques which have been proven to improve the aspects of imperceptibility and security [8].

2. Related Work

Research on the combination of steganographic and cryptographic techniques has been developed. As has been done in the research of Najih et al [8]. In the study, a combination of cosine transformations for steganography and OTP methods was proposed to encrypt messages before being embedded. PN generators are also proposed to randomize the embedding process based on binary numbers generated by PN generators. The results are quite satisfying where the PSNR value increases around 3dB as well as its security aspects.

Another study conducted by Setyono et al [9] also proposed OTP cryptography techniques combined with wavelet transformations as steganographic techniques. Wavelet transformation is carried out on four levels, where the first three levels are decomposed in the low subband and the last level is decomposed in the high subband. The results of this method are of good quality where the imperceptibility level reaches 54 dB when measured with PSNR.

Devi and Shivakumar [12] in their research also proposed steganography techniques using wavelet transforms and visual cryptography in images. Huffman coding is also applied to the proposed method to increase the embedded message payload. The reason for choosing wavelet transformation is because of its superiority in the imperceptibility aspect when combined with visual cryptography methods. The results of this method proved to be quite good with a PNSR value of around 35dB with a relatively large message payload.

Yadav and Dutta [13] also proposed a combination of steganography and cryptography techniques using the LSB and RSA methods. The combination of the two methods is used to provide two levels of security in the message. While at the third security level, the PN generator is implemented to spread the location of message embedding. In this way, there are three levels of security in the message.

From several related studies above wavelet transformations appear to be superior compared to other methods in steganography techniques. The OTP cryptographic algorithm is also proven to be powerful for data security. In addition, the PN algorithm has also been proven to improve the security and imperceptibility aspects of steganography techniques. Therefore, this research proposes a combination of wavelet transformations, OTP cryptography and PN generators to optimize the level of security and imperceptibility in stegocrypt techniques.

3. Theory

3.1. Wavelet Transform

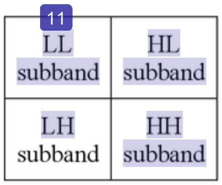

Figure 1. Wavelet Decomposition Results

Wavelet transform works by using low pass filters and high pass filters to divide images into four subband types in the frequency domain [19]. Wavelet transform has advantages when returning an image to a spatial form because this transformation is multi-resolution in accordance with the human vision system [9]. Wavelet transform transforms the image in four subbands namely LL, LH, HL, and HH [20]. In steganography techniques, message embedding is mostly done in LL and HH subband. Embedding in the LL subband to improve message resistance to image manipulation, while the HH subband is used to improve the message imperceptibility. Figure 1 is a result of wavelet transformation.

3.2. One-Time Pad (OTP) and PN Generator

OTP is a cryptographic technique that is widely combined with steganography techniques [5]. This cryptographic technique is a substitution technique with simple computing because it only uses modulo operations [5] [9]. The strength of OTP encryption is on random keys and is only used once [8]. The OTP formula used in this study is (1) for encryption and (2) for decryption.

$$o = (i + k) mod\ x \tag{1}$$

$$i = (o - k) mod\ x \tag{2}$$

Where o is output image of encryption results, i is input image or decrypt image, k is random key, x is range, in this research $x = 256$.

While the generator PN is an algorithm that can generate random binary numbers based on the binary key input. If the PN generator key is not in the form of a binary number, then the key needs to be changed to binary numbers. The random number generated by the PN generator will always be the same if given the same key input [8]. Usually said binary is used to spread messages [13] or it can also be used to modify encryption techniques.

4. Proposed Method

4.1. Embbeding Process

The embedding method proposed in this study requires input in the form of a grayscale image with size m * m as the cover image, a binary image with size n * n as message image, the random key for OTP and binary key for PN generator, the following steps:

- Read the cover image and then do the three DWT transformation levels to get the LL level 3 subband, see Figure 2.
- Transform the LL level 3 subband, then select level 4 HH subband, see Figure 3.

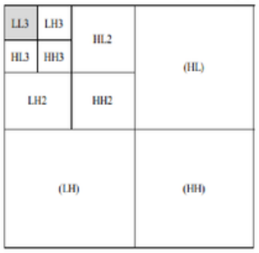

Figure 2. Three level DWT to get subband LL level 3

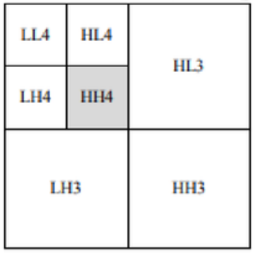

Figure 3. Decomposition results after DWT on subband LL level 3 to get subband HH level 4

- Encrypt the message(m) using the OTP algorithm with a random key using formula (3) if the value $PN_j = 0$ or formula (4) if the value $PN_j = 1$ to produce an encrypted message (e).

$$e_j = (m_j + k_j) mod\ x \tag{3}$$

$$e_j = (m_j - k_j) mod\ x \tag{4}$$

- Generate random binary numbers with PN generators.
- Embed the message with formula (5) if the value $PN_j = 0$ or formula (6) if the value $PN_j = 1$.

$$S_j = C_j - (e_j * \alpha) \tag{5}$$

$$S_j = C_j + (e_j * \alpha) \tag{6}$$

Where S is stego image, C is the cover image, M is message image, α is intensity

- Perform inverse DWT as many as four levels to return the stego image to the spatial domain.

4.2. Extracting Process

In the extraction process requires input consisting of stego image, original cover image, OTP key, and PN generator key, the following steps:

- Perform a DWT transformation of three levels in the LL stego subband image.
- Take LL level 3 subband then do DWT transformation, to get level 4 HH subband, save it on S variable
- Do the two steps above, to the original cover image to get a level 4 HH subband, then save it on the C variable.
- Extract the encrypted message (e) based on the binary number of the generator PN results with formula (7) if the value of $PN_j = 0$ or formula (8) if the value $PN_j = 1$.

$$e_j = (C_j - S_j)\,/\alpha \tag{7}$$

$$e_j = (S_j - C_j)\,/\alpha \tag{8}$$

- Decrypt the results of extraction messages based on the binary number of the generator PN results with formula (9) if the value $PN_j = 0$ or formula (10) if the value $PN_j = 1$ to get the decrypted message (d).

$$d_j = (e_j - k_j) mod\ x \tag{9}$$

$$d_j = (e_j + k_j) mod\ x \tag{10}$$

5. Implementation and Results

In this study used standard cover images such as cameraman, Lena, mandril, and peppers as shown in Figure 4. While the message image used is shown in Figure 5.

cameraman lena mandril peppers

Figure 4. Cover Image Used

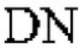

Figure 5. Message Image Used

Furthermore, the embedding process is based on the proposed method, the results of the embedding process are shown in Table 1. The quality of the embedding process results is measured by PSNR and MSE which can be calculated by the formula (11) for MSE and formula (12) for PSNR [21]. Table 1 also shows the quality comparison of the methods proposed in the method [9] and the proposed method, where the same OTP key and PN generator key are used.

Table 1. Experiment Results from Proposed Method Compared with Method in [9] based on PSNR and MSE Value

	Method in [9]		Proposed Method	
Image Name	PSNR (dB)	MSE	PSNR (dB)	MSE
Cameraman	54.0515	0.2558	54.3161	0.2407
Lena	54.0013	0.2588	54.2631	0.2437
Mandrill	54.0178	0.2578	54.3956	0.2363
Peppers	54.1345	0.2510	54.2805	0.2427

$$MSE = \sum_{a=0}^{A-1} \sum_{s=0}^{S-1} \| S_i(a,s) - C_i(a,s) \|^2 \tag{11}$$

$$PSNR_{dB} = 10\, log\, 10 \left(\frac{255^2}{\sqrt{MSE}} \right) \tag{12}$$

Where a and s is the size of the image, S is stego image, C is the cover image.
Based on Table I it appears that the PSNR and MSE values generated from the proposed method are slightly superior compared to the method [9]. Where the generator PN is not used in the study [9] after the PN generator is used the imperceptibility aspect can increase. This proves that the hypothesis discussed above proved true, that using PN generators can improve the imperceptibility and security aspects. In the extraction stage, the message can be extracted perfectly where all messages get the correlation coefficient (cc) value of 1. Where the cc formula is calculated by the formula (13).

$$cc = \frac{\sum_a \sum_s (M_o - \overline{M_o})(M_r - \overline{M_r})}{\sqrt{(\sum_a \sum_s (M_o - \overline{M_o})(\sum_a \sum_s M_r - \overline{M_r})}} \tag{13}$$

Where $M_o$is original message image, M_r is srecover message image

6. Conclusion

Based on the results of the experiment it can be concluded that the proposed method can be successfully implemented. The PN generator is proven to increase imperceptibility quality in the stego image. Based on Table I, the average PSNR value generated by the method [9] is 54.0513dB and the proposed method has an average value of 54.3138dB, so the difference in PSNR value is only about 0.26dB. Although the quality difference is imperceptibility insignificant, it can be concluded that the proposed method can produce a stego image that is better than the previous method. With conditional embedding based on PN values, security also increases because embedding variations are increasing.

References

[1] Sharma, V. K., Srivastava, D. K. & Mathur, P. 2018. Efficient image steganography using graph signal processing, *IET Image Processing*, vol. **12**, no. 6, pp. 1065 - 1071.

[2] Setiadi, D. R. I. M. & Jumanto, J. 2018. An Enhanced LSB-Image Steganography using the Hybrid Canny-Sobel Edge Detection, *Cybernetics and Information Technologies*, vol. **18**, no. 2, pp. 74-88.

[3] Winarno, A., Setiadi, D. R. I. M., Arrasyid, A. A., Sari, C. A. & Rachmawanto, E. H. 2017, *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.

[4] Nasution, A. B., Efendi, S. & Suwilo, S. 2018, *Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB)*, Journal of Physics: Conference Series, vol. 1007.

[5] Sari, W. S., Rachmawanto, E. H., Setiadi, D. R. I. M. & Sari, C. A. 2017, A Good Performance OTP Encryption Image based on DCT-DWT Steganography, *TELKOMNIKA*

Telecommunication, Computing, Electronics and Control, vol. **15**, no. 4, pp. 1987-1995.

[6] Hu, D., Xu, H., Ma, Z., Zheng, S. & Li., B. 2018, A Spatial Image Steganography Method Based on Nonnegative Matrix Factorization, *IEEE Signal Processing Letters*, vol. **25**, no. 9, pp. 1364 - 1368.

[7] Kim, C., Lee, S., Lee, J. & Park, J.-I. 2018, Blind decoding of image steganography using entropy model, *Electronics Letters*, vol. 54, no. 10, pp. 626 - 628.

[8] Najih, M. N. M., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A. & Astuti, S. 2017, *An improved secure image hiding technique using PN-sequence based on DCT-OTP*, in International Conference on Informatics and Computational Sciences (ICICoS), Semarang.

[9] Setyono, A., Setiadi, D. R. I. M. & Muljono. 2017, *StegoCrypt method using wavelet transform and one-time pad for secret image delivery*, in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang.

[10] Yadav, S. K. & Dixit, M. 2017, *An improved image steganography based on 2-DWT-FFT-SVD on YCBCR color space*," in International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli.

[11] Sharma, P. & Sharma, A. 2018, *Robust technique for steganography on Red component using 3-DWT-DCT transform*, in International Conference on Inventive Systems and Control (ICISC), Coimbatore.

[12] M.D, A. D.& Shivakumar, K. B. 2017, *A Novel Image Steganography Technique for Secured Online Transaction Using DWT and Visual Cryptography*," IOP Conference Series: Materials Science and Engineering, vol. 225.

[13] Yadav, P. & Dutta, M. 2017, *3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio*, in International Conference on Image Information Processing (ICIIP), Shimla.

[14] Nipanikar, S. I. & Deepthi, V. H. 2017, *Entropy based cost function for wavelet based medical image steganography*," in International Conference on Intelligent Sustainable Systems, Palladam.

[15] Setyono, A., Setiadi, D. R. I. M. & Muljono, M.. 2018, Dual Encryption Techniques for Secure Image Transmission, *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. **10**, no. 3-2, pp. 41-46.

[16] Maulana, H. & Syahputra, E. R. 2017, *Analysis of Multiple Data Hiding Combined Coloured Visual Cryptography and LSB*," Journal of Physics: Conference Series, vol. 930.

[17] Irawan, C., Setiadi, D. R. I. M., Sari, C. A. & Rachmawanto, E. H. 2017, *Hiding and securing message on edge areas of image using LSB steganography and OTP encryption*, in International Conference on Informatics and Computational Sciences (ICICoS), Semarang.

[18] Suhardi, Suwilo, S. & Nababan, E. B. 2017, "*Use of One Time Pad Algorithm for Bit Plane Security Improvement*," Journal of Physics: Conference Series, vol. 930.

[19] Sudibyo, U., Eranisa, F., Rachmawanto, E. H., Setiadi, D. R. I. M. & Sari, C. A. 2017, *A secure image watermarking using Chinese remainder theorem based on haar wavelet transform*, in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang.

[20] Ardiansyah ,G., Sari, C. A., Setiadi, D. R. I. M. & Rachmawanto, E. H. 2017, *Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm," in International conferences on Information Technology*, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta.

[21] Kusuma, E. J., Indriani, O. R., Sari, C. A., Rachmawanto, E. H & Setiadi, D. R. I. M. 2017, *An Imperceptible LSB image Hiding on Edge Region using DES Encryption*," in International Conference on Innovative and Creative Information Technology (ICITech), Salatiga.

JOP_1

ORIGINALITY REPORT

13%	7%	11%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Strathclyde Student Paper	3%
2	eprints.whiterose.ac.uk Internet Source	3%
3	jtsiskom.undip.ac.id Internet Source	1%
4	Submitted to National Institute of Technology, Silchar Student Paper	1%
5	Muhammad Najih Muhammad Najih, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, Setia Astuti. "An improved secure image hiding technique using PN-sequence based on DCT-OTP", 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), 2017 Publication	1%
6	Nurul Diyah Ayu Partiningsih, Rizki Ramadhan Fratama, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto.	1%

"Handwriting Ownership Recognition using Contrast Enhancement and LBP Feature Extraction based on KNN", 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 2018
Publication

---

7 Anuj Rani, Manoj Kumar, Payel Goel. "Chapter 15 Image Modelling: A Feature Detection Approach for Steganalysis", Springer Nature, 2017
Publication
1%

---

8 Submitted to University of Liverpool
Student Paper
<1%

---

9 Submitted to Universitas Jember
Student Paper
<1%

---

10 Sahib Khan, Arslan Arif, Syed Tahir Hussain Rizvi, Nasir Ahmad. "Increasing Distance Increasing Bits Substitution (IDIBS) Algorithm for Implementation of VTVB Steganography", Computer Modeling in Engineering & Sciences, 2018
Publication
<1%

---

11 Yen-Yu Chen, Shen-Chuan Ti. "Embedded medical image compression using DCT based subband decomposition and modified SPIHT data organization", Proceedings. Fourth IEEE
<1%

Symposium on Bioinformatics and Bioengineering, 2004
Publication

12 Yudit Arum Mekarsari, De Rosal Ignatius Moses Setiadi, Christy Atika Sari, Eko Hari Rachmawanto, Muljono. "Non-blind RGB image watermarking technique using 2-level discrete wavelet transform and singular value decomposition", 2018 International Conference on Information and Communications Technology (ICOIACT), 2018 <1%
Publication

13 Eko Hari Rachmawanto, Rofi' Syaiful Amin, De Rosal Ignatius Moses Setiadi, Christy Atika Sari. "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size", 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), 2017 <1%
Publication

14 Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, Brendan Halloran. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", Neurocomputing, 2019 <1%
Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		