Imperceptible and secure image watermarking using DCT and random spread technique

Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi*, Christy Atika Sari, Nova Rijati
Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia
*Corresponding author, e-mail: moses@dsn.dinus.ac.id

Abstract

Watermarking is a copyright protection technique, while cryptography is a message encoding technique. Imperceptibility, robustness, and safety are aspects that are often investigated in watermarking. Cryptography can be implemented to increase watermark security. Beaufort cipher is the algorithm proposed in this research to encrypt watermark. The new idea proposed in this research is the utilization of Beaufort key for watermark encryption process as well as for spread watermark when inserted as PN Sequence substitute with the aim to improve imperceptibility and security aspects. Where PN Sequence is widely used in spread spectrum watermarking technique. Based on the experimental results and testing of the proposed method proved that imperceptibility and watermark security are increased. Improved imperceptibility measured by PSNR rose by about 5dB and so did the MSE score better. Robustness aspect is also maintained which has been proven by the excellent value of NCC.

Keywords*: beaufort cipher, copyright protection, DCT, random, spread spectrum*

1. Introduction

Watermarking is a technique for protecting the copyrights from irresponsible parties [1]. Watermarking is a technique similar to steganography because these two techniques both hide data [2]. Watermarking can be done in various digital media such as audio, image, and video. The rapid and sophisticated technological developments demand that embedded watermarks can enhance three aspects i.e. robust, secure, and imperceptible [3, 4]. So research on watermarking is still being developed to improve these aspects.

Watermarking techniques, especially in digital images can be done with two kinds of domains, the spatial domain and frequency domain [3]. Spatial domains can be done by the LSB and Zero Distortion Technique (ZDT) methods [5], but they are weak against various image manipulations. Frequency domains with the use of transformations are considered more robust to various manipulating digital images [1-6]. Transformation domains such as Discrete Cosine Transform (DCT), is a very popular transformation used in watermarking techniques [7, 8].

DCT has been widely applied in many image watermarking studies because DCT has many advantages over other transformations. Some of the advantages of DCT are a relatively fast calculation, good energy compactness, and has been embedded on various hardware such as cameras. DCT is also used in JPEG and MPEG compression standards [2-9] . While JPEG is a very popular extension and widely used for image storage. Some DCT research on image watermarking has also proven that is a robust transformation against various image manipulations [7, 8].

The imperceptibility aspect can also be enhanced, some studies combine with several other transformations such as wavelet transform or singular value decomposition or both [3-10]. However, the combination of some domain transformations does make the calculation code more complex and higher coding complexity. Other technique such as PN sequences can also improve aspects of imperceptibility [11], this technique is widely implemented in spread spectrum technique, and with this technique can improve watermark security automatically [12]. PN Sequence is used to embed a watermark with a specific pattern of distribution [13]. This makes better imperceptibility and security aspects than without used PN sequence [14, 15].

In an effort to improve the security of watermarks, image watermarking techniques are also combined with many cryptographic techniques [8]. The popular cryptography used in

Received March 11, 2018; Revised March 14, 2019; Accepted April 17, 2019

the watermark image is the chaotic map [7, 8, 10, 16, 17]. There are various chaotic map methods, such as Arnold map, Logistic map, Kent map, and others. This method is an image scramble technique with a certain iteration so the image looks random, but the pixel value contained in the image does not change. Other cryptographic methods that are also widely applied to the watermark image is a one-time pad (OTP) [2, 3, 11, 18, 19]. With this method, the image information can be completely random and different from the original image. Commonly, OTP is a derivative of the Vigenere algorithm that can use XOR or modulo functions to perform image encryption. This method is a classical cryptographic method that in its development has several types of algorithms such as Vigenere and Beaufort. Vigenere's algorithm is becoming more popular, but in Alallayah's et. al research [20], it has been proven that Beaufort performs better than Vigenere. So, in this study we combine DCT, Beaufort cipher, to improve safety and robustness, Beaufort key that is generated with random function is also used as a substitute of PN sequence to improve imperceptibility.

2. Research Method

2.1. Discrete Cosine Transform (DCT)

DCT is a very popular transformation and widely applied in the various science of digital image processing. DCT is also used as a popular JPEG standard compression transformation. Some of the advantages of DCT are its ability to rapidly transform pixel values [3], has a good energy compactness [2], has a low-grade error rate and high compression ratio [21] DCT is also widely implemented in software and hardware of image processing. This makes the use of DCT in image watermarking has many advantages. There are two kinds of coefficients produced DCT, namely Direct Current (DC) and Alternating Current (AC). DC is the coefficient that contains the main information of the transformation, while the AC is a coefficient containing additional information [2]. The coefficient of AC is divided into three kinds of frequencies, namely low, mid and high.

Embedding and spreading watermarks on DCT well and able to withstand attacks. The insertion technique and the selection of embedment coefficients also greatly determine the quality of imperceptibility and robustness. Message insertion on DC coefficient and low-frequency coefficient AC can improve the quality of robustness because the energy is concentrated in this passage [9]. In matrix 8*8 forward DCT can be defined as follows [3].

$$T_{mn} = \alpha_m \beta_n \sum_{p=0}^{P-1} \sum_{q=0}^{Q-1} S_{pq} cos \frac{\pi(2p+1)m}{2P} cos \frac{\pi(2q+1)n}{2Q} \tag{1}$$

where, S is a spatial matrix, T is a transform matrix, m= 0, 1, 2, ..., P-1, n= 0,1,2,..., Q-1, and

$$\alpha_m = \begin{cases} \frac{1}{\sqrt{P}}, m = 0 \\ \sqrt{\frac{2}{P}}, m > 0 \end{cases} \quad \beta_n = \begin{cases} \frac{1}{\sqrt{Q}}, n = 0 \\ \sqrt{\frac{2}{Q}}, n > 0 \end{cases} \tag{2}$$

as for the DCT inverse is defined by (3).

$$S_{pq} = \sum_{p=0}^{P-1} \sum_{q=0}^{Q-1} \alpha_m \beta_n \, T_{mn} cos \frac{\pi(2p+1)m}{2P} cos \frac{\pi(2q+1)n}{2Q} \tag{3}$$

2.2. Beaufort Cipher

Beaufort cipher is another form of Vigenere cipher that has been widely implemented in one-time encryption pad (OTP). OTP is cryptography can be used for text and image. Vigenere is one of the most popular substitution cipher [2-22]. While the Beaufort cipher uses a substitution technique similar to Vigenere [20]. Encryption using Beaufort cipher in the image is defined by formula (4).

$$E_{xy} = (K_{xy} - M_{xy}) mod \, V \tag{4}$$

Where E is encrypted message, K is the key generated by the random function, M is the message, V is maxed value of the pixel, and xy is coordinate of the pixel. As for the decryption is defined by the formula (5).

$$M_{xy} = (K_{xy} - E_{xy}) mod\ V \tag{5}$$

In order to ensure the safety of the Beaufort cipher algorithm, the keys used must be random, once used and the size is the same as the plain message [2]. In this study, the random key will also be used as a substitute of PN Sequence to insert a watermark. Utilization of the random key is used to improve the imperceptibility of watermark [11].

2.3. Image Watermarking

Image watermarking is a copyright insertion technique into an image in order to protect the copyright. There are two main processes in image watermarking, namely the insertion process and the encryption process. Both processes are performed in the frequency domain. The study proposes DCT to transform images into frequency domains, to improve safety, Beaufort ciphers are proposed for watermark encryption. The random function is used to generate Beaufort key as well as utilized in the insertion and extraction process to improve the watermark imperceptibility aspect. While the tools used in this research is Matlab R2015 For more details can be seen in the following sub-chapters.

2.3.1. Proposed Embedding Method

In the embedding process required three inputs, namely a cover image, watermark image and Beaufort key. Figure 1 can be observed to decrypt watermark insertion steps more clearly.

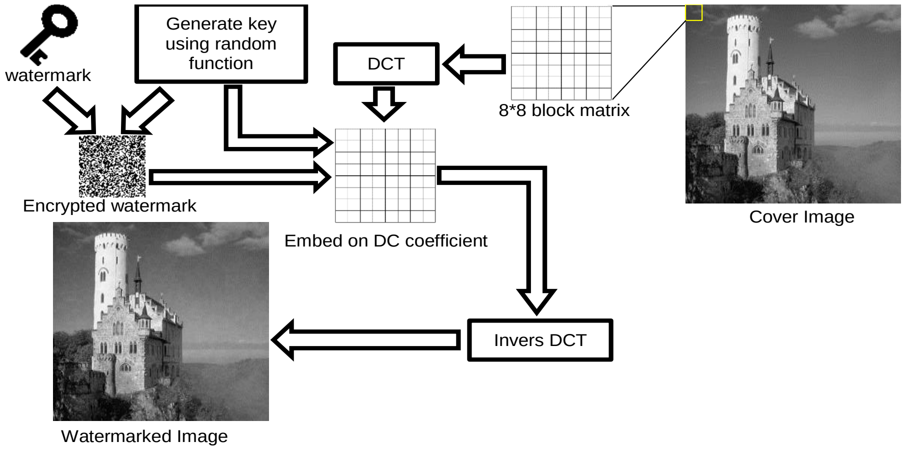


Figure 1. Proposed embedding method

Here are the details of the steps:

a. Read watermark image (wi), using the imread function.
b. Create Beaufort key (Bk) using random function, where Beaufort key is binary image.
c. Perform watermark encryption (ew) using Beaufort key.
d. Read cover image using the imread function.
e. Split the image into matrix blocks of 8*8 pixels
f. Perform transformations on matrix blocks using DCT.
g. Insert encrypted watermark with Beaufort cipher on DC coefficient using factor value (z). The insertion is done by the Beaufort key (Bk) using (6). The value will affect the aspects of imperceptibility and robustness.

$$DCw\begin{cases}DC + (ew_{xy} * z), Bk = 0\\ DC + (ew_{xy} * z), Bk = 1\end{cases} \quad (6)$$

h. Perform inverse DCT on each block that has been inserted a watermark.
i. Combine all DCT inverse blocks into one to get the watermarked image.

2.3.2. Proposed Extraction Method

This stage is part of doing watermark extraction from the watermarked image. The proposed method is a non-blind method. This method requires a cover image for the extraction process. So at this stage, it takes the watermark image, the original cover image, and the Beaufort key, to gain a clearer understanding of the steps can see the decryption of the extraction step in Figure 2.

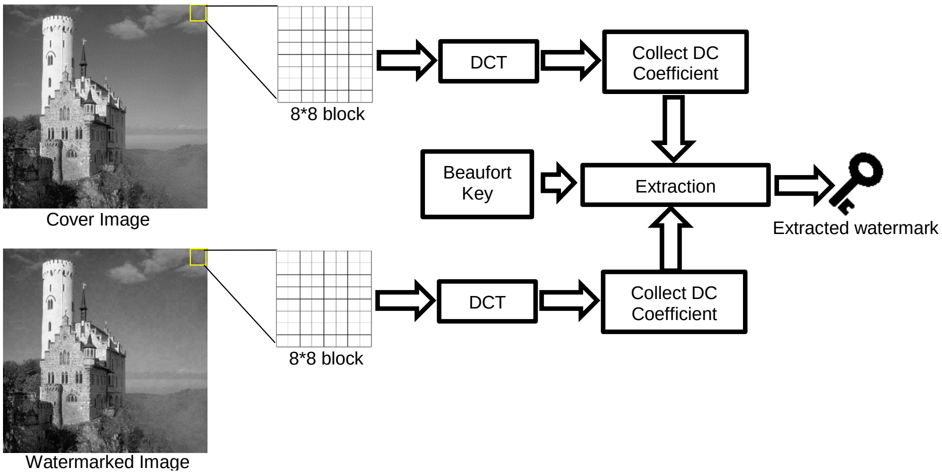


Figure 2. Proposed extraction method

Here is a detailed step of the extraction process:
- Read the watermarked image with the imread function, then break the image within matrix blocks of size 8*8.
- Perform DCT on each matrix block, then collect DC coefficients in a matrix(DCw).
- Perform step 1 and 2 on the original cover image.
- Extract the watermark image with the formula (7) based on the Beaufort key (Bk).
- Get the watermark image extraction (We).

$$We\begin{cases}(DCc_{xy} - DCw_{xy})/z, Bk = 0\\ (DCw_{xy} - DCc_{xy})/z, Bk = 1\end{cases} \quad (7)$$

Where DCc is a DC matrix of the original cover image whereas DCw DC matrix is a watermarked image.

2.4. Measurement Tools

This study uses several measuring tools to determine the quality of watermarking. The quality of the watermarking algorithm is measured in two aspects, namely imperceptibility and robustness. The imperceptibility of the watermarked image can be measured by means such as mean square error (MSE), and peak signal to noise ratio (PSNR). MSE and PSNR are commonly used measuring tools for measuring image quality. MSE is an estimate of the mean value of the squared error of reconstruction of the cover image after the watermark inserted. Increasing MSE values indicate that more errors, while the MSE value near 0 indicates better image quality. PSNR is the value of the ratio of the noise value that can damage the image representation with the maximum value of the signal strength of an image. In contrast to MSE the better the PSNR value is the greater value, the perfect PSNR value is infinity. The MSE and PNSR formulas are respectively shown in (8), and (9) [23].

$$MSE = \sum_{x=1}^{X-1} \sum_{y=1}^{Y-1} \|A(x,y) - B(x,y)\| \quad (8)$$

$$PSNR = 10log_{10}\left(\frac{(2^8)-1}{MSE}\right) \quad (9)$$

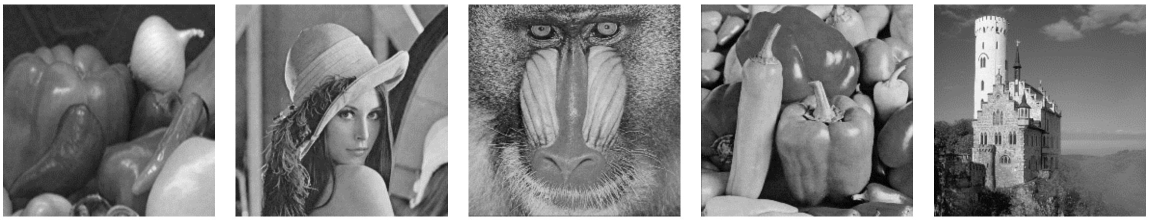
Where A is a cover image, B is a watermarked image, X is number of row, Y is number of coloumn. In this study, the quality of robustness is measured by normalized cross-correlation (NCC). The NCC value is generated from the comparison between the original message image and the image of the extracted message. Perfect message extraction will result in NCC value 1. NCC value ranges from 0 to 1, that's mean if the value of NCC close to 0 then the quality of extraction is getting worse [24]. Watermarks should be resistant to various image manipulations. To test the watermark resistance in this study the watermarked image will be tested with JPEG, mid filter, crop, scaling, Gaussian noise, and salt and pepper attacks. The NCC can be calculated by the formula (10).

$$ncc = \frac{M \times M\prime}{M \times M} \quad (11)$$

This study also measured the computational performance of the proposed algorithm using tic toc function in Matlab to find out the time required to perform the watermarking process.

3. Results and Analysis

The image dataset used in this research are grayscale images with size 512*512 which can be downloaded at http://sipi.usc.edu/database/ [25]. While the watermark used is a black and white image with size 64*64. Figure 3 shows the cover image used, while figure 4 is a watermark image. Before the process of embedding, encryption is imposed on the watermark image watermark to improve security. Watermark image encryption is performed with the Beaufort algorithm. Figure 5 shows the Beaufort key used and the watermark encryption results.



Onion.bmp Lena.bmp Mandrill.bmp Peppers.bmp Lichtenstein.bmp

Figure 3. Cover image used

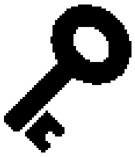


Figure 4. Watermark image used

BeaufortKey.bmp EcncryptedWatermark.bmp

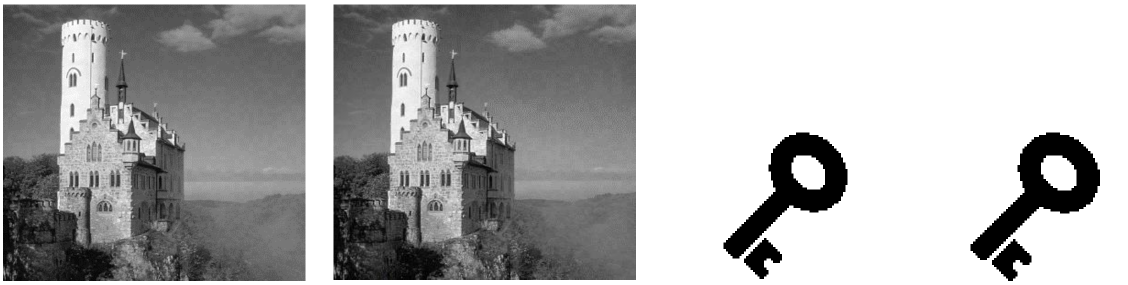
Figure 5. Watermark encryption process

Based on the hypothesis that has been discussed on Beaufort cipher key background will be utilized to improve security and imperceptibility of the watermark. This key will be used to spread encrypted watermarks. Table 1 shows the value of MSE, PSNR watermarked image and NCC values of non-attack image extraction. Table 1 also compares the embed results by utilizing Beaufort and without Beaufort keys.

Table 1. MSE, PSNR, SSIM and NCC Value of Watermarked Image without An Attack

	Using Beaufort cipher key (proposed)			Without Beaufort cipher key		
Image	MSE	PSNR (dB)	NCC	MSE	PSNR (dB)	NCC
Onion	44.6241	2.2422	1	39.1425	7.9219	1
Lena	44.5565	2.2773	1	39.1382	7.9297	1
Mandrill	44.3033	2.4141	1	39.0999	8.0000	1
Peppers	44.4607	2.3281	1	39.0766	8.0430	1
Lichtenstein	44.3888	2.3670	1	39.1168	7.9689	1
Average	44.4667	2.3257	1	39.1148	7.9727	1

Based on the observation in Table 1, it can be concluded that the use of Beaufort key at the time of embedding watermark proved to improve the quality of imperceptibility, and of course also the security of watermark. The mean difference of PSNR value reaches 5.3519 dB and MSE reaches 5.6470. Extraction can also be done perfectly as evidenced by the value of NCC 1. Although the invisible eye does not appear a significant difference as shown in Figure 6.



Without Beaufort key Using Beaufort key Without Beaufort key Using Beaufort key

Figure 6. Sample the watermarked image and extracted watermark result

Robustness testing is done by giving some manipulation to the watermarked image. After the watermarked image manipulation is extracted to get the watermark image. After manipulation is usually a watermark image cannot be extracted perfectly, but at least the watermark can still be identified. Table 2 shows the comparison results of the watermark resistance test against various attacks. JPEG compression, mid filter, crop, scaling, Gaussian noise, and salt and pepper.

The last test in this study is the computational performance test of the algorithm. In this study only gauge the time required when computing. This time is measured by tic toc function in Matlab. The use of the tic toc function will indeed result in different times on each computer. But at least the measurement results with the tic toc function can provide an overview of the time required to compute the embedding process, encryption, extraction and watermark decryption. Computers used in this research is a desktop computer with Intel i3 processor, 4GB memory, and onboard VGA. Table 3 shows the calculation of each process in each image with the tic toc function.

Table 2. NCC Value of the Watermarked Image with Various Attack

	NCC using Beaufort cipher key (proposed)					NCC without Beaufort cipher key				
Attack	Img1	Img2	Img3	Img4	Img5	Img1	Img2	Img3	Img4	Img5
JPEG	0.9606	0.9493	0.9489	0.9536	0.9522	0.9620	0.9507	0.9538	0.9509	0.9493
Salt Peppers	0.9857	0.9813	0.9812	0.9802	0.9782	0.9748	0.9714	0.9813	0.9792	0.9794
Scalling	0.9908	0.9911	0.8534	0.9619	0.9526	0.9913	0.9936	0.8512	0.9561	0.9502
Gaussian	0.9561	0.9619	0.9548	0.9687	0.9601	0.9579	0.9713	0.9668	0.9713	0.9612
Mid Filter	0.9982	0.9953	0.8416	0.9882	0.9322	0.9986	0.9994	0.8440	0.9905	0.9363
Crop	0.9186	0.9138	0.9251	0.9230	0.9191	0.9149	0.9182	0.9231	0.9181	0.9212
Average	0.9683	0.9655	0.9175	0.9626	0.9491	0.9666	0.9674	0.9200	0.9610	0.9496

Table 3. Time Taken to Process the Watermark

Image	Embedding	Encrypt	Extraction	Decrypt
Onion	0.7464	0.0004	0.6841	0.0005
Lena	0.7524	0.0005	0.6857	0.0005
Mandrill	0.7161	0.0005	0.6933	0.0006
Peppers	0.8591	0.0012	0.6857	0.0005
Lichtenstein	0.7307	0.0007	0.7041	0.0005
Average	0.7609	0.0007	0.6906	0.0005

4. Conclusion

This research proposes a watermark algorithm using block-based DCT, in which DC coefficient is selected to keep the watermark resistance inserted. Beaufort ciphers are also proposed for improved watermark security. In order for the algorithm to run efficiently Beaufort's key is also used for enhancement of imperceptibility aspects. This idea is based on spread spectrum techniques that use PN sequences. By utilizing Beaufort keys instead of PN sequences, imperceptibility can increase. The time required in the entire computation process of the proposed method is also relatively very fast with an average time of fewer than 1.5 seconds.

References

[1] SN Neyman, INP Pradnyana, B Sitohang. A New Copyright Protection for Vector Map using FFT-based Watermarking. *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2014; 12(2): 367-378.

[2] WS Sari, EH Rachmawanto, DRIM Setiadi, C A Sari. A Good Performance OTP Encryption Image based on DCT-DWT Steganography. *TELKOMNIKA Telecommunication Computing Electronics and Contro.* 2017; 15(4): 1987-1995.

[3] F Ernawan, M Ramalingam, AS Sadiq, Z Mustaffa. An Improved Imperceptibility and Robustness of 4x4 DCT-SVD Image Watermarking Using Modified Entropy. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC).* 2017; 9(2-7): 111-116.

[4] A Winarno, DRIM Setiadi, AA Arrasyid, CA Sari, EH 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.

[5] DA Iskandar, AB Rahhal, W Abdul. Block Based Image Steganography in Spatial and Frequency Domain. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC).* 2017; 9(2-10): 191-198.

[6] U Sudibyo, F Eranisa, EH Rachmawanto, DRIM Setiadi, CA Sari. *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, 2017.

[7] Z-C Yang, Z-H Li. *An Anti-JPEG Compression Digital Watermarking Technology with an Ability in Detecting Forgery Region for Color Images*. in International Conference on Computer Distributed Control and Intelligent Environmental Monitoring (CDCIEM), Hunan, 2012.

[8] C Pradhan, V Saxena, A K Bisoi. *Non Blind Digital Watermarking Technique using DCT and Cross Chaos Map.* in International Conference on Communications, Devices and Intelligent Systems (CODIS), Kolkata, 2012.

[9] J Li, Y Wang, S Dong. *Video Watermarking Algorithm based DC Coefficient*. in International Conference on Image, Vision and Computing (ICIVC), Chengdu, 2017.

[10] C Wei, L Zhaodan. *Robust Watermarking Algorithm of Color Image Based on DWT-DCT and Chaotic System*. in International Conference on Computer Communication and the Internet (ICCCI), Wuhan, 2016.

[11] MNM Najih, DRIM Setiadi, EH Rachmawanto, CA Sari, SetiaAstuti. *An Improved Secure Image Hiding Technique Using PN-Sequence Based on DCT-OTP.* in International Conference on Informatics and Computational Sciences (ICICoS), Semarang, 2017.

[12] Y Xiang, I Natgunanathan, D Peng, G Hua, B Liu. Spread Spectrum Audio Watermarking Using Multiple Orthogonal PN Sequences and Variable Embedding Strengths and Polarities. IEEE/ACM T*ransactions on Audio, Speech, and Language Processing*. 2017; 26(3): 529-539.

[13] V Bánoci, G Bugár, M Broda, D Levický. *Robust Spread Spectrum Watermarking System in Video*. in International Symposium ELMAR (ELMAR), Zadar, 2014.

[14] B Mathon, F Cayre, P Bas, B Macq. Optimal Transport for Secure Spread-Spectrum Watermarking of Still Images. IEEE Transactions on Image Processing. 2014; 23(4): 1694-1705.

[15] A Ansari, H Danyali, MS Helfroush. *Spread-Spectrum Robust Image Watermarking for Ownership Protection*. in Iranian Conference on Electrical Engineering (ICEE), Tehran. 2014.

[16] H Seddik, EB Braiek. *Image Securing based Chaotic Encryption Coupled with DCT Robust Watermarking*. in International Conference on Electrical Engineering and Software Applications (ICEESA), Hammamet. 2013.

[17] P Singh, S Shivani, S Agarwal. *A Chaotic Map Based DCT-SVD Watermarking Scheme For Rightful Ownership Verification*. in Students Conference on Engineering and Systems (SCES), Allahabad. 2014.

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

[19] A-F Drăgan. *Another Steganographic LSB-based Function*. in International Conference on Communications (COMM), Bucharest, 2012.

[20] K Alallayah, M Amin, WA El-Wahed, A Alhamami. Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier. *The International Arab Journal of Information Technology.* 2010; 7(4): 365-372.

[21] H-a Li, Z Li, Z Du, Q Wang4. Digital Image Watermarking Algorithm Using the Intermediate Frequency. *TELKOMNIKA Telecommunication Computing Electronics and Control.* 2014; 14(4): 1424-1431.

[22] C Irawan, DRIM Setiadi, CA Sari, EH Rachmawanto. *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, 2017.

[23] DRIM Setiadi, J Jumanto. An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection. *Cybernetics and Information Technologies*. 2018; 18(2): 74-88.

[24] P Singh, S Shivani, S Agarwal. *A Chaotic Map based DCT-SVD Watermarking Scheme for Rightful Ownership Verification*. in Students Conference on Engineering and Systems (SCES), Allahabad. 2014.

[25] Migh Hsieh Department of Electrical Engineering. SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/. [Accessed March 2018].