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
www.iosrjournals.org

Efficient Image Encryption Approach Based on Chaos Technique

Muzhir Shaban Al-Ani
University of Human Development, College of Science and Technology, Department of Computer Science, Sulaimani, KRG, Iraq [E-mail: muzhir.al-ani@uhd.edu.iq]

Abstract : *Image encryption is one of the most common and important method of image data encryption. Image encryption deals with applying image encryption algorithms to the sending image and convert it into cipher-image, and only authorized person can decrypt the cipher-image to gent the original image, this done using secret key(s). There are big numbers of encryption techniques including chaos-based schemes, some of them utilize one-dimensional chaotic maps for encryption, and other using two-dimensional or more dimensions chaotic maps. The big challenge in this field is how to generate a cipher-image with smooth normal distribution, in addition that the decrypted image is retrieved with minimum error. The aim of this work is to implement an acceptable image encryption approach to achieve high system performance. The implemented system based on chaos technique in which the original image is divided into parts and then replacing the positions of these parts to form the first level of encryption, then you can go down in the division process at the desired level. The proposed approach is implemented via three steps; flipping, shifting and adding fft operation. This approach achieve a good encrypted image, in addition the retrieved image will be at high performance.*

Keywords : *Image Encryption; Image Decryption; Cipher-Image; Decipher-Image; Chaos Techniques.*

I. Introduction

Recently with the growth of using smart phones, Internet and computer networks, there are vast amount of data, information, images, videos and multimedia daily transmitted via the Internet [1],[2]. These data may be hacked by unknown individuals, so it is very important to save these data against hackers [3],[4]. Now a days data security plays an important part of persons, companies, organizations, countries and also it becomes a part of each system [5],[6]. Due to the Internet development (storage and speed) by introducing advanced technologies, Internet becomes vast store and manipulating of data in all forms [7],[8]. This leads public and private business to go deeply for find an adequate and acceptable method for saving their data [9],[10]. According to these new environments, digital image encryption plays an important role in multimedia security in storing and transmitting of multimedia data [11],[12]. Encryption has been used to facilitate secure data storage and secret communication [13],[14]. Encryption have large number of applications such as governments and militaries in addition encryption is commonly used in protecting of data and information with civilian systems [15],[16]. Encryption is also used to protect transmitted data via networks, Internet, mobile telephones, wireless media, wireless systems, Bluetooth devices and other communication systems [17],[18]. There are many fast encryption algorithms are implemented using different approaches and methods [19],[20]. The main purpose of image encryption is to convert original image into unreadable image and then in the decryption side recovers it back with minimum losses as possible [21],[22]. The encryption system in general (Fig. 1) consists of two main parts; encryption process in which converts the original image (or data) into encrypted image (or data), and decryption process in which the encrypted image (or data) is converted into the original image (or data) [23],[24]. According to this system there is a certain key known only by the authenticated person [25],[26].

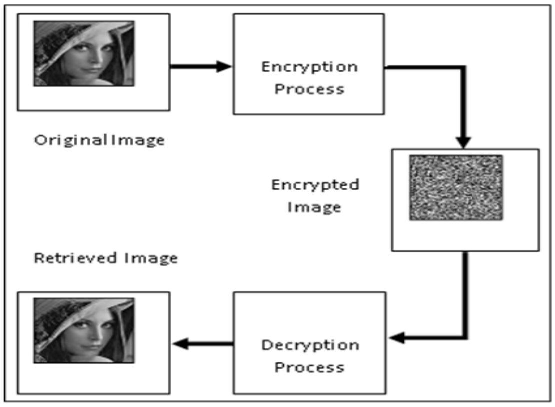


Figure 1 encryption and decryption system

II. Literature Review

This field have big amount of published papers and books, these published works explained different types of encryptions, and below some of these works:

C. Y. Song et al. (2013) introduced a chaotic system using spatiotemporal, they proposed nonlinear chaotic algorithm that defined the local nonlinear map. They proposed an image encryption scheme based on permutation diffusion mechanism. The implemented encryption algorithm based on diffused the plain image with the bitwise applying XOR. Then the chaotic sequence is used to generate the map to permute the pixels of the output image. The chaotic sequence is diffused with the shuffled image. The experimental results indicated that the encryption scheme is high secure and gives high sensitivity and large space [27].

X. J. Tong (2013) presented a chaotic map approach depended on topological aspect, and then improved the characteristics of chaotic. Block Cat map based on multiple-dimensional chaotic map is used to produce a large key space. The permutation–substitution is applied for image encryption approach, then different chaotic maps is used to control each key. Many statistical analysis methods such as entropy, differential, weak-keys, cipher random, and cipher sensibility are used to test the security of the encryption approach. The comparison method of this approach to encryption methods indicated that this approach gave a good solution of the low precision problem in addition it has high speed and high security [28].

J. S. Armand Eyebe Fouda et al. (2014) implemented fast generation of large permutation based round encryption in addition it applied diffusion keys based on sorting of linear Diophantine equation. This approach achieve high security and low computational complexity by both permutation and sorting linear Diophantine equation, then the aspect of updating the integers greater than the permutation is applied.

The evaluation of the performance of the implemented approach using various types of analysis are applied. The obtained results compared with other encryption methods indicated that this approach is secure and fast [29].

M. Zhang and X. Tong (2014) proposed many image encryption algorithms for different image formats such as JPEG, GIF, PNG, and TIFF. The proposed chaotic approach based on dynamic block dividing of the 3D baker, this approach used for diffusion and permutation in encryption. In addition an authentication process is applied using information hiding. Applying these methods deals with high performance output image, in addition the output image can be retrieved without losses. The obtained results indicated that these methods have high speed and high security [30].

W. Zhang et al. (2015) focused on an efficient confusion approach depended on double interpermuting views. This approach based on random exchange strategy in which replace the traditional methods. The histogram distribution, correlation coefficients, speed and security are applied to analyze the efficiency of the system. Applying simulation, this approach leaded to good results that guaranteed the high security and high speed of this approach compared to other available algorithms [31].

L. Mohammed Jawad and G. Sulong (2015) designed a novel secret keys algorithm used for symmetric block cipher based on generating dynamic non-linear, this approach used XOR operation. This proposed approach based on mixing of piecewise chaotic map and logistic methods according to initial values creation. The creation of initial values based on the development of new strategy for seeds creation based on spiral points of sunflower. High advantage of experimental results are obtained via applying the key generator algorithm. An efficient image encryption approach is achieved through correlation coefficient approach to zero and entropy approach to eight. So, high security and strong dynamic secret key are achieved [32].

J. Kumar and S. Nirmala (2016) proposed an effective approach depended on moves of strong pieces to generate a high security image. The big advantage of this approach deals with the replacing of these pieces in parallel and the key sequence generation, this operation based on crossover. This approach is implemented via three stages. First stage deals with the number of pieces which applied in parallel in which is selected automatically. Second stage deals with the random keys generation. An arithmetic crossover operation is applied in order to select points in the second stage. Third stage deals with applying exclusive OR operation that served to produce the encrypted image via the selected position of piece and generated key [33].

C. Sivapong Nilwong and W. San-Um (2016) presented an efficient image encryption approach based on chaotic map method applied for an Android application. An experimental results of bifurcation diagram and spectrum analysis are used to analyze the dynamic properties. The encryption and decryption operations are implemented for Android application. The designed approach based on XOR operation and the key image which is generated from the chaotic map. The system characteristics are evaluated, qualitatively through applying correlation and histogram and then quantitative evaluation of speed and correlation are measured [34].

M. Kumar et al. (2016) introduced a novel image security approach using elliptic curve cryptography based on DNA encoding. The first step of the algorithm started with encoding the RGB image via DNA encoding, then the second step is implemented using asymmetric encryption based on Elliptic Curve. The encrypted image was tested and analyzed using standard forms analysis such as statistical analysis, key spaces and key sensitivity. The obtained analyzed results indicated that the implemented algorithm can resist against exhaustive attacks [35].

D. Xiaoa and L. Wang et al. (2017) implemented an encrypted algorithm to reduce the size of data transmission and resist against different attacks. Firstly, discrete wavelet transform is applied to perform image fusion that generates complete scene images. The obtained images are represented via discrete cosine transform and then sampled using structurally random matrix that realizes the encryption and resize the data. Then combining permutation and diffusion in order to resist noise and crop attack. Then reconstruction and decryption processes are applied to recover the original images at the receiver side. The implemented approach indicated an efficient security and robustness of the system [36].

M. Zhang and X. Tong (2017) proposed an efficient approach for image encryption and compression. This approach is performed via set partitioning in hierarchical trees (SPIHT) and integer wavelet transform (IWT). This approach is focused on combining the characteristics of set partitioning in hierarchical trees (SPIHT) and integer wavelet transform (IWT). The implemented approach indicated that there is no effect on compression performance of the coding process. This approach is applied on various environments to evaluate the security performance. High security and good security performance are obtained from the evaluation of the tested results [37].

S. Koppu and V. Madhu Viswanatham (2017) implemented chaotic cryptosystem for image security via hybrid approach. This approach concentrated on fast image encryption and decryption. The eigenvectors are generated using pseudorandom generator. The proposed approach achieved excellent randomness via pixels shuffled. The proposed approach indicated a good performance compared with other methods when it is tested for different. In addition a better results are obtained with this approach via the simulated results for protecting and complexity [38].

III. Methodology

Image Data Set

In order to start encryption process, it better to prepare the data set which concentrated on image data set. In this approach two image data set are prepared to be tested. First image data set (Slbirc) is stored in 24 bit RGB, JPEG format of size 180*200 (Fig. 2). This image data set having only female face images.

Second image data set (Faces94) is stored in 24 bit RGB, JPEG format of size 180*200 (Fig. 3). This image data set having male and female face images.

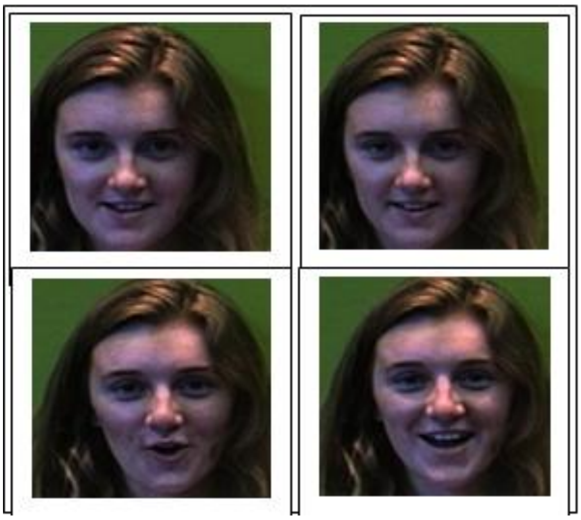


Figure 2 first data set of size 180*200

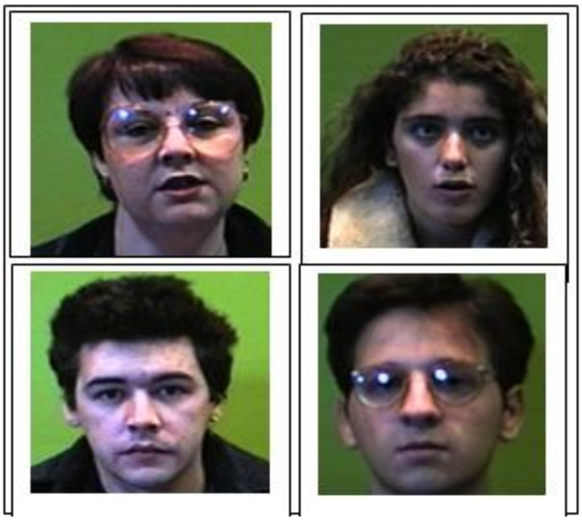


Figure 3 second data set of size 180*200

Encryption Approach

The encryption approach contains many steps as shown in Fig. 4:

- Step one: preprocessing, this step deals with preparing the original image to be processed in the next step. This step including noise removal, enhancement, and resizing.
- Step two: this step deals with converting the image into frequency domain by applying two dimensional fast Fourier transform (2D-FFT).
- Step three: triangular division, this step deals with dividing the image into four quarters and eight triangular as shown in Fig. 5.

- Step four: switching step, this step deals with switching of positions between the pixels of left and right sides as shown in Fig. 6.
- Step five: this step deals with converting the image into frequency domain by applying two dimensional fast Fourier transform (2D-FFT).

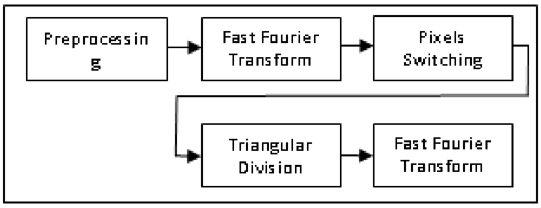


Figure 4 encryption approach

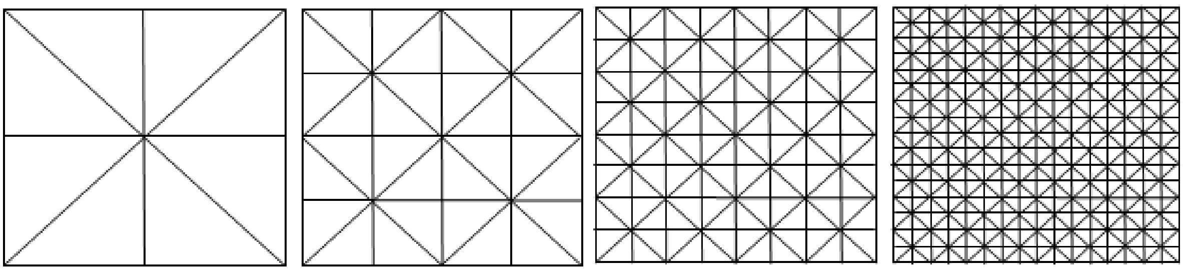
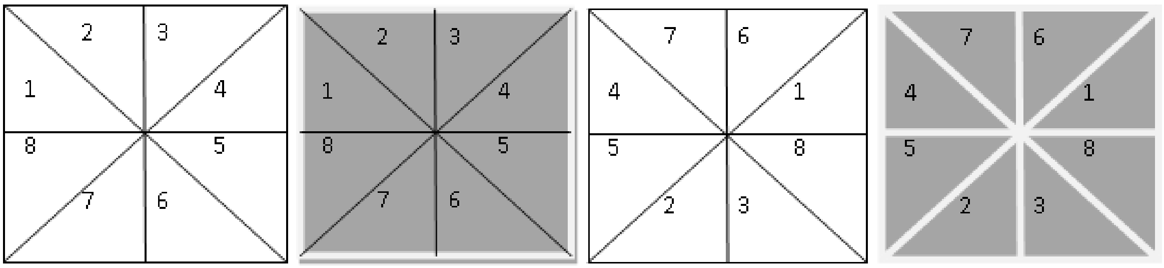

a. 1st level b. 2nd level c. 3rd level d. 4th level

Figure 5 levels of triangular partition



a. partition of image b. applying FFT c. bits switching d. applying FFT

Figure 6 bit switching steps

IV. Results and discussions

The implementation of the image encryption approach is applied to inshore the effectiveness of the obtained results. Two image data set are used to realize this implemented approach. Many steps are applied to perform this system and these steps will be explained below.

- First step; preprocessing step in which noise removing and resizing the original images in order to be ready for processing as shown in Fig. 7. A certain filtering process is applied to remove the unwanted noise from the original image. The resizing process is operated to uniform all the images to be of the size 256*256.
- Second step; these color images are converted into gray scale as shown in Fig. 8.

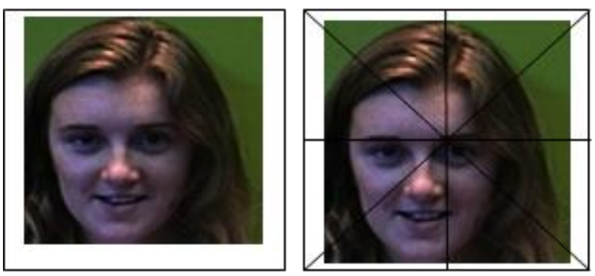


Figure 7 original color image and partitions

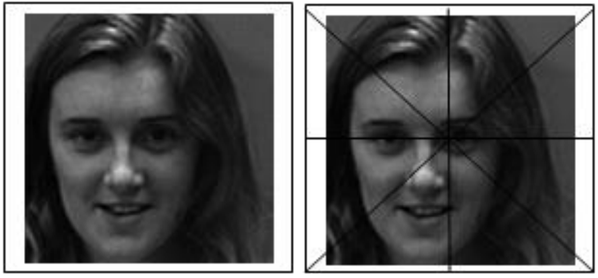


Figure 8 gray image and partitions

- Step three; applying fast Fourier transform to get the spectrum of image as shown in the first part of Fig. 9.
- Step four; applying triangular division as shown in the second part of Fig. 9.

- Step five; applying pixel switching of the nearby positions. This step is applied to destroy the image details. In addition that this step can be repeated until reach a good encrypted image.

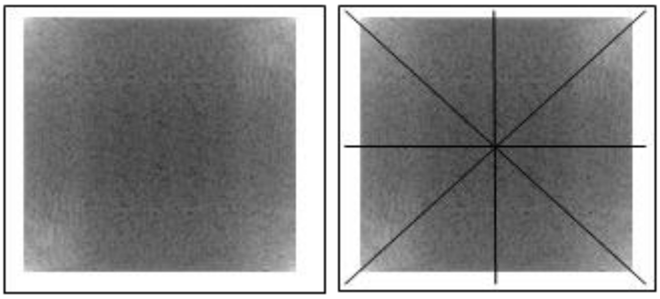


Figure 9 image after applying fft and partitions and partitioning

The MSE and PSNR are used to measure the quality of an image after the reconstruction. As an evaluation step we measure PSNR, MSE and MAXERR between the original image and the retrieved image as below:

- MSE is the mean square error between the original image and the retrieved image.
- PSNR is the peak signal-to-noise ratio in decibels (dB).
- MAXERR is the maximum absolute squared deviation of the original image and the retrieved image.

The tested images are passed through three phases. First two steps applying flipping operation and shifting operations respectively. Table 1 and Table 2 illustrated the results of PSNR, MSE and MAXERR. The tested image indicated that the values MSE and MAXERR are approach to zero, but the values of PSNR are approach to infinity. These simple and easy methods approximately have no indicated error in the implementation. The third step is applying fft after the previous two steps. Table 3 demonstrate the values of PSNR, MSE and MAXERR after applying fft. The error appears after applying fft is so small and can be neglected. More details of adding fft of the two above steps for PSNR, MSE and MAXERR are demonstrated in Figs. 10, 11 and 12.

T**able 1** Retrieved images after flipping

Retrieved Images	PSNR	MSE	MAXERR
Image1	∞	0	0
Image2	∞	0	0
Image3	∞	0	0
Image4	∞	0	0
Image5	∞	0	0

Table 2 Retrieved images after sifting

Retrieved Images	PSNR	MSE	MAXERR
Image1	∞	0	0
Image2	∞	0	0
Image3	∞	0	0
Image4	∞	0	0
Image5	∞	0	0

Table 3 Retrieved images after fft

Retrieved Images	PSNR	MSE	MAXERR
Image1	327.7398	1.0942e-028	5.6843e-014
Image2	327.0384	1.2860e-028	5.6843e-014
Image3	325.7128	1.7450e-028	8.5265e-014
Image4	326.3460	1.5083e-028	8.5265e-014
Image5	327.1111	1.2646e-028	5.6843e-014

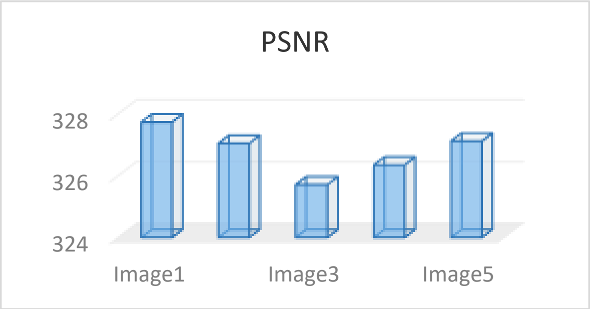


Figure 10 Peak signal to noise ratio after fft step

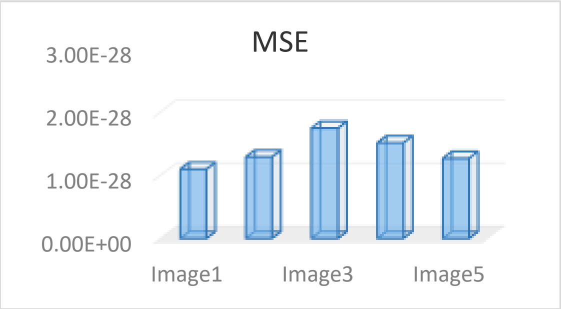


Figure 11 Mean square error after fft step

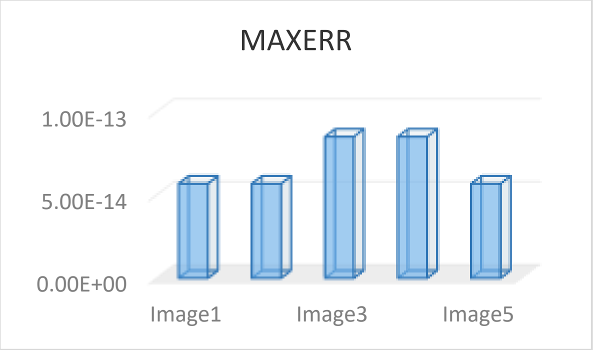


Figure 12 Maximum error after fft step

V. Conclusion

The field of image encryption occupies big amount of applications and play an important part of data encryption. An efficient image encryption approach is implemented to achieve a good performance. Two types of image data set are used to evaluate this approach. Two mixed techniques are applied in this approach to reach a good performance of encryption. The mixing between fast Fourier transform and switching between neighbors of pixels. This leads to an efficient powerful approach. In addition that this approach is simple and easy to apply all types of images. The obtained results of the flipping and shifting indicated mean square error of the retrieved image approach to zero and peak signal to noise ratio approach to infinity. On the other hand by adding fft step appeared a very small value of error.

VI. References

[1] K. Murali, Yu. Haiyang, V. Varadan, H. Leung, “Secure Communication Using a Chaos Based Signal Encryption Scheme” Consumer Electronics, IEEE Transactions on Vol. 47, Issue 4, 2001, pp. 709-714.

[2] W. Zhu, Y. Shen, “Encryption Algorithms Using Chaos and CAT Methodology” Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference, 2010 , pp. 20 – 23.

[3] V. Patidar, N. K. Pareek , G. Purohit, and K. K. Sud , “A Robust and Secure Chaotic Standard Map Base Pseudorandom Permutation Substitution Scheme for Image Encryption,” Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.

[4] A. Awad, S.E. Assad, and D. Carragata, “A Robust Cryptosystem Based Chaos for Secure Data,” IEEE Int. Symp. Image/Video Commun. over Fixed Mobile Networks, Bilbao, Spain 2008.

[5] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image Compression and Encryption Scheme Based on 2D Compressive Sensing and Fractional Mellin Transform, Opt. Commun. 343 (2015) 10–21.

[6] A. Alfalou, C. Brosseau, Optical Image Compression and Encryption Methods, Adv. Opt. Photonics 1(3) (2009).

[7] Yupu Dong; Jiasheng Liu; Canyan Zhu; Yiming Wang; “Image Encryption Algorithm Based on Chaotic Mapping” Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Vol.1, 2010 , pp. 289–291.

[8] N. Zhou, A. Zhang, J. Wu, D. Pei, Y. Yang, Novel Hybrid Image Compression and Encryption Algorithm Based on Compressive Sensing, Optik 125 (2014) 5075–5080.

[9] S. Behnia, A. Akhshani , H. Mahmodi, and A. Akhavan, “A Novel Algorithm for Image Encryption Based on Mixture of Chaotic Maps, ”Chaos Solit . Fract., vol. 35, no. 2, pp. 408–419, 2008.

[10] D. Yang et al., “A Novel Block Cryptosystem Based on Iterating Map with Output Feed Back,” Chaos, Solutions and Fractals, vol. 41, 2009, pp. 505-510.

[11] Li. Chengqing, “On the Security of a Class of Image Encryption Scheme”, IEEE International Symposium on Circuit & System ,2008 ISCAS, Department of Electronics Engineering, University of Hong Kong , pp. 3290-3293.

[12] A. Jolfaei, A. Mirghadri, “An Image Encryption Approach Using Chaos and Stream Cipher” Journal of Theoretical and Applied Information Technology 2010.

[13] T. Xiang et al., “A Novel Block Cryptosystem Based on Iterating a Chaotic Map,” Phys. Lett. A, vol. 349, 2006, pp. 109-115.

[14] Q. Wang, Q. Ding, Z. Zhang, L. Ding, “Digital Image Encryption Research Based on DWT and Chaos” Natural Computation, 2008. ICNC '08. Fourth International Conference Vol. 5, 2008, Pages 494–498.

[15] G. J. Zhang, Q. Liu, ”A Novel Image Encryption Method Based on Total Shuffling Scheme” Optics communications, 284, pages. 2775-2780 (2011).

[16] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, Y. Yu, Chaos Based Digital Image Encryption Scheme With an Improved Diffusion Strategy, Opt. Express 20 (3) (2012) 2363–2378.

[17] P. Raviraj and M. Y. Sanavullah, “The Modified 2D Haar Wavelet Transformation in Image Compression” Middle East Journal of Scientific Research, Vol. 2, Issue: 2, pp. 73-78, Apr-Jun, 2007.

[18] T. Acharya, C. Chakrabarti, A Survey on Lifting Based Discrete Wavelet Transform Architectures, Journal VLSI Signal Process. 42 (2006) 321–339.

[19] H. S. Kwok and W. K. S. Tang, “A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation,” Chaos Solit. Fract., vol. 32, no. 4, pp. 1518–1529, 2007.

[20] K. W. Wong, B. S. H. Kwok, and W.S. Law, “A Fast Image Encryption Scheme Based on Chaotic Standard Map,” Phys. Lett. A, vol. 372, no. 15, 2008, pp. 2645-2652.

[21] R. B. Lee, Z. Shi, and X. Yang, “Efficient Permutation Instructions for Fast Software Cryptography,” IEEE Micro, vol. 21, no. 6, 2001, pp. 56-69.

[22] D. Kong, X. Shen, Multiple Image Encryption Based on Optical Wavelet Transform and Multichannel Fractional Fourier Transform, Opt. Laser Technol. 57 (2014) 343–349.

[23] V. Chappelier, C. Guillemot, Oriented Wavelet Transform for Image Compression and Denoising, IEEE Trans. Image Process. 15 (10) (2006) 2892–2903.

[24] Y. Zhou, L. Bao, C.L.P. Chen, Image Encryption Using a New Parametric Switching Chaotic System, Signal Process. 93 (11) (2013) pp. 3039–3052.

[25] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, O.R. Acosta Del Campo, A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos, Signal Process. 109 (2015) pp. 119–131.

[26] S. Lian, J. Sun, Z. Wang, A Block Cipher Based on a Suitable Use of Chaotic Standard Map, Chaos Solitons Fractals 26 (1) (2005) pp.117-129.

[27] C. Y. Song, Y. L. Qiao, X. Z. Zhang, "An Image Encryption Scheme Based on New Spatiotemporal Chaos", Optik 124 (2013) pp. 3329– 3334.

[28] X. J. Tong, "Design of an Image Encryption Scheme Based on a Multiple Chaotic Map", Commun Nonlinear Sci Numer Simulat 18 (2013) pp. 1725–1733.

[29] J. S. Armand Eyebe Fouda, J. Yves Effa, Samrat L. Sabat, Maaruf Ali, "A Fast Chaotic Block Cipher for Image Encryption", Commun Nonlinear Sci Numer Simulat 19 (2014) pp. 578–588.

[30] M. Zhang, X. Tong, "A New Chaotic Map Based Image Encryption Schemes for Several Image Formats", The Journal of Systems and Software 98 (2014) pp. 140–154.

[31] W. Zhang, H. Yu, Z. L. Zhu, "Color Image Encryption Based on Paired Interpermuting Planes", Optics Communications 338 (2015), pp. 199-208.

[32] L. Mohammed Jawad, G. Sulong, "A Novel Dynamic Secret Key Generation for an Efficient Image Encryption Algorithm", Modern Applied Science; Vol. 9, No. 13; 2015, pp. 85-97.

[33] J. Kumar, S. Nirmala, "A Novel and Efficient Method Based on Knight Moves for Securing the Information Contents of Images: A Parallel Approach", Journal of information security and applications 30 (2016) pp. 105–117

[34] C. Sivapong Nilwong, W. San-Um, "An Image Encryption Scheme and Its Android Application Using Robust Chaotic Map with Absolute Value Nonlinearity", ITMSOC Transactions on Information Technology Management 01 (2016) pp. 26–32.

[35] M. Kumar, A. Iqbal, P. Kumar, "A New RGB Image Encryption Algorithm Based on DNA Encoding and Elliptic Curve Diffie Hellman Cryptography", Signal Processing, 125 (2016) pp. 187–202.

[36] D. Xiaoa, L. Wang, Tao Xiang, Yong Wang, "Multifocus Image Fusion and Robust Encryption Algorithm Based on Compressive Sensing", Optics & Laser Technology 91 (2017) pp. 212–225.

[37] M. Zhang, X. Tong, "Joint Image Encryption and Compression Scheme Based on IWT and SPIHT", Optics and Lasers in Engineering 90 (2017) pp. 254–274.

[38] S. Koppu, V. Madhu Viswanatham, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based onHybrid Chaotic Magic Transform", Hindawi Publishing Corporation, Modelling and Simulation in Engineering, Published 4 January 2017, Article ID 7470204, pp.1-12.