Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT APPROACH FOR IMAGE HIDING USING HYBRID TECHNIQUE

ABDULLAH MOHAMMED AWAD[1], MUZHIR SHABAN AL-ANI[2]

[1]Lecturer, University of Anbar, College of Computer and Information Technology, Department of Information System, Ramadi, Iraq [am_awad2@yahoo.com]

[2]Professor, Development University of Human, College of Science and Technology, Department of Information Technology, Sulaimani, KRG, Iraq [muzhir.al-ani@uhd.edu.iq]

ABSTRACT

Recently, many works are published concerned with image encryption and information hiding. Some of these works are concentrated on hiding of image and others are concentrated on hiding of text. These works have various applications such as; communication systems, multi-media systems, image and data compression and cryptography. The research aims to introduce an efficient approach for image hiding using hybrid technique**.** The proposed approach based on hiding the information via the cover image and then encrypting the image to generate a new image carry the information. This paper deals with the efficient method for image hiding taking into consideration the features which are built applying discrete wavelet transform (DWT). The achieved contribution from this research is concentrated on applying DWT leading to powerful hiding technique**.** A good performance and result for image hiding are obtained using this approach.

Keywords: *Image Hiding; Image Compression; DWT; Image Encryption.*

1. INTRODUCTION

Multimedia development and multimedia data, especially image data are utilized by a great number of people in various situations by exploiting the network device. A large part of multimedia data is specified to create a sense of amusement, politics, economics, armies, industries or education. Thus, it is necessary to secure this data by providing privacy, trustworthiness, and possession or individuality. Many practical functions are needed to protect image contents. Cryptology, which are viewed as competent style for information privacy and safety.

However, traditional Cipher methods are used as IDEA RSA, IDES and AES of employed for binary data or content are not suitable for image encrypt because the size of digital image very large. Indeed, the conventional ciphers usually used to encrypting image data is highly in cost. Furthermore, and most importantly to have an accurate encryption that maintains information to get successful practical applications. Chaotic non-linear have not static features and they have a high sensitivity to start conditions. Chaotic system commonly active aspects. Since chaotic systems have superior qualities, they are usually utilized in communications and encryption of the image in 1989 Mathews presented the discrete chaotic not static or named dynamical system as Initial application in cryptography [1]. Chaotic system is a nonlinear dynamic system. As the chaos system are sensitive to and randomness to initial condition and high-speed characteristics calculation make the chaos encryption proper for image encryption.

The goal of our research to get high performance for hiding image using the characters of chaotic system specification. The transformed image keep all the original image information. Traditional image hiding techniques are not suitable to protect image information. This paper proposed a technique to hide image by mixing two techniques is good choice for this issue.

The remaining objectives of this paper is organized as follow:

- First: Explain survey on some significant related work
- Second: Show the basic concepts of image hiding.
- Third: Summarizes the discrete wavelet transform.
- Fourth: Proposed the sufficient model.
- Fifth: Discuss the results.
- Sixth: show the main conclusions.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. RELATED WORKS

In 1950s, Shannon clearly states that cryptographic chaos can be archived due to its central crease mechanism and its stretching [2]. The need for encryption turns out to be an urgent need and the chaos theory grows until it is approved by the cryptographers of the time until the 1980s. Shannon confirms that the fulfillment of chaos overcame the chaos and proposes the figure the first fundamental chaos and coincidence of chaos in the 1980s and it was clearly seen in 1990 as well. The first figure based on chaos was suggested in 1990 and chaos entered the scene. In fact, many books related to chaos have been published. (Baplista 1998) 1996 extended the chaotic encryption. Although the origins of the system of standard chaos are based on continuous systems and distinctive features since 2000, the chaos emerged as a protected statement as an application in Chaotic cryptography in chaotic cryptography was carried out in 2006 by Alvarez and Li, where some consequences of the non-static or dynamic fall of a chaotic map are exposed within the core of cryptography. Undoubtedly, the researchers focused on this study to evaluate the chaotic encryption technique. The chaotic encryption techniques are similar, but here the activation was carried out only by chaos. The algorithm based on the chaotic key (CKBA) as an encryption method generates a bit sequence key using a chaotic system proposed by (Yen and Guo) [5], the binary sequence is generated and, consequently, the key pixel of the selected image arranged. There are certain techniques that encrypt part of the image or audio and not all the content [6, 7].

An efficient algorithm is proposed as a partial wavelet fast transformation (DWT) and flow encryption (RCY) scheme for image encryption. According to its technique, the lowest frequency band is achieved by the encryption of flow to obtain the encryption.

The main method of his proposal was to maintain the information of the image. In fact, one byte at a time should generally be encrypted. Flow ciphers consume more time than we can combine between the original image and the key stream using the XOR bit (XOR) when the first can be generated by random number. A reordering algorithm is used when edges are found [9]. We can reduce the encryption and the lower frequency band of the image is encrypted and the rest of the image is mixed. A high level can be maintained by a large key space 256 using a reorganization algorithm. The entropy result is approximately 4.7807 since the encrypted image can be observed to provide reliable intruder to decipher the secret key used to encrypt the image because the PSNR approximately 20.7056 dB and this value is very strong against the attack [8].

The fields of encryption, compression and hiding were found for long time. Most of the above related works are concentrated on a single problem to be solved. This research try to combine both chaotic for encryption and discrete wavelet transform for compression in order to generate an efficient hybrid technique.

3. STATEMENT OF THE PROBLEM

Many works have been published in the field of encryption and compression. The main challenges in this area is how to reach a minimum time of processing, means how to reduce number of operations as possible, and how to reach a high level of compression with minimum error of the retrieved data. The proposed approach try to overcome these challenges as possible by introducing a hybrid approach of chaotic encryption and discrete wavelet transform compression.

4. CHAOTIC CRYPROGRAPHY

Baptista, (1998) proposed the chaotic figure section [3]. This section provides a better encryption algorithm than the traditional key algorithm and the start state. First, find the route of the curve from the map of the map to the encryption of the message. Then, discover the configuration. The initial state was considered the constant route (trajectory). To achieve a meaningful result, the chaotic equation must be repeated until the route reaches the destination site and the amount of repetition is maintained later, since the code of each message is the curved route that is based on the same process to produce the next digit.

The essential thing to achieve the chaotic signal is the flow of succession of the process for the encryption, since an entry reproduces the parameter and the first condition to decipher the message there try to use for each decipherment the same mapping scheme the number of repetitions was made by the encryption to the chaotic equation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consider the location of the road ultimately belongs, keep the location figure as a message symbol then by the following message decryption by the message symbol we can repeat the next symbol and so on [10]

The method of encrypting the message or video data by chaotic equation can be achieved by the broad chaos encryption method. This method can facilitate the idea of finding essential information to provide the level of security of life. This can be considered as the advantage of chaotic encryption [10]:

- High level security.
- Repetition is essential to obtain encryption.
- Simple method used.
- Shortcuts will not be accepted.

Two reasons make chaotic encryption attractive for any business to keep data communications simple and inexpensive. The cell phone industry would be included in this process. The chaotic data encrypted for the essential and flourishing decryption that three components face at the end of the receiver and the transmitter end that the procedure is connected to a formula called a card:

- Original conditions: this is a value selected by the patented chaotic encryption systems:
- Map: it is composed of parameters; these parameters are shared by the issuer to use it when mixing the data of the underlying message and by the receiver to use them as descramblers.
- Configurations. All types of parameters must be adapted in the transmitter and the receiver.

In 1976, O. Rossler suggested a new chaotic attractor with a basic and simple non-linear set arrangement of differential mathematical equations [19]. From a set of differential equations, the first widely-known chaotic attractor was the Rossler attractors, which are defined by three non-linear differential equations. This non-linear dynamical system displays a strange attractor.

$$dx / dt = -y - z$$
$$dy / dt = x + Ay$$
$$dz / dt = B + xz - Cz$$

A , B and C are cons .

5. DISCRETE WAVELET TRANSFORM

Frequency domain is an important domain for image processing. Images can be transformed from the time domain to frequency domain using discrete Fourier transform or discrete wavelet transformation. Discrete wavelet transformation procedure is used to be done before encryption process [17]. Discrete wavelet transformation can be implemented via the combination of both low pass filter and high pass filter. If one attempt to assess the lower or higher repetition the input data is run through which is named filter bank of low pass or high pass. Signal data is divided into approximation; signal of the lower recurrence and full information. By filter operation the decision of signal data is affected. Then the lower sampling is followed to cause a sort of deletion to some part of pieces from signal [18]. Figure 1 shows the main structure understanding breakdown of image using discrete wavelet transformation.

Blocks Lo or Hi demonstrate impulse reaction of low pass filter or high pass filter and block signed as 2 and this operation makes down sampling by 2 [19].

The final result of applying discrete wavelet transformation on image gives four sets of degrees are established after procedure of breakdown or dyadic decomposition of the image data [20,21]:

LL: The estimation of image data.

LH: The image characteristics in horizontal direction.

HL: The image characteristics in vertical direction.

HH: The image characteristics in diagonal direction.

There are many types (families) of wavelet such as Haar wavelet, integer wavelet and Dubchies wavelet. The Haar wavelet is the simple and easy type that utilized for this dyadic decomposition [22].
The image after transformation was broken down into frequency sub bands and the sub band of the lowest frequency was constantly broken down. However, reconstruct of image is achieved to the main level via applying inverse discrete wavelet transformation [23,24].

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

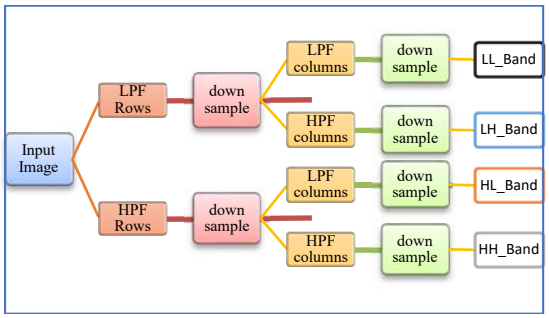


Figure 1: Wavelet Transform

6. THE PROPOSED HIDING ENCODING APPROACH

Chaotic is a powerful unpredictability and sensitivity to initial conditions. In accordance with the digital image feature of poor security and high repetition and chaotic encryption with the characteristic feature of high speed, we proposed a new image encryption algorithm that was used and mixed wavelet transformation with chaotic theory. However, it is able to study the encryption algorithm based on safety analysis through key sensitivity analysis, key space and statistical analysis.
The expected results will highlight the efficient image encryption method, which is faster than current methods, in wavelets the transmission of information is very low and the key space is large enough to handle the aggressive attack with an acceptable encryption result.

The suggested approach as shown in Figure 2 and Figure 3 clarifies the coding and decoding method in this order. The coding encryption process starts after the transformation of the image using wavelet transformation. At this time, the small rate values are chosen to encrypt using AES with the undisclosed input means.

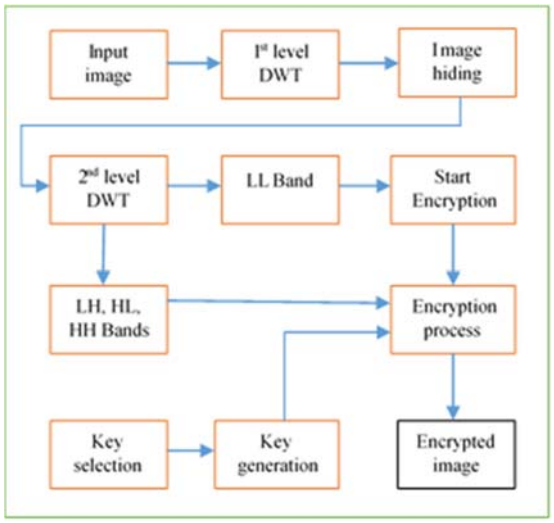


Figure2: Proposed Image Hiding And Encryption Model

At the same time, the chaotic sequence is generated using the Rossler Attractors map method to encrypt the other high frequency values of the transformed image. Finally, the result of these two encryption operations is merged by exchanging their values to obtain an encoded image.

The inverse of each operation is performed in the decoding model as shown below to decrypt each block and the inverse transformation to obtain the reconstructed image.

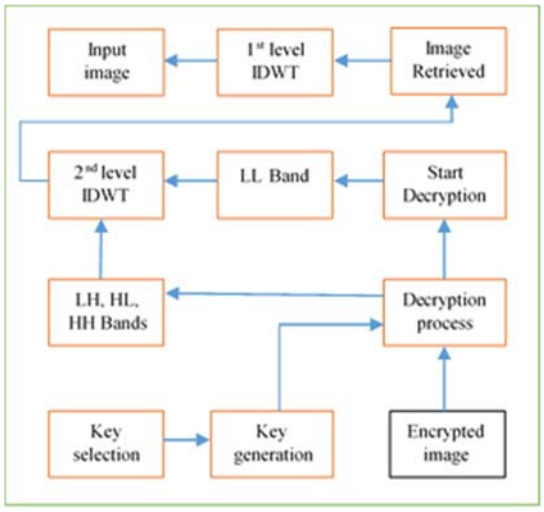


Figure 3: Proposed Image Retrieving And Decryption Model

The following algorithm 1 shows the main basic encoding operations that started from applying first level DWT then applying image hiding then

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

complete the encryption of image using selected key.

Algorithm 1: Hiding and Image Encoding.

Input: Original Image I , Parameters and Secret Choatic Keys (A, B, C, X0, Y0, Zo), where A, B and C are constants.

Output: Encoded Image C.

Step-1 Compute of Forward IWT for Image I.

(LL, LH, HL, HH) = IWT(I)

Step-2 Image hiding in LL band

Step-3 The LL part are encrypted by using AES

Generate Chaotic Sequence according to Rossler Attractor map to encrypted high frequency values:

Step-4

$$dx / dt = -y - z$$
$$dy / dt = x + Ay$$
$$dz / dt = B + xz - Cz$$

A B and C are Const .

Step-5 Convert the sequences Xi ,Yi,Zi into integer value.

Step-6
- Encrypt the red colore by Xi.
- Encrypt the green colore by Yi.
- Encrypt the blue colore by Zi.

Step-7 Spread each pixel in LL into each block of the LH, HL, HH according the following chaotic swapping:

C = Chaotic_Swap (LL, (LH, HL, HH))

The wavelet transform is used to transform the input image into their bands. The top left corner is denoted by LL frequency as a lowest frequency block and this block is encrypted by using AES directly that this block is very important information.The Chaotic Sequence according RosslerAttractors map is generatedto encrypted high frequency values.
The X key is used to encrypt the red color in image:

CERI i = ERIi ⊕ Xi

The Y key is used to encrypt the green color in image :

CEGI i = EGIi ⊕ Yi

The Z key is used to encrypt the blue color in image.

CEBI i = EBIi ⊕ Zi

The final operation of encoding technique is merging of CLL and CLH, CHL, CHH by spread each pixel in CLL into the blocks of the CLH, CHL, CHH according the following chaotic swapping:

C = Chaotic Swap [CLL, (CLH, CHL, CHH)].

The chaotic swapping parameter are:

$$I_{r1} = \lfloor X_0 * 8 \rfloor$$
$$I_{c1} = \lfloor Y_0 * 8 \rfloor$$

Where Ir and Ic represent the location shifting index of row r and column c for each pixel .

$$I_{rnew} = I_i * 8 + I_{r1}$$
$$I_{cnew} = I_j * 8 + I_{c1}$$

Algorithm 2 The Proposed Image Decryption Model	
Input: Encryption Image C and Secret Choatic Keys (A, B, C, X0, Y0, Zo), where a, b and r are constants. Output: The Reconstructed Image (RI).	
Step-1	Apply invers chaotic swapping C = Chaotic_Swap (LL, (LH, HL, HH))
Step-2	Image retriving
Step-3	Generate Chaotic Sequence according Rossler Attractors map to decrypted high frequency values: $dx / dt = -y - z$ $dy / dt = x + Ay$ $dz / dt = B + xz - Cz$ A B and C are Const .
Step-4	Convert the sequence Xi ,Yi and Zi into integer value.
Step-5	Decrypt the red colore by Xi. Decrypt the green colore by Yi. Decrypt the blue colore by Zi.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step-6	Decrypt (CLL) using AES by Secret Key Y: (LL) = AES_Decryption((CLL), Y)
Step-7	Comput the inverse of IWT

The next operation is to retrive the image from the coded one. The received enciphered image is isolated into lowest frequency parts CL and CH according inverse of chaotic swapping.

(CL, CH) = Chaotic_Swap (C).

With swapping parameter

$$I_{r1} = \lfloor X_0 * 8 \rfloor$$
$$I_{c1} = \lfloor Y_0 * 8 \rfloor$$

Where Ir and Ic represent the location shifting index of row r and column c for each pixel .

$$I_{rnew} = I_i * 8 + I_{r1}$$
$$I_{cnew} = I_j * 8 + I_{c1}$$

The blocks HL, LH, HH is decrypted using a chaotic encryption sequence where it is generated in encryption from the secret input values R and X0, R0, Z0. The LL will be deciphered using decryption AES with the secret key to obtain the upper left corner block. The last step of the inverse of the reconstruction of the original image can be implemented when the result of the decryption is processed with the invers wavelet transformation. The last step to concentrate on recovering the hidden image.

7. RESULTS AND DISCUSSIONS

The proposed system is implemented using C#.Net with PC specifications: intel coreTM2 duo processor 2GH, 4GB RAM and 2 GB video card based on Windows 8.1 operating system.

The proposed chaotic image encryption and hiding based on integer wavelet transforms and Rossler Attractors map. The improved chaotic image encryption method includes the following steps:

1. Five Keys are generated to be used for encryption.

- Computing Forward IDWT for input image and
- The hiding of iamge is applied in LL band and then encrypted using AES .

2. Generate Chaotic sequence according Rossler Attractors map and encrypt the red, green and blue colors respectively.

This system is implemented and tested for different images (Bear, Horses, Bridge and Autumn).

Figures (4,5,6 and 7(a)) show the encryption image and the histogram for the encrypted and original images. The encryption image appears as a scrambling image. In addition, the histogram does not indicate any information for the image, after the encryption this randomness is covered. The pixel distribution for original and encrypted images is shown in three horizontal, vertical and diagonal dimensions for three colors.

The retrived image is reconstructed via applying the decryption process on the encrypted image, this process is achived by reversing of each operation in the encryption process. There is small bit difference between original image and reconstructed image as indicated in thier histogram.

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

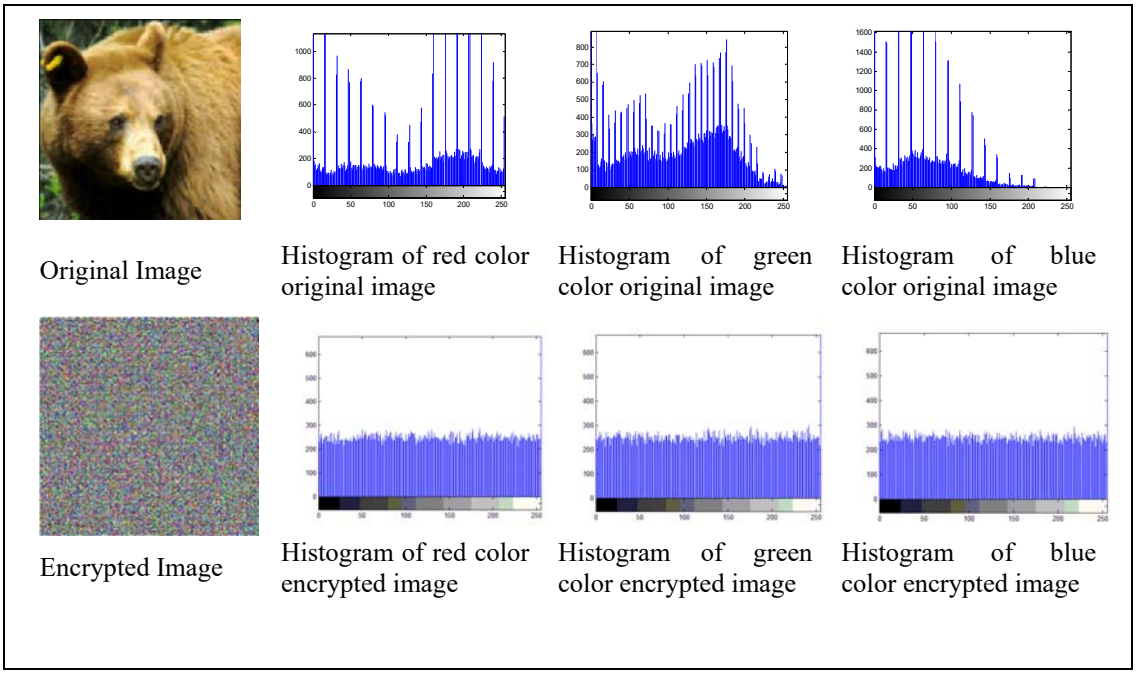


Figure 4(a): Histogram of Bear Image Before and After Encryption.

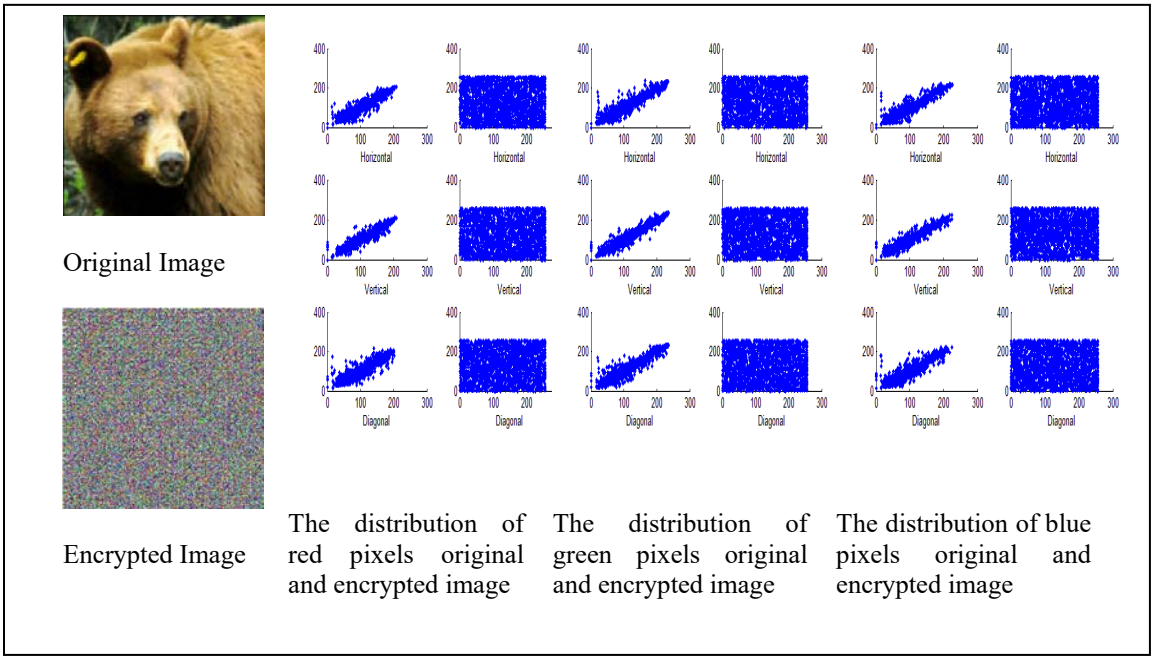


Figure 4(b): Distribution of Pixels in Bear Image Before and After Encryption.

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

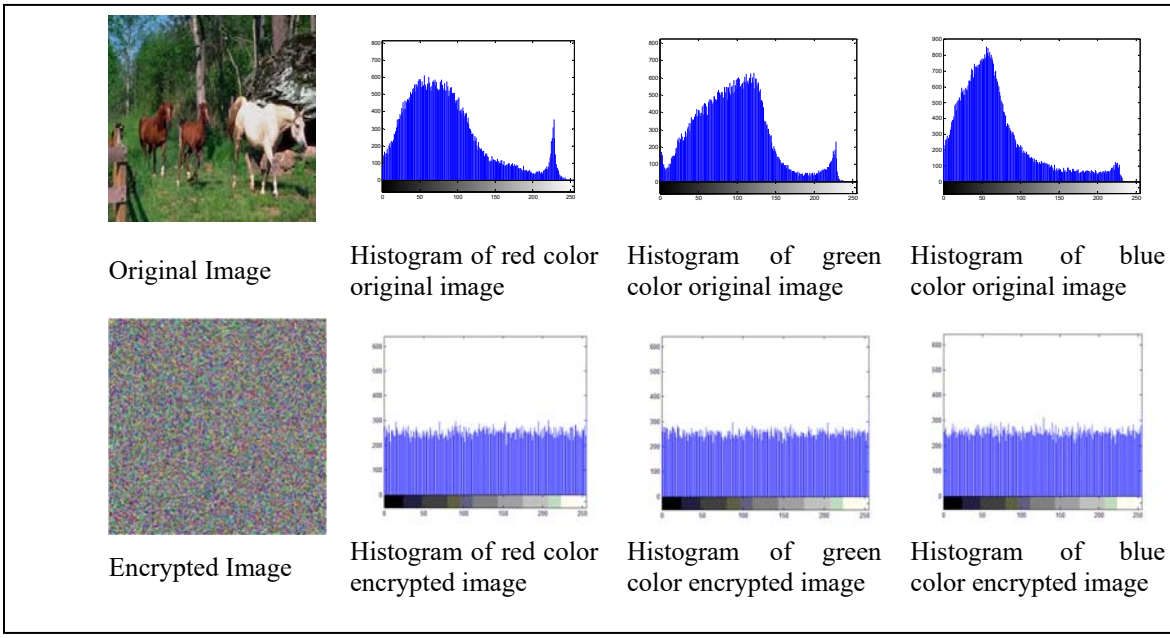


Figure 5(a): Histogram of Horses Image Before and After Encryption

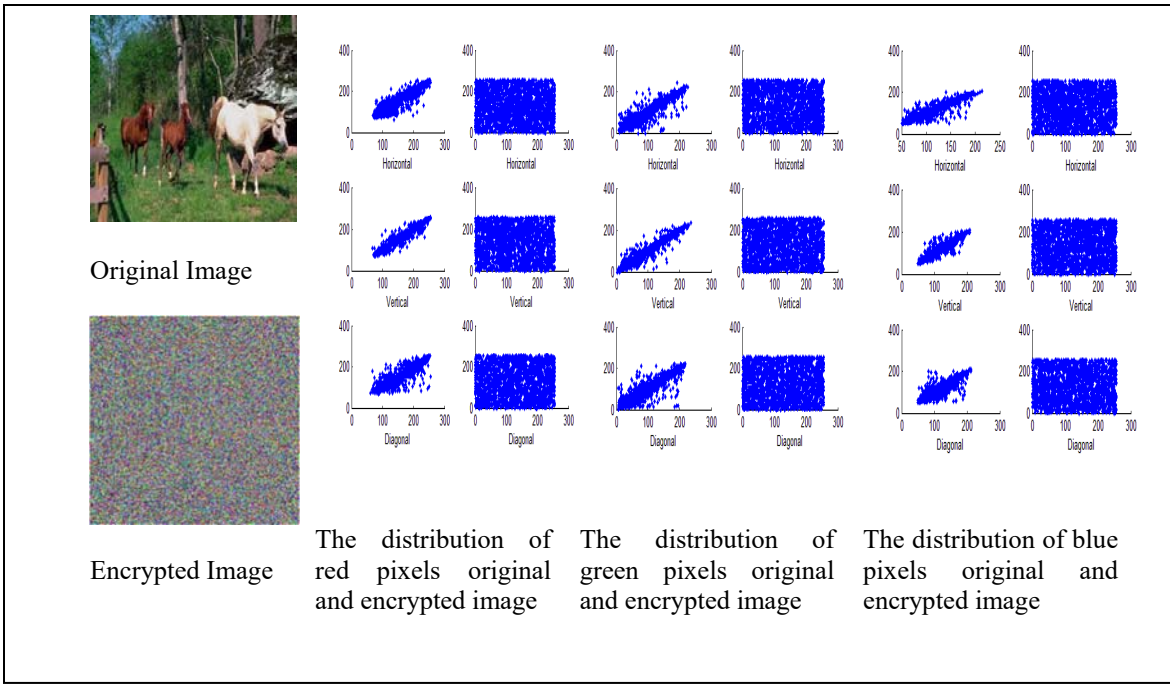


Figure 5(b) Distribution of Pixels in Horses Image Before and After Encryption.

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

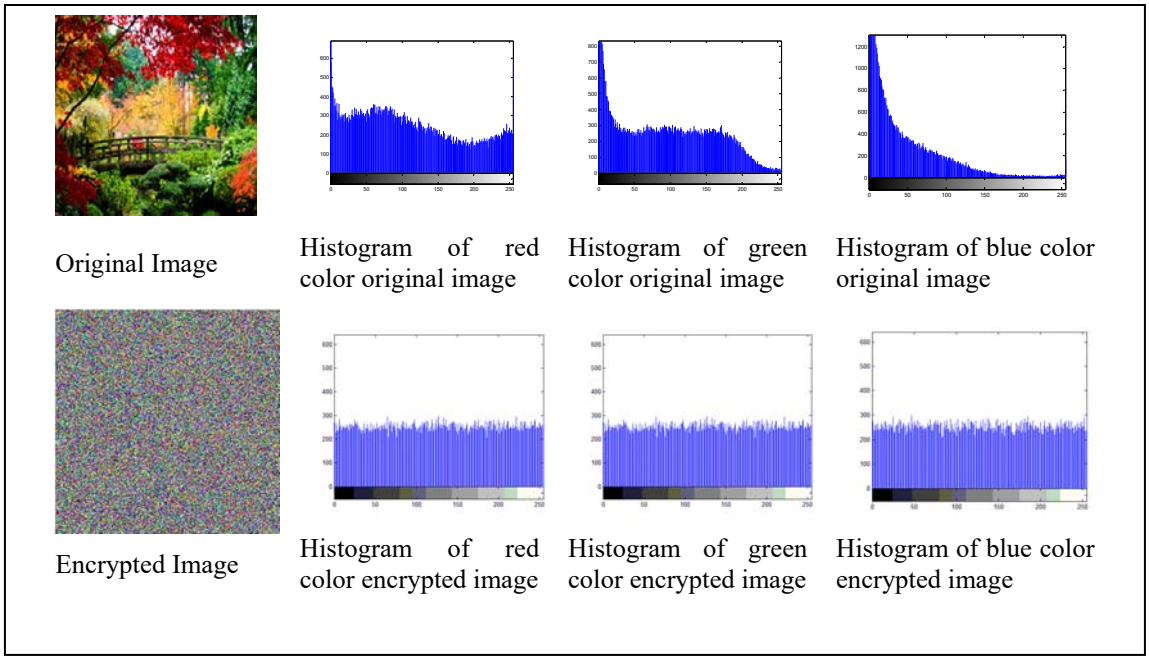


Figure 6(A): Histogram Of Bridge Image Before And After Encryption

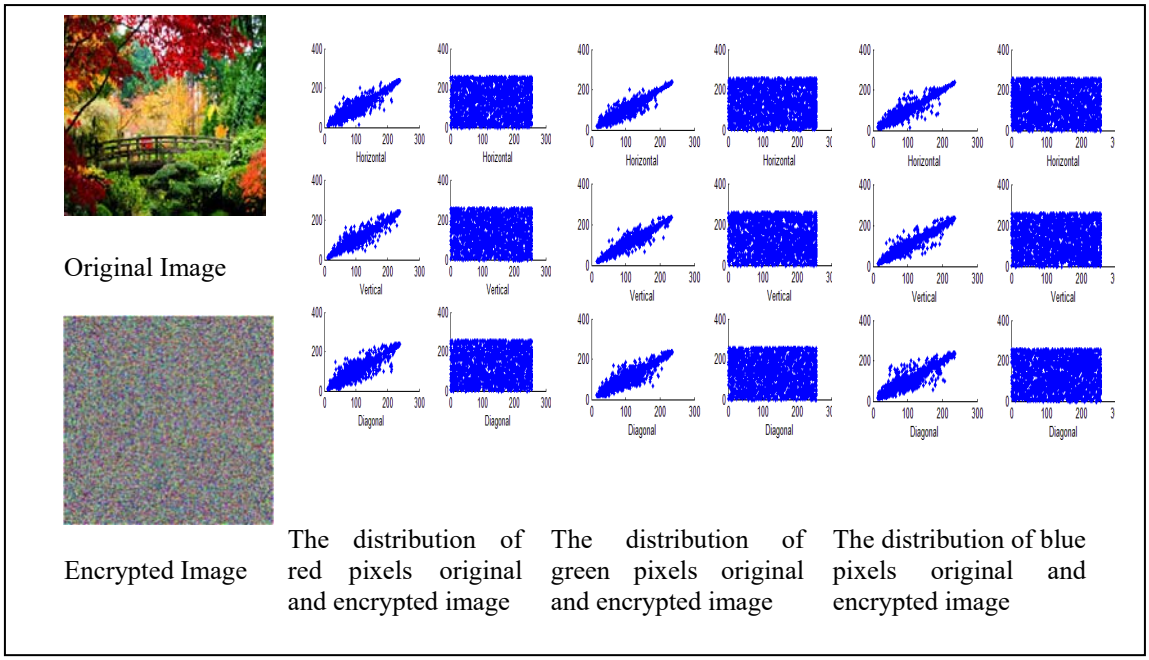
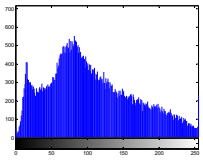
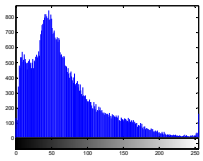
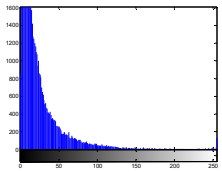


Figure 6(B): Distribution Of Pixels In Bridge Image Before And After Encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195





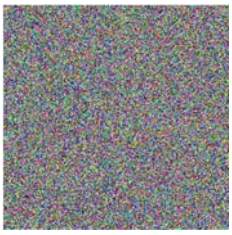


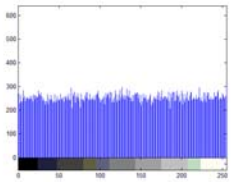
Original Image

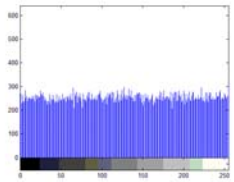
Histogram of red color original image

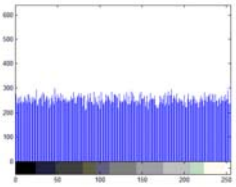
Histogram of green color original image

Histogram of blue color original image









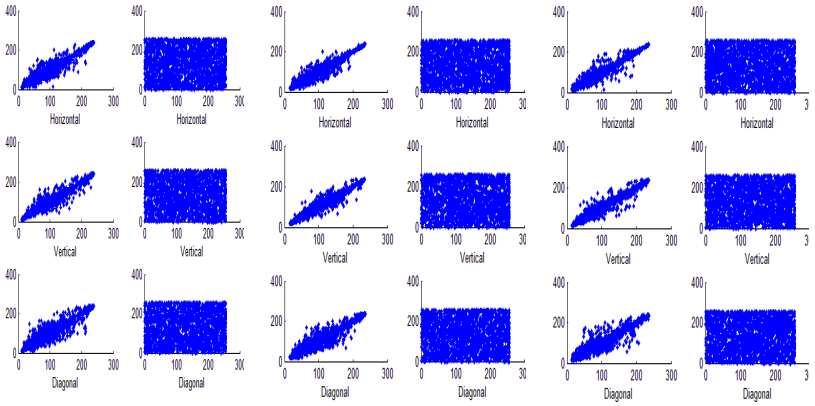
Encrypted Image

Histogram of red color encrypted image

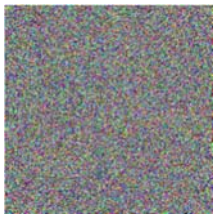
Histogram of green color encrypted image

Histogram of blue color encrypted image

Figure 7 (A): Histogram Of Autumn Image Before And After Encryption.



Original Image



Encrypted Image

The distribution of red pixels original and encrypted image

The distribution of green pixels original and encrypted image

The distribution of blue pixels original and encrypted image

Figure 7 (B): Distribution Of Pixels In Autumn Image Before And After Encryption.

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 8 shows the peak signal to noise ratio (PSNR), the value more than 28 is acceptable and all values are more than 49 as shown in figure.

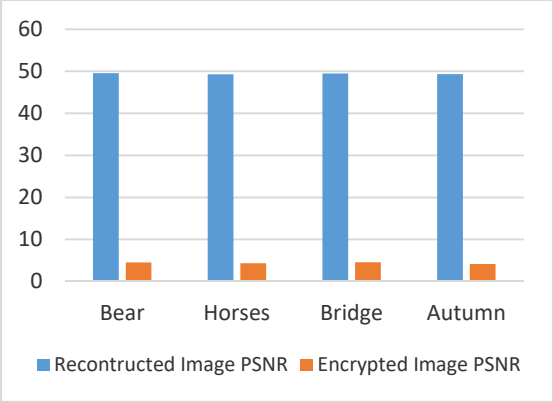


Figure 8 PSNR of Four Tested Image

Figure 9: shows the mean of execution time of each operation in the encryption and decryption stages. The execution time is computed in milleseconds.

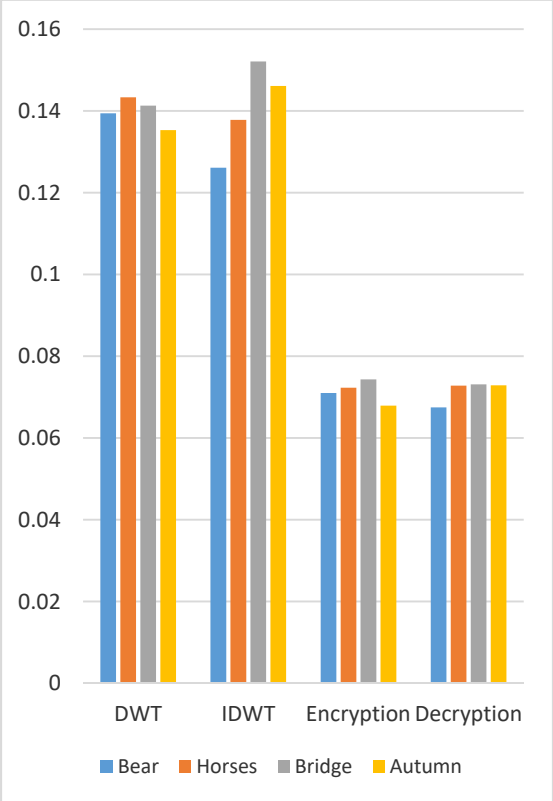


Figure 9: Execution Time for Four Tested Images

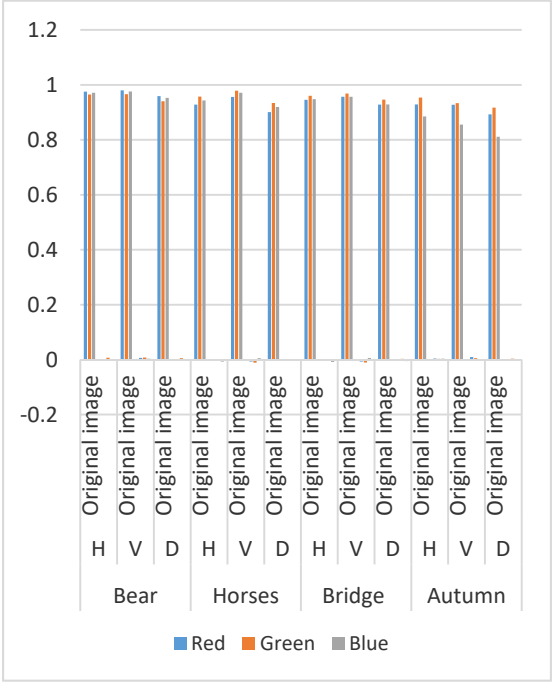


Figure 10: Correlation Coefficient Between Adjacent Pixels.

Figure 11 refers to entropy analysis and the values are near to be eight which indicated very good values referrred to eight bit per pixel. The ideal value of entropy is eight and all values are comparable to eight as shown in figure.

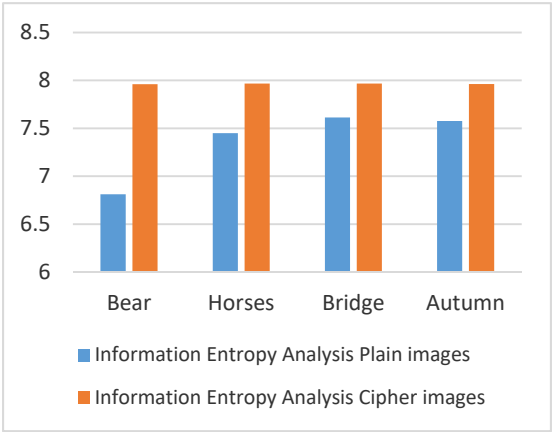


Figure 11: Entropy Analysis

Figure 12 refers to mean square error, the high values in mean that this method gives good results because of the high values of MSE.

Journal of Theoretical and Applied Information Technology
15th June 2018. Vol.96. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

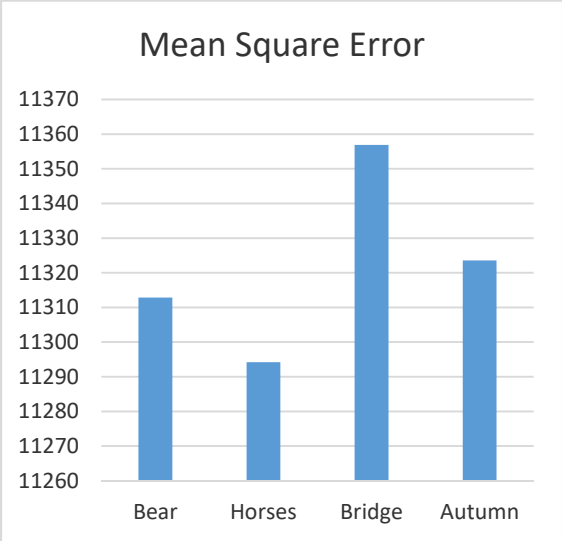


Figure 12: Mean Square Error.

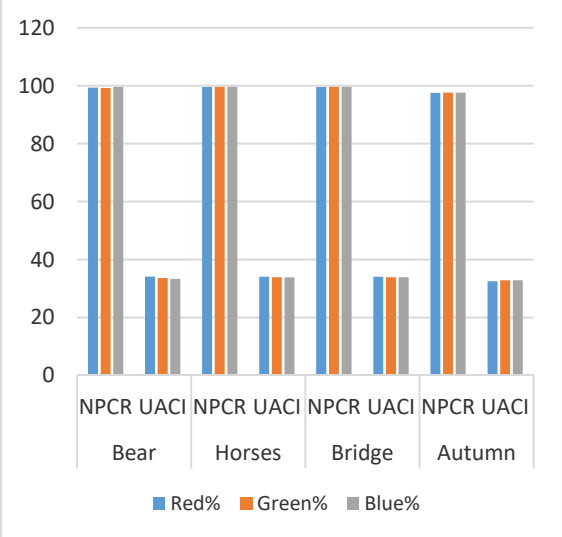


Figure 13: NPCR and UACI of Different Color Components.

8. FEATURES AND LIMITATIONS

The system has been tested and applied to a number of images and the obtained results were good in both encryption and compression. This system indicated high privacy to merging the two processes together to achieve high efficiency for encryption and compression.

As for the limitations, during the work there was little, except that it is possible to obtain some comments in the event of an increase in the volume of data to be hidden, which can be placed in the future work that can be proposed.

9. CONCLUSIONS

Hybridizing both image hiding and image encryption leading to and efficient approach of encryption. An effectiveness of the obtained results offered via applying the proposed image encryption technique. Wavelet transform is used to generate the four required bands and it is able to isolate the most important information (lowest frequency values) to encrypt by AES.

The space of the key is sufficient to protect this method and deny the brute-force attack with high security with high security of encryption influences. The chaotic encryption application provides the use of a secret key as the primitive key to generate a chaotic secret key sequence of a pseudorandom key to encrypt the inactive image blocks LH, HL and HH. This approach is fast enough technique in which the average time of each coding or decoding step is approximately 2.4ms. The reconstructed image has good quality compared to the original image, where the PSNR average is approximately 50 db.

REFERENCES

[1] Matthews, R A J., On the derivation of a chaotic encryption algorithm [J]. Cryptologia. 1989, 13(1): 29-42.

[2] Shannon, C. 1949, Communication Theory of Secrecy Systems. Bell System Technical Journal, Vol.28, Issue 4, pp 656–715.

[3] Baptista, M.S., Cryptography with Chaos, Physics Letters A 240: 50–54, 1998.

[4] Alvarez, G., Li, S., Breaking an encryption scheme based on chaotic baker map. Physics Letters A 352 (12), 2006., 78–82.

[5] Yen, J.C. and Guo, J.I., A New Chaotic Key Based Design For Image Encryption And Decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.

[6] Rahma, A.S. and Yacob, B. Z, Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD), Eng.& Tech. Journal ,Vol. 30 , No.5, 2012

[7] Rahma, A.S. and Ali, M. A., To Modify the Partial Audio Cryptography for Haar Wavelet Transform by Using AES Algorithm, Eng. & Tech. Journal , Vol.32,Part (B), No.1, 2014

[8] Sasidharan, S. and Philip, D. S., "A Fast Partial Encryption Scheme with Wavelet Transform and RC4", International Journal of Advances in Engineering &

Technology(IJAET), vol. 1, no. 4, 2011, pp. 322–331.

[9] Lahieb M. J., Ghazali B. S., A Review Of Color Image Encryption Techniques, IJCSI International Journal of Computer Science, Issues, Vol. 10, Issue 6, No 1, November 2013, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784, www.IJCSI.org

[10] Ancy Mariam Babu and K. John Singh, Performance Evaluation Of Chaotic Encryption Technique, American Journal of Applied Sciences, 10 (1): 35-41, 2013, ISSN: 1546-9239

[11] Geocities, Chaotic Encryption, www.geocities.ws/maheshskm/seminar.pp.

[12] Baker, G.L. and J.P. Gollub, Chaotic dynamics an introduction. First ed. 1990, New York: Press Syndicate of the University of Cambridge.

[13] Alligood, K.T., T.D. Sauer, and J.A. Yorke, Chaos an Introduction to Dynamical Systems. First ed. 1996, New York: Springer-Verlag.

[14] May, R.M., Simple mathematical models with very complicated dynamics. Nature, 1976. 261: p. 459-467.

[15] Wikipedia. Logistic map. [cited February 20, 2009; Available from: http://en.wikipedia.org/w/index.php?title=chaotic_maps&oldid=261864353.

[16] Naess, A., Chaos and nonlinear stochastic dynamics. Probabilistic Engineering Mechanics, 2000. 15: p. 37-47.

[17] Sheng, Y., Wavelet transform. CRC Press LLC, 2000.

[18] Kiselev, A., Fundamentals of the Wavelet Transform Theory [online]. Available at WWW: http://www.basegroup.ru/filtration/intro-towavelets.en.htm, 2004.

[19] Giesl, J., Vlcek, K., Fractal Image Compression using the wavelet transformation. IWCIT 2007 - International Workshop Control and Information Technology, VŠB - Technical University of Ostrava, 2007.

[20] Podoba, T, Giesl, J., and Vlcek, K., Image Encryption in Wavelet Domain Based on Chaotic Maps, 978-1-4244-4131-0/09/©2009 IEEE.

[21] Muzhir Shaban Al-Ani, "Efficient Image Encryption Approach Based on Chaos Technique", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 3 Ver. II (May – June 2017), PP54-60

[22] Abdullah Mohammed Awad, Muzhir Shaban Al-Ani, "Efficient Image Compression Based on Modified Haar Transform", Journal of Theoretical and Applied Information Technology, 15th June 2017. Vol.95. No. 11.

[23] Dr. R. Satya Prasad, Muzhir Shaban Al-Ani, Salwa Mohammed Nejres, "Human Identification via Face Recognition: Comparative Study", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. II (May.-June. 2017), PP 17-22

[24] Muzhir Shaban Al-Ani, "Efficient Image Encryption Approach Based on Chaos Technique", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 3 Ver. II (May – June 2017), PP.54-60