TELKOMNIKA, Vol.15, No.4, December 2017, pp. 1982~1989
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v15i4.5883

A Good Performance OTP Encryption Image based on DCT-DWT Steganography

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

Abstract

The security aspect is very important in data transmission. One way to secure data is with steganography and cryptography. Surely research on this should continue to be developed to improve security. In this paper, we proposed a combination of steganographic and cryptographic algorithms for double protection during data transmission. The selected steganographic algorithm is the use of a combination of DCT and DWT domain transformations. Because the Imperceptibility aspect is a very important aspect of steganographic techniques, this aspect needs to be greatly improved. In the proposed method of DCT transformation first, proceed with DWT transformation. From the experimental results obtained better imperceptibility quality, compared with existing methods. To add OTP message security applied algorithm to encrypt the message image, before it is inserted. This is evidenced by experiments conducted on 20 grayscale images measuring 512x512 with performance tests using MSE, PSNR, and NC. Experimental results prove that DCT-DWT-OTP generates PNSR more than 50 dB, and NC of all images is 1.

Keywords*: image steganography, image cryptography, one time pad, DWT, DCT*

Copyright © 2017 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

In the last few decades, there are several branches of science that can be used to secure secret communications such as cryptography, watermarking, and steganography. Delivery of data through public media such as the internet is possible the occurrence of theft and data manipulation. Therefore, this Science must be developed in view of the need for security is very necessary. Steganography and Watermarking have in common that hide secret messages into the cover file [1]. The difference is the purpose, where watermarking serves to protect the copyright while steganography serves to hide the message. Usually, the message can not be detected by the human senses so it is difficult to distinguish between the original data with other data that already contains the message [2]. While cryptography serves to change the form percent to form an irregular or seem to look damaged [3].

In steganography, there are two kinds of domains that are often used, namely domain and spatial domain transformation [4-5]. Domain transformation has the advantage of spreading messages across the entire file cover. While spatial domains excel in simpler operations. DCT and DWT are the most popular transformations in steganographic transformation domains [6-8]. DCT has advantages in compact energy and computing relatively faster than DWT [6], whereas DWT is an algorithm with low bit error rate and resistance to distortion [9]. Another advantage is that DCT is used as the standard transformation of JPEG and DWT as the standard transformation of JPEG 2000 [10]. In other studies [11-14] evidenced by the merging of these two transformations in a steganographic scheme can be further optimized.

Many such studies on [14-18], combine steganographic techniques with cryptography to enhance the security of secret messages. There are many popular cryptographic techniques such as Blowfish, DES, RSA, AES, and One Time Pad (OTP) [18-20]. OTP is the method that is processed per block and simplest compared to other methods. Another difficult algorithm to solve [20-21] and makes it possible to be used on image media as has been done by previous studies of image cryptography. The main contribution of this research is to formulate the best

Received Mar 5, 2017; Revised September 18, 2017; Accepted September 30, 2017

combination of DCT and DWT to improve the imperceptibility aspect, while also adding OTP encryption to encrypt the message before it is embedded in the cover file so that double protection on the message is sent.

2. Research Method

2.1. Data Gathering

In this experiment, we used 20 standard grayscale image data with the .jpg format with 512x512 size coming from source [22], while the secret message image is a 32x32 pixel binary image as shown in Figure 1. The experiment was tested executed with the Matlab tool. Here is an image used to experiment.

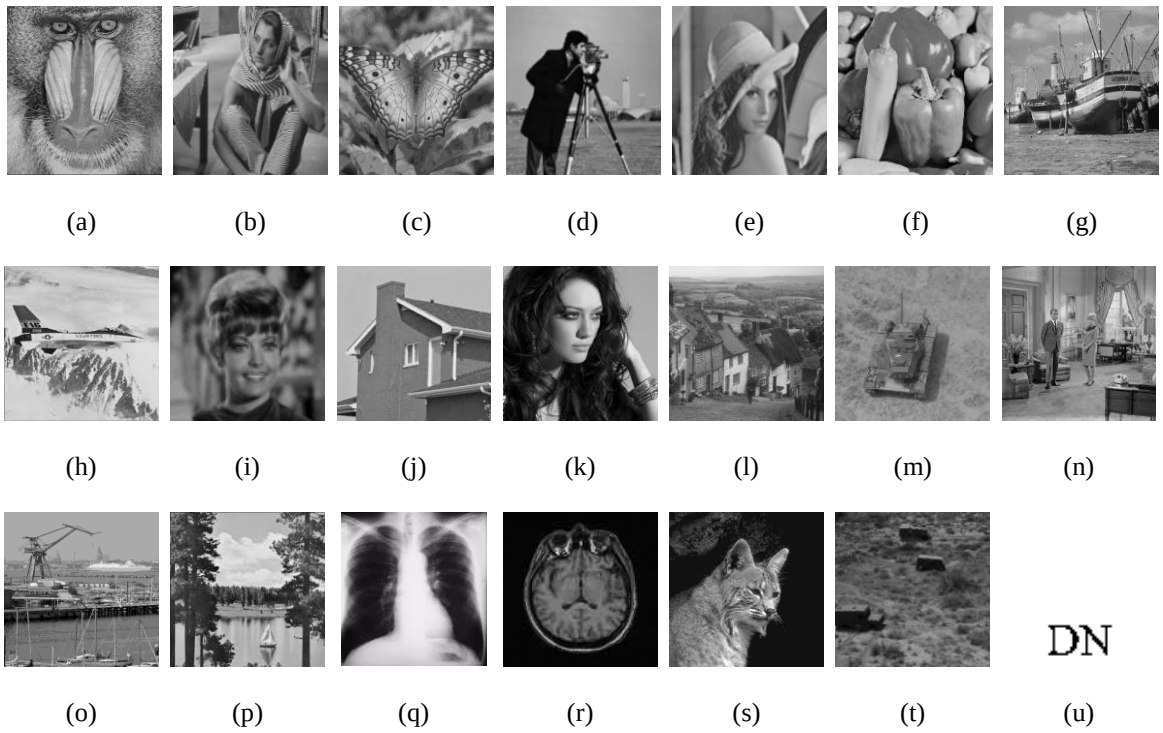

Figure 1. Images Database: (a) babbon.jpg, (b) barbara.bmp, (c) butterfly.png, (d) cameraman.jpg, (e) lena.bmp, (f) peppers.tiff, (g) fishingboat.jpg, (h) f16.jpg, (i) zelda.gif , (j) house.jpg, (k) girlface.jpg, (l) goldhill.jpg, (m) tank.tiff, (n) couple.jpg, (o) kiel.gif, (p) view.jpg, (q) lung.jpg, (r) brain.jpg, (s) cat.jpg, (t) trucks.tiff, (u) message.bmp

2.2. Theoretical Basis

2.2.1. One Time Pad (OTP)

OTP is a popular algorithm that is often used through cryptographic techniques. OTP belongs to a group of symmetric cryptographic algorithms where one key is used for encryption and decryption [20]. The algorithm used in OTP is very simple that is by using XOR operation or can also use modulo (mod). Although very simple, OTP has the advantage that is very difficult to solve because it has a key that is only once used and has the same length as the message to be encoded [23]. This algorithm will also be very difficult to describe because the attacker should try every possible key when decrypting and it is very difficult to guess the original plaintext. The equation of OTP encryption can be seen on Equation 1, whereas OTP decryption can be seen on Equation 2.

$$Ci = (Pi + ki)\ mod\ z \quad (1)$$

$$Pi = (Ci - ki)\ mod\ z \quad (2)$$

Where,
Ci = Cipherteks,
Pi = Plaintext,
ki = Random key,
z = the number of possible characters

2.2.2. Discrete Cosine Transform (DCT)

DCT is the transform is resistant to attack lossless image compression [11] and working to change the function of the spatial domain into the frequency domain [10]. DCT transforms the input signal into two kinds of coefficients ie direct current (DC) and alternating current (AC) [24]. The DC coefficient is a representation of approximation and illumination and contains the image core information [10]. While the AC coefficients consist of three frequencies, namely: high frequency, low frequency, and medium frequency. Message insertion can be done on all coefficients, it's just insertion in the DC part has advantages that are more robust but the quality of stego image is maintained [7]. Figure 2 is an illustration of the AC and DC coefficients in the input image of size 8x8.

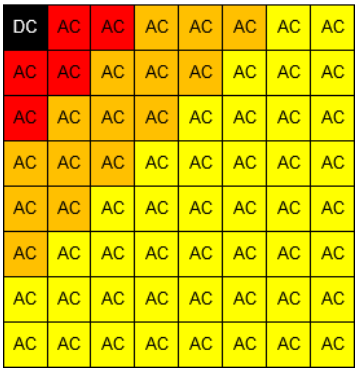

Figure 2. Mapping of Coefficients and Frequencies at DCT

DCT is a transformation that is often used in compression, steganography, and watermarking techniques. DCT is operated using base and column of the image (MxN). DCT operations on images, in general, can be translated through Equation 3 and Equation 4 for inverse DCT operation.

$$H(f,g) = a(f)a(g)\sum_{o=0}^{M-1}\sum_{p=0}^{N-1} s(o,p)\ cos\frac{(2o+1)f\pi}{2M} cos\frac{(2p+1)g\pi}{2N} \quad (3)$$

$$s(o,p) = 1/o = \frac{2}{\sqrt{M.N}}a(f)a(g)\sum_{o=0}^{M-1}\sum_{p=0}^{N-1} H(f,g)\ cos\frac{(2o+1)f\pi}{2M} cos\frac{(2p+1)g\pi}{2N} \quad (4)$$

Where,
f is $0,1,2,\dots,M-1$ with signal length M = 8
g is $0,1,2,\dots,N-1$ with signal length N = 8
N and M is signal length

2.2.3. Discrete Wavelet Transform (DWT)

DWT is a transform domain that uses an operating model based on subband LL, LH, HL, and HH as shown in Figure 3 [24]. The four subband is obtained by using two kinds of filters, namely low pass filter and high pass filter. The use of this filter is done through rows

(vertical) and column (horizontal) on the image. Subband LL contains low frequency, while subband HH contains high frequency. Subband LH and HL are medium frequencies, the difference is HL obtained from low frequency using high pass filter vertically, whereas LH is obtained from high frequency using low pass filter vertically [15] [25]. In steganography theory, each subband has advantages and disadvantages to insert messages. Message insertion on subband LL can improve robustness but reduce imperceptibility, subband HH otherwise, whereas HL and LH tend to be more neutral [26]. However, some studies suggest that insertion in LL subband is still quite good in the imperceptibility aspect [6].

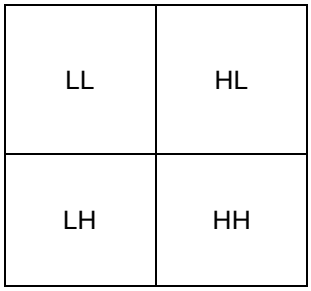

Figure 3. Wavelet Subbands

2.3. The Proposed Method

Based on the above literature it is proposed a combination of DCT-DWT method and OTP encryption to improve message security. In this paper, there are two main processes, namely the process of embedding and extracting. Where in each process, DCT transform is done first, then proceed with DWT transformation. The message image is encrypted with the OTP method before it is inserted in the cover image. For more details see Figure 4 and Figure 5.

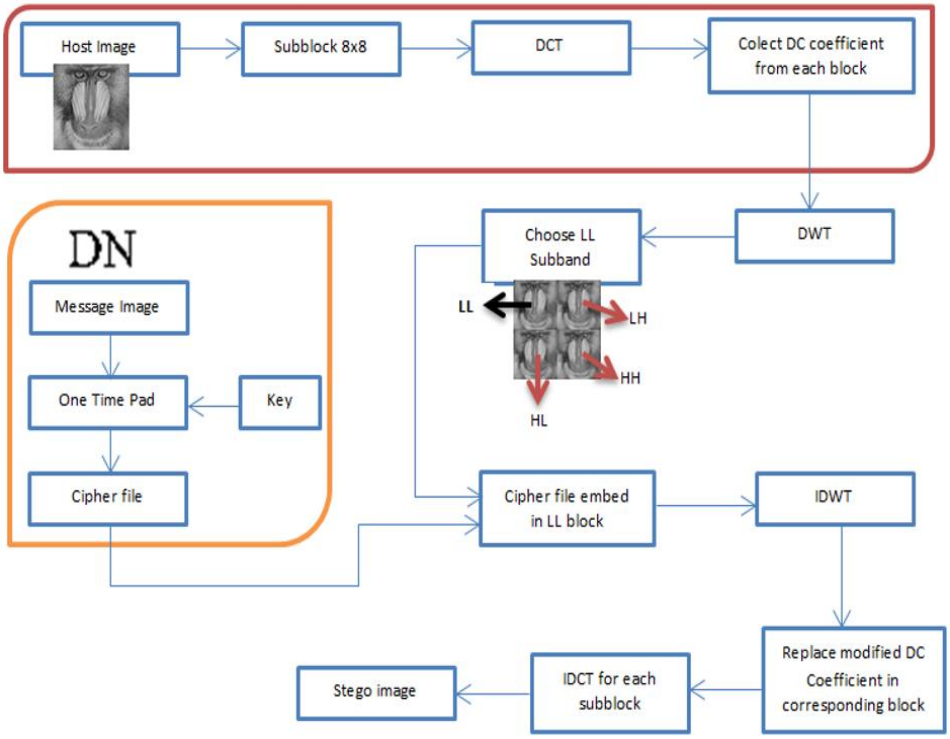

Figure 4. Embedding Scheme using DCT-DWT-OTP

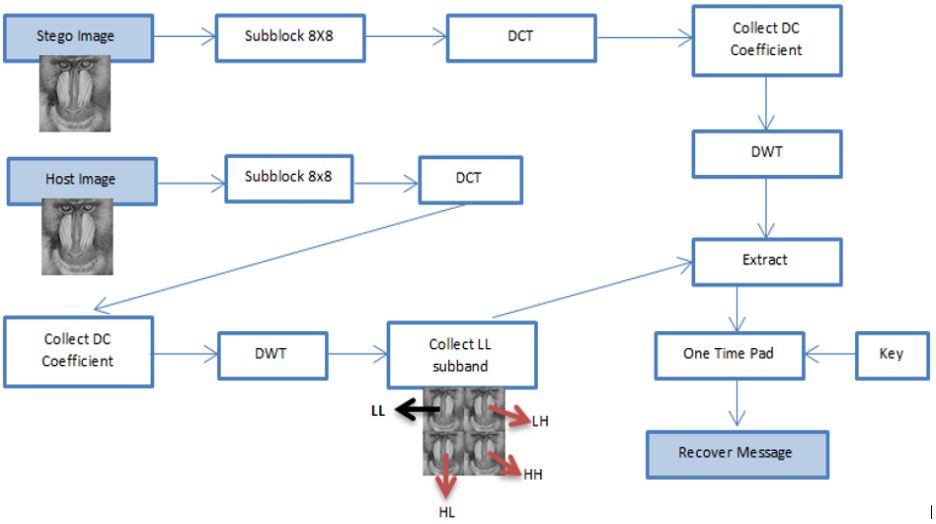

Figure 5. Extraction Scheme using DCT-DWT-OTP

2.3.1 Embedding Scheme

The embedding process that will be done in this research can be translated into:

1. Select a 512x512 pixel image host then split into 8x8 sized sub-blocks.
2. The sub-blocks are then transformed by DCT and collect the DC coefficients on every sub-block.
3. The DC coefficients of every sub-block are then aggregated into one in the reference image(CR_i).
4. Then transform the Reference image DWT and grab subband LL, resulting in transform image(CR_{ll}).
5. On the other hand, pass encryption to the image image image with the OTP algorithm and the secret key generated from the rand function using Eq.1, thus forming the cipher image(c_i).
6. Embed the cipher image(c_i) on LL subband reference image(CR_{ll}), with Eq. 5, thus generating mofidied LL subband reference image(MR_{ll}).

$$MR_{ll} = CR_{ll} + (c_i * \beta) \quad (5)$$

Where β is embedding factor .

7. Next, do the inverse DWT (IDWT) process on the transformed image to get modified reference image. Thus replace the DC coefficients on every sub block.
8. Finally, do IDCT for each subblock, this process got stego image.

2.3.2 Extracting Scheme

The following is a stego image extracting process in Figure 5:

1. Stego image is divided into 8x8 subblock and processed using DCT.
2. Collect the DC coefficients on each subblock to reference the image.
3. Continue with DWT on the reference image and select LL subband.
4. Do the same on the host image starting from point 1 to point 3.
5. Extract by comparing the LL subband on the stego image and host image, using Equation

$$rc_i = (HR_{ll} - SR_{ll})/\beta \quad (6)$$

Where,rc_i is recover chipper file, HR_{ll} is LL subband of host reference image, SR_{ll} is LL subband of stego refecence image

6. The extraction results are then processed with OTP using Equation 2 so it will generate decryption of recovery message

3. Results and Analysis

To find out the proposed algorithm's performance, the embedding process will be measured with PSNR and MSE, while the extraction results will also be measured by NC.

$$MSE = \frac{1}{MxN}\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}[\{x(p,q) - y(p,q)\}^2] \quad (7)$$

Equation 7 is an equation for computing MSE, where M and N are rows and columns of pixels in the image. MSE is a quadratic function used to measure the difference between a host image and a stego image. Where the smaller the value of MSE, the quality of the more closely resembles the cover image. The good value of PSNR in the realm of steganography is at least 40 dB [27]. The equation for calculating PSNR as shown in Equation 9.

$$PSNR = 10\ log_{10}\left(\frac{MxN}{MSE}\right) \quad (8)$$

From Equation 8 above, it is known that PSNR is calculated by using the inverse operation of the exponent in a natural logarithm based on 10 and multiplied by M, N which is the row and column of the measured image. While the formula of NC can be elaborated through Equation 7.

$$NC = \frac{\sum_{i,j=0}^{N-1}\big(H(p,q)S(p,q)\big)}{\sum_{i.j=0}^{N-1}\big(H(p.q)\big)^2} \quad (9)$$

Based on Equation 9, N is the image size to be measured, $H(p,q)$ is the pixel value of the original image, while $S(p,q)$is the pixel value of the stego image. If the value of NC close to one, then the image of extraction is also increasingly identical with the original message image. Table 1 shows the results of the experiment to show DCT-DWT-OTP performance.

Table 1. Embedding and Extraction Results using DCT-DWT-OTP (in PSNR, MSE, and NC)

Cover Image	MSE	PSNR	NC without attack
Baboon	0.4980	51.3053	1.0000
Barbara	0.4863	51.2615	1.0000
Buterfly	0.4990	51.2615	1.0000
Cameraman	0.5117	51.1496	1.0000
Lena	0.4961	51.1752	1.0000
Peppers	0.4834	51.2878	1.0000
Fishingboat	0.5156	51.1754	1.0000
F16	0.4961	51.1923	1.0000
Zelda	0.4971	51.2878	1.0000
House	0.5176	51.3853	1.0000
Girlface	0.4853	51.2704	1.0000
Goldhill	0.5137	51.1752	1.0000
Tank	0.4971	51.1666	1.0000
Couple	0.5176	50.9910	1.0000
Kiel	0.4853	51.2705	1.0000
View	0.4990	51.1497	1.0000
Lung	0.5010	51.1326	1.0000
Brain	0.5107	51.0488	1.0000
Cat	0.4873	51.2529	1.0000
Trucks	0.5156	51.0075	1.0000

From Table 1 above it can be seen that all images during embedding process produce PSNR more than 50 dB and the highest PSNR value is 51.3853 dB. Thus it can be concluded that this algorithm is stable when applied to various types of images. As for the MSE in all images also did not reach 0.52. For extraction result, all image got value 1, where this value indicates there is no difference between original message image with the image of extraction message. This result is a perfect extraction result.

In this study also performed comparisons with studies conducted by [13], [14], and [24]. In the study [13] and [14] used a combination of DCT and DWT transformations, while in the study [24] only used DCT transformation. Fig. 6 is a chart that presents a comparison of PSNR scores of the three previous methods and the method proposed in this study.

Based on Figure 6 it can be seen that the score of PSNR in the proposed method in this study is superior to the previous study. Research conducted by [13] and [14] both use two transformations ie DWT and DCT. In the study [14] additionally Arnold's transformation to improve the security of the message image. Both of these studies performed DWT transformation first, then continued with DCT transformation. While in this study DCT transformation done first, then transformed by DWT.

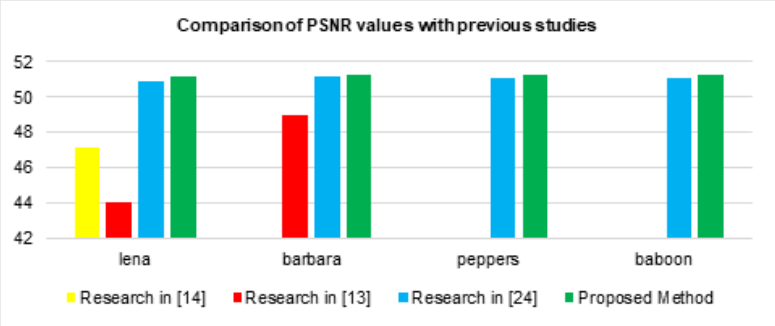

Figure 6. Comparison of PSNR Values with Previous Studies

4. Conclusion

In this study, DCT-DWT steganography was combined with OTP cryptography on the image media. Of the 20 512x512 pixel grayscale-formatted images tested in this paper, all of the images all receive a PSNR value of more than 40 dB, which means that the quality of imperceptibility meets the human visual system aspect. The lowest PSNR is 50.9910 dB and the highest is 51.3053 dB. Performance tests were also assessed using MSE and NC. Each managed to get an MSE value between 0.4 to 0.5, while the NC value of all images is 1. This value indicates that the message can be extracted well and has 100% similarity with the original message image. Selection of DCT coefficients, subband DWT and embedding factor value greatly affect the quality of imperceptibility. In this study, DC coefficients of DCT transform and LL subband on DWT transformation were chosen as the place of embedding of message image. Based on the results comparable with the studies [13], [14], and [24], the proposed method suggests that the PSNR score is higher than the previous three studies.

References

[1] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt. Digital image steganography: Survey and analysis of current methods. *Signal Processing.* 2010; 90(3); 727-752.

[2] K. Joshi and R. Yadav. *A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication*. in International Conference on Image Information Processing (ICIIP), Waknaghat, 2015.

[3] P. V. Nadiya and B. M. Imran. *Image Steganography in DWT Domain using Double-Stegging with RSA Encryption*. in International Conference on Signal Processing Image Processing & Pattern Recognition (ICSIPR), Coimbatore, 2013.

[4] H. E. Suryavanshi, A. Mishra and S. Kumar. Digital Image Watermarking in Wavelet Domain. *International Journal of Electrical and Computer Engineering (IJECE).* 2013; 3(1): 1-6.

[5] V. Kumar and D. Kumar. *Performance Evaluation of DWT Based Image Steganography*. in International Advance Computing Conference (IACC), Patiala, 2010.

[6] 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.

[7] 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.

[8] 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.

[9] P. Bedi, V. Bhasin, and T. Yadav. *2L-DWTS — Steganography technique based on second level DWT.* in International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Jaipur, 2016.

[10] J. Li and Q. C.. DSDWA: A DCT-based Spatial Domain Digital Watermarking Algorithm. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2014; 12(1): 693-702.

[11] M. A. Faizal, H. B. Rahmalan, E. H. Rachmawanto and C. A. Sari. Impact Analysis for Securing Image Data Using Hybrid SLT and DCT. *International Journal of Future Computer and Communication.* 2012; 1(3): 308-311.

[12] A. Goswami and S. Khandelwa. Hybrid DCT-DWT Digital Image Steganography. *International Journal of Advanced Research in Computer and Communication Engineering,* 2016; 5(6): 228-233.

[13] A. Goswami and S. Khandelwal. Coloured and Gray Scale Image Steganography using Block Level DWT DCT Transformation. *International Journal of Computer Applications.* 2016; 148(7): 1-3.

[14] A. Nambutdee and S. Airphaiboon. *Medical Image Encryption Based on DCT-DWT Domain Combining 2D-DataMatrix Barcode.* in Biomedical Engineering International Conference (BMEiCON), Pattaya, 2015.

[15] M. R. Pour Arian and A. Hanani. Blind Steganography in Color Images by Double Wavelet Transform and Improved Arnold Transform. *Indonesian Journal of Electrical Engineering and Computer Science.* 2016; 3(3): 586-600.

[16] P. G. Jose, S. Chatterjee, M. Patodia, S. Kabra and A. Nath. Hash and Salt based Steganographic Approach with Modified LSB Encoding. *International Journal of Innovative Research in Computer and Communication Engineering.* 2016; 4(6): 10599-10610.

[17] 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.

[18] P. Patel and Y. Patel. *Secure and Authentic DCT Image Steganography through DWT - SVD Based Digital Watermarking with RSA Encryption*. in International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, 2015.

[19] J. Thakur and N. Kuma. DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering.* 2011; 1(2): 6-12.

[20] N. Nagaraj and P. G. Vaidya. One-Time Pad, Arithmetic Coding and Logic Gates: An unifying theme using Dynamical Systems. arXiv.org, New York, 2008.

[21] O. Tornea, M. E. Borda, V. Pileczki and R. Malutan. *DNA Vernam cipher*. in E-Health and Bioengineering Conference (EHB), Iasi, 2011.

[22] F. Petitcolas. The Information Hiding Homepage. 1997. [Online]. Available: http://www.petitcolas.net/watermarking/image_database/. [Accessed 2 2017].

[23] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman and G. Varadan. *Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem*. in International Conference on Machine Intelligence and Research Advancement (ICMIRA), Katra, 2013.

[24] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *Journal of Applied Intelligent System.* 2017; 2(1): 1-11.

[25] H. Gao, L. Jia, and M. Liu. A Digital Watermarking Algorithm for Color Image Based on DWT. *TELKOMNIKA.* 2013; 11 (6) 3271-3278.

[26] K. Yun. In the Network Communication an Improved Algorithm of Image Watermarking based on DWT. *TELKOMNIKA.* 2013; 11(11): 6304-6308.

[27] P. S. Addison. A Review of Wavelet Transform Time–Frequency Methods for NIRS-Based Analysis of Cerebral Autoregulation. *IEEE Reviews in Biomedical Engineering.* 2015; 8: 78 - 85.

[28] B. Li, J. He, J. Huang, and Y. Q. Shi. A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing.* 2011; 2(2): 142-172.