CONFIDENTIAL DATA TRANSPORT IN NOISE IMAGE

Abdurrahman HAZER [1], *İbrahim ÖZEN* [2], *Remzi YILDIRIM* [3]

[1] Yıldırım Beyazıt University, Ankara/Turkey, 155105128@ybu.edu.tr
[2] Yıldırım Beyazıt University, Ankara/Turkey, ibrahimozen5817@gmail.com
[3] Yıldırım Beyazıt University, Ankara/Turkey, remzi1963@gmail.com

***Abstract* – In this work, cryptography has been developed to ensure that confidential information is communicated securely. As a method, a randomly generated phase mask and a grey level picture made entirely of noise is used. The information that is corrupted in phase is placed in this noisy image according to a predetermined algorithm. First of all, the image is closed with a randomly generated phase mask and then the pixel values of the image whose phase value is completely corrupted are scattered into the carrier by sliding along with certain mathematical operations. In order to recover the encrypted image and information, carrier and randomly generated phase keys are used respectively. It has been tested that the reliability of the algorithm developed with two keys and robustness of the algorithm to noise attacks. In addition, the reliability of the developed algorithm is also tested with techniques such as correlation, histogram and contrast stretching.**

***Keywords* – cryptography, data security, image processing, phase retrieval**

I. INTRODUCTION

Recently, with the rapid increase in internet usage, multimedia sharing such as photos and videos on the internet has increased. For this reason, secure transmission of multimedia data to the other side has become a very important issue. To provide this security, cryptography techniques are of great interest and there are many different studies on the subject in the literature. AES [1], DES [2], RSA [3], chaotic based encryption [4], S-box [4], phase retrieval based encryptions and transform based encryptions [5, 6, 7] are widely known data encryption algorithms. In addition to data encryption algorithms, the data can be transmitted by hiding into a carrier image and this technique is called Steganography in the literature. LSB [8], PVD [9] and transform based algorithms [10] are some of the Steganography techniques. It is important to note that when transmitting data with classical steganography technique, the difference between the original form of carrier image and the form after concealment of the data into the carrier image must be minimal. If the difference between these forms of the carrier image increases, the steganography algorithm fails. In this work, a hybrid method has been developed by combining encryption and steganography. Since the information matrix can be converted completely into white noise, phase retrieval based optical encryption is used on the encryption side. In this way, if the hidden data is somewhat exposed, there will be only a white noise. In the steganography side, a different method than the classical steganography techniques has been applied. A completely noisy and large-scale image has been created for the carrier to give the illusion that the data is directly encrypted. Thus, the actual size of the data matrix to be transmitted and encrypted with phase retrieval based technique is known only by the algorithm. Security is further enhanced by scattering the encrypted data into the carrier.

II. DEVELOPED ENCRYPTION METHOD

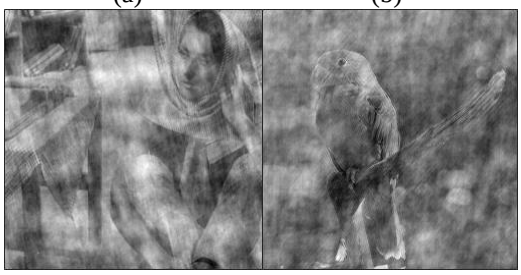
The encryption method developed in this study consists of two main algorithms. One of these algorithms is the phase retrieval algorithm, and the other is the algorithm that distributes the corrupted information into a noisy image. The details of the algorithms used are described in this section together with the encryption and decryption processes.

A. Phase Retrieval Algorithm

An image consists of amplitude and phase components. However, the amount of information they carry is not the same. Since the phase component carries more information about the image, if the phase is removed or corrupted, the image itself is distorted. In order to appreciate the importance of the phase, two images have been selected and the phase information of these two images has mutually exchanged. The results of the modified phase images are given in Figure 1. As can be easily understood from Figures 1(c) and 1(d), the phase component of an image carries more information than its amplitude. In order to recover the phase of an image in which the phase information has disappeared or corrupted, phase retrieval algorithms have been written. The purpose of these algorithms is to recover the phase information from the Fourier amplitude of the image. Phase retrieval algorithms which have a lot of application fields are used for the purpose of data encryption in this work. In this area, encryption algorithms are also known as optical encryption, and two random phase encoding algorithm done by Refregier and Javidi is one of the studies leading to the field of optical cryptography [11]. Over time, optical cryptography has been further developed using different matrix spaces such as Fresnel, Gyrator and Fractional Fourier [5, 6, 7]. In this study, Error Reduction (ER) algorithm, which is a classical method, is used because it can obtain the phase of an image accurately and quickly [12].

Let $y \in \mathbb{R}^{mxn}$ is the image to be recovered and $a = |Fy| \in \mathbb{R}_{+}^{m \times n}$ is the Fourier amplitude of image [12]. Here, $\mathbb{R}$ and $\mathbb{R}_{+}$ denotes set of real numbers and set of positive real numbers, and y represents image matrix. In equations m and n denotes row and column numbers of the

(a) (b)



(c) (d)

Figure 1: (a) Parrot image, (b) Barbara image, (c) new image consisting of the amplitude of Parrot image and the phase of Barbara image, (d) new image consisting of the amplitude of Barbara image and the phase of Parrot image.

image matrix respectively. The term F represents 2 dimension (2-D) discrete Fourier transform and "a" represents Fourier amplitude. The aim here is to find out itself of an image given Fourier amplitude. Accordingly, the Error Reduction algorithm can be expressed as

$$y_{d+1} = P_D P_A y_d, \tag{1}$$

where "y" and sub-index "d" denote image matrix and number of iterations respectively. In Equation (1), $P_D(y)$ and $P_A(y)$ denotes the projection operators that contain the operations necessary to retrieve the image and they can be written as

$$P_D(y) = \begin{cases} y_{i,j} & \text{if } (i,j) \in E \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

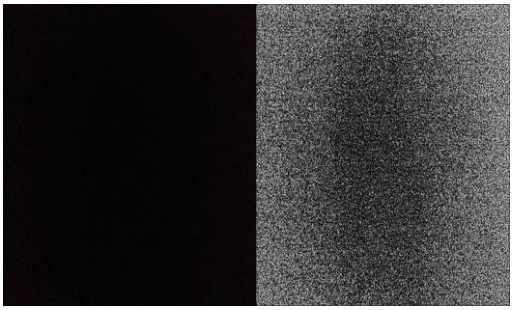
and

$$P_A(y) = F^{-1}(z),\ z_{i,j} = \begin{cases} a_{i,j} \dfrac{Fy_{i,j}}{\left|Fy_{i,j}\right|}, & \text{if } Fy_{i,j} \neq 0 \\ Fy_{i,j}, & \text{otherwise} \end{cases}, \tag{3}$$

where y and E denote image matrix and bounded set, and (i, j) represents row and column numbers of the image matrix respectively. In Equation (3), $a_{i,j}$ denotes Fourier amplitude of image and $Fy_{i,j}$, $\left|Fy_{i,j}\right|$, $\left(Fy_{i,j} / \left|Fy_{i,j}\right|\right)$ represent 2-D discrete Fourier transform of the image, Fourier amplitude of the image and phase information respectively. The term F^{-1} denotes inverse Fourier transform.

B. Creation of The Carrier Matrix

In order to create the carrier matrix used in this work, firstly



(a) (b)

Figure 2: (a) 4608x3870 pixel-sized photo taken in the dark and (b) 16-bit depth image with contrast stretching.

a photograph is taken with an ordinary camera in a rather dark environment. Secondly, the size of this photo with a pixel size of "3264x2448" is scaled up to "4608x3870" in the Matlab and the image in Figure 2(a) is obtained. Afterward, the image whose pixel size is enlarged is converted to 16-bit depth and then the image of Figure 2(b) is generated by subjecting the image to contrast stretching. The image in Figure 2(b) is also the final form of the image used as a carrier.

C. Encryption Process

First of all, around the data to be encrypted is added zero as the size of the data with the oversampling method used in the phase retrieval algorithms. Let $y \in \mathbb{R}^{mxn}$ is data that doubles the pixel size and $D \in \mathbb{C}^{m \times n}$ is diagonal matrix created by a random phase mask. Here, $\mathbb{R}$ and $\mathbb{C}$ represent set of real numbers and set of complex numbers respectively. In this case, the data is corrupted and its Fourier amplitude is calculated by

$$a = \left|F(Dy)\right|. \tag{4}$$

In Equation (4), "F" and "a" represent 2-D discrete Fourier transform and the Fourier amplitude of the corrupted data respectively. Accordingly, the projection operator P_A in Equation (3) can be rewritten as

$$P_A(y) = \frac{F^{-1}(z)}{D},\ z_{i,j} = \begin{cases} a_{i,j} \dfrac{Fy_{i,j}}{\left|Fy_{i,j}\right|}, & \text{eğer } Fy_{i,j} \neq 0 \\ Fy_{i,j}, & \text{otherwise} \end{cases}. \tag{5}$$

The only difference of projection operator that is rewritten according to Equation (4) from the operator in Equation (3) is that the diagonal matrix represented by "D". The Fourier amplitude of data, which is transformed into completely white noise by the distortion defined in Equation (4), is distributed into the carrier by subjecting to the algorithm of Figure 3. According to the algorithm, the data that transforms into white noise is first divided into cellular matrices, each of which is represented by "Λ" and is of size "4x4". Then, a new block matrix is generated from these cellular matrices, whose total number depends on the size of the data and is represented by "B". In the algorithm, "ax" and "ay" are used as row and column shift operators, respectively, and their values are changed according to the size of the data. With the transform

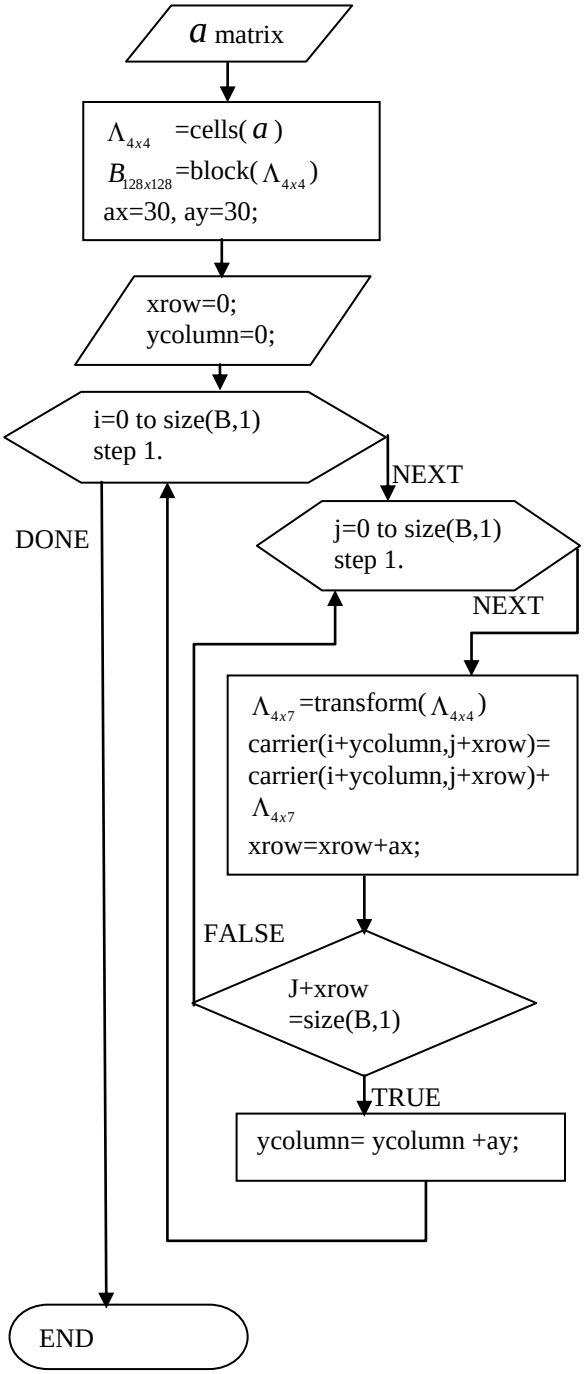
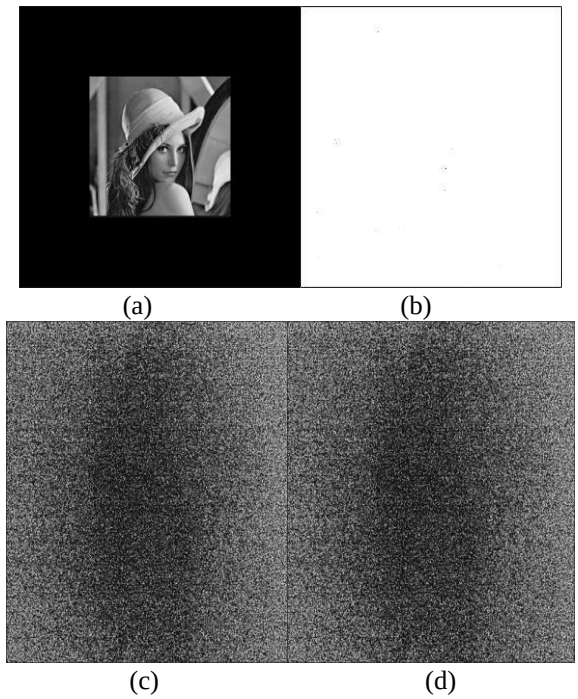


Figure 3: Algorithm for distributing the encrypted data into the carrier.

$$\Lambda = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}, \mathrm{B} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{31} & a_{41} & \\ & a_{22} & a_{23} & a_{24} \\ & a_{32} & a_{42} & \\ & & a_{33} & a_{34} \\ & & a_{43} & \\ & & & a_{44} \end{pmatrix}$$

(a) (b)

Figure 4: (a) "4x4" cell matrix and (b) "4x7" new matrix



(a) (b) (c) (d)

Figure 5: (a) 512x512 Lena, (b) the Fourier amplitude of the corrupted by random phase mask, (c) 4608x3870 noisy carrier (second key), (d) the data-added carrier

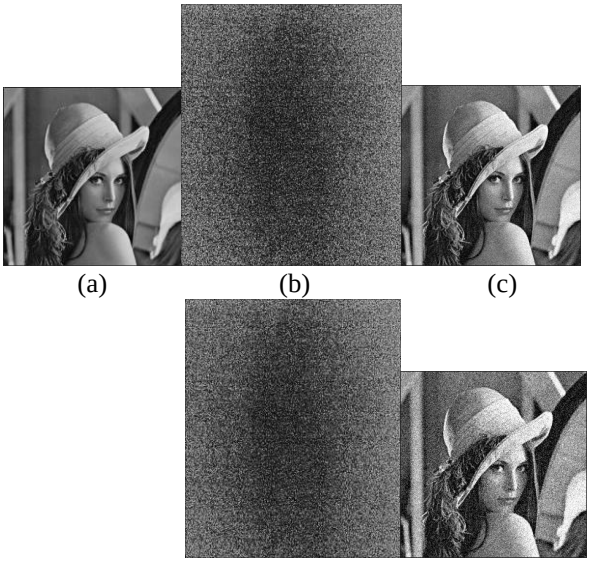
function, each cell (Λ) in the (B) matrix is transformed into a new "4×7" matrix as shown in Figure 4(b). Each cell that is transformed is distributed into the carrier according to the values of "ax" and "ay".

D. Decryption Process

In the decoding process, the cells placed in the carrier according to the algorithm of Figure 3 are recombined with the inverse of the same algorithm to obtain encrypted data consisting entirely of white noise. At this stage, encrypted data is decrypted by using Error Reduction algorithm described in Equation (1) with second key which is random phase mask.

III. Experimental Studies

The number of iterations can be selected at the desired value for the phase retrieval algorithm. However, when the iteration value is chosen less than 100, the encrypted data is decrypted as noisy. At the same time, choosing a value greater than 100 for the iteration value has no effect on the image except for slowing down processing time of the algorithm. Because of these reasons, the number of iterations has been chosen as 100 for this study. The "ax" and "ay" values used to shift row and column respectively in the algorithm given as Figure 3 are changed according to the size of the data matrix. In experimental study of the method, "ax"=50, "ay"=70 for "128x128" size of matrix, "ax"=35, "ay"=40 for "256x256" size of matrix and "ax"=25, "ay"=25 for "512x512" size of matrix. Figure 5 shows the encryption of the "512x512" size Lena image. The image of Lena, which is sampled according



(a) (b) (c)

(d) (e)

Figure 6: (a) 256x256 Lena, (b) the encrypted image with σ=5 Gaussian noise, (c) the decrypted image (MSE=0.0051, PSNR=23.8105), (d) the encrypted image with σ=10 Gaussian noise, (e) the decrypted image (MSE=0.0155, PSNR=20.3603)

to the Nyquist criterion, has become a matrix of size "1024x1024" as shown in Figure 5(a). Then, the sampled image is distorted by the random phase mask and its Fourier amplitude is obtained as shown in Figure 5(a). Finally, this Fourier amplitude is scattered into the carrier shown in Figure 5(c) by applying the algorithm of Figure 3 and the result is given in Figure 5(d).

IV. Security Tests

The reliability of the encryption method being developed to ensure secure transmission of information has been tested by standard methods as follows: noise attack, contrast stretching, correlation and histogram analysis [2, 6, 11, 13].

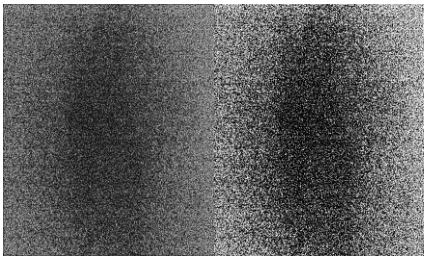
A. Noise Attack

Gaussian noise with sigma values of 5 and 10, respectively, is added to the encrypted image to measure the noise resistance of the method used. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters are used to analyze the results of the noise test. Mean Square Error (MSE) is a measurement parameter that shows the similarity between two images, and it can be expressed as

$$MSE = \frac{1}{nm}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}\left(y(\mathrm{m},\mathrm{n}) - \mathrm{yrec}(\mathrm{m},\mathrm{n})\right)^2, \qquad (6)$$

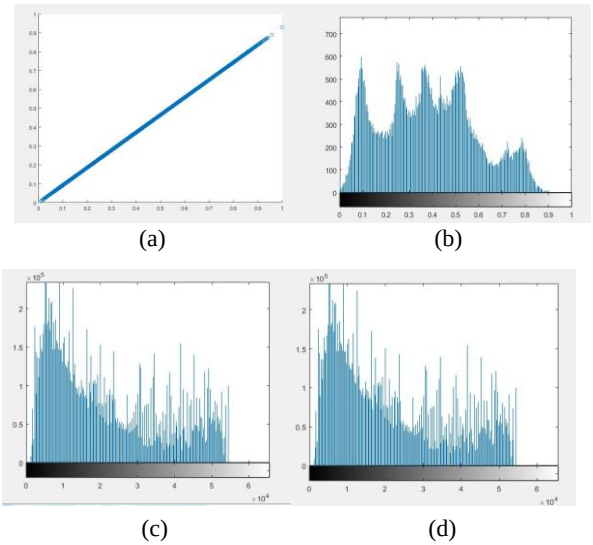
where "y" and "yrec" denote original image and noisy image, and (m, n) denote row and column numbers of the image matrix respectively. If the Mean Square Error value is low, the difference between the images is small, while if it is too much, the difference between the images is high. Peak Signal to Noise Ratio is the ratio of the noise to the image and is in dB. Peak Signal to Noise Ratio can be described as

$$PSNR = 10\log_{10}\frac{S^2}{MSE}, \qquad (7)$$



(a) (b)

Figure 7: (a) Encrypted data and (b) image resulting from contrast stretching operation.



(a) (b)

(c) (d)

Figure 8: (a) the correlation analysis between carrier and the data-added carrier, (b) the histogram of the data (Lena) to be transmitted, (c) the histogram of the carrier and (d) the histogram of the data-added carrier

where "S" and MSE represent the maximum pixel value in the image matrix (for gray-level 8 bits images S=255) and the mean square error value defined in Equation (6). If the PSNR value is low, the difference between the original image and the noisy image is small, while if it is too much, the difference between these images is high. The results of the noise attack test for the hybrid method used in this work are shown in Figure 6.

B. Contrast Stretching

Contrast stretching is usually used for image enhancement. In this study, however, the carrier has been subjected to contrast stretching in order to detect the encrypted data placed on the carrier. It has been tested that no information other than noise has been obtained by contrast stretching and the result has been given in figure 7.

C. Correlation Analysis

Correlation analysis for an image shows whether the pixels are adjacent to each other by looking at the relationship between the two selected pixels. Correlation analysis can be done between two images as it is done in this study. While it is expected that this correlation is close to 0 in direct image

encryption algorithms, it is expected to be close to 1 in steganography algorithms. For the algorithm used in this study, the result of the correlation analysis by selecting a random 10000 pixel pair between the carrier and the data-added carrier is given in Figure 8(a). As a result, the correlation coefficient is 1, and these two images are interpreted as identical except for very small changes.

D. Histogram Analysis

Although the histogram analysis is used for image processing in many different purposes, the similarity of two images can be measured for the encryption field. Figure 8(b) shows the histogram of the data to be encrypted, while Figure 8(c) and Figure 8(d) shows the histogram graphs of the carrier and the data-added carrier, respectively. As can be seen from the graphs, there is no difference between the carrier and the data-added carrier histograms, but the result is that the histogram of the data is different than these two images.

V. Conclusions

This work has been done using a hybrid method consisting of encryption algorithm and algorithm inserting encrypted data into a noisy carrier. While the section of encryption consists of phase retrieval algorithm, the section of inserting encrypted data into a noisy carrier consists of a block based algorithm. The hybrid method used consists of two keys. One of the keys is the same as the size of the encrypted matrix and 512 * 512 = 262144 for this work. The second key is the carrier matrix itself and the size of it is 4608 * 3870 = 17832960. Gaussian noise test with sigma values of 5 and 10 has been applied on the method. As a result of the test, the MSE value of the reconstructed image for sigma value 5 is 0.0051, the PSNR value is 23.8105 dB, while the MSE value of the reconstructed image for sigma value 10 is 0.0155 and the PSNR value is 20.3603 dB. The result in Figure 7 (b) shows that no information other than the noise is obtained by contrast stretching. Correlation and histogram tests applied to carrier matrix and data-added carrier matrix shows that the correlation coefficient 1 and the histogram graphs of the two matrices are the same.

References

[1] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., & Tourki, R. (2007). A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering, 1(1), 70-75.

[2] Yun-Peng, Z., Wei, L., Shui-ping, C., Zheng-jun, Z., Xuan, N., & Wei-di, D. (2009, October). Digital image encryption algorithm based on chaos and improved DES. In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on (pp. 474-479). IEEE.

[3] El-Deen, A., El-Badawy, E., & Gobran, S. (2014). Digital image encryption based on RSA algorithm. *J. Electron. Commun. Eng*, *9*(1), 69-73.

[4] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons & Fractals, 95, 92-101.

[5] Rajput, S. K., & Nishchal, N. K. (2014). Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxton phase-retrieval algorithm. Applied optics, 53(3), 418-425.

[6] Singh, H., Yadav, A. K., Vashisth, S., & Singh, K. (2015). Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. *Optics and Lasers in Engineering*, *67*, 145-156.

[7] Wang, X., Chen, W., & Chen, X. (2014). Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. *Optics express*, *22*(19), 22981-22995.

[8] Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In *Computer Communication and Informatics (ICCCI), 2014 International Conference on* (pp. 1-4). IEEE.

[9] Hussain, M., Wahab, A. W. A., Anuar, N. B., Salleh, R., & Noor, R. M. (2015, June). Pixel value differencing steganography techniques: Analysis and open challenge. In *Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on* (pp. 21-22). IEEE.

[10] Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. *Procedia Computer Science*, *46*, 612-618.

[11] Refregier, P., & Javidi, B. (1995). Optical image encryption based on input plane and Fourier plane random encoding. *Optics Letters*, *20*(7), 767-769.

[12] Fannjiang, A., & Liao, W. (2012). Phase retrieval with random phase illumination. JOSA A, 29(9), 1847-1859.

[13] Ghani, A. S. A., & Isa, N. A. M. (2015). Underwater image quality enhancement through integrated color model with Rayleigh distribution. *Applied soft computing*, *27*, 219-230.