JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AN EFFICIENT IMAGE ENCRYPTION APPROACHE MODIFIED DISCRETE WAVELET DOMAIN USING STEGNOGRAPHY

Alaudeen.B.M[1]., Dr.G.Tholkappia arasu[2]

Research Scholar[1], Associate Professor[2]

Manonmaniam Sundaranar University, Tirunelveli[1]., AVS College of Technology, Salem[2]

Abstract: The wavelet algorithms are applying the high level of image/data compression by using transforms. The main processes of wavelets are allowing some complex information such as images and videos to be decomposed into elementary forms. These processes are applied at different positions and balancesto rebuild with high precision. Signal transmission depends on the transmission of a progression of numbers. The series portrayal of capacity is significant in a wide range of sign transmission. The wavelet portrayal of capacity is another strategy. Wavelet change of a volume is the improved variant of Fourier transform. This chapter discusses more on applying an encryption standard by modifying the Discrete Wavelet Domain (DWT). In this work, the performance of modified DWT image encryption algorithms is measured and equated using the computation time. The entropy of the process determined the Randomness and provides how secure the image is encrypted. In this paper, we approach this issue by building up a scientific model for obviously scrambled pictures and afterward determine expectations and differences of NPCR and UACI metrics. Further, these hypothetical qualities are utilized to frame measurable theory NPCR and UACI tests. Basic estimations of tests will help in predicting an encryption standard. Thus, the topic of whether a given NPCR/UACI score is adequately high to such an extent that it isn't noticeable from ideally encoded pictures is replied by observing at real NPCR/UACI scores with comparing basic qualities. Test results utilizing the NPCR and UACI irregularity tests will determine the existing encryption techniques are really equivalentor not.

Keywords: Number of Changing Pixel Rate, Unified Averaged Changed Intensity, Discrete Wavelet Domain

Introduction

The computerized watermark can be named dynamic watermark, delicate watermark, and semi-delicate watermark. The vigorous watermark endures when the watermarked advanced content is seriously assaulted and hence can be applied in copyright assurance. Then again, the delicate watermark will be pulverized regardless of whether the adjustment in the checked computerized media is minute. By reason of this property, picture validation turns into a forthcoming utilization of it. As a tradeoff of heartiness and delicacy, a semi-delicate watermark that can oppose content preserving activities, (for example, JPEG pressure) and be touchy to content

altering changes, (for example, include substitution) is increasingly practicable than delicate watermark in picture confirmation. Figure 1 explain the proposed system architecture diagream (Al-Haj., 2007).

Delicate or semi-delicate watermarking plans dependent on ordinary DWT have been accounted for during the most recent couple of years. Alter identification at multi-goals had been accomplished. Be that as it may, it abuses the idea of the human visual framework. It carries distinguishable twisting to the watermarked pictures. Noxious alter has a huge difference while spontaneous alter has little variation. They inserted mark dependent on regulating the mean of certain coefficients rather than singular coefficients (Lagzian et al., 2011).

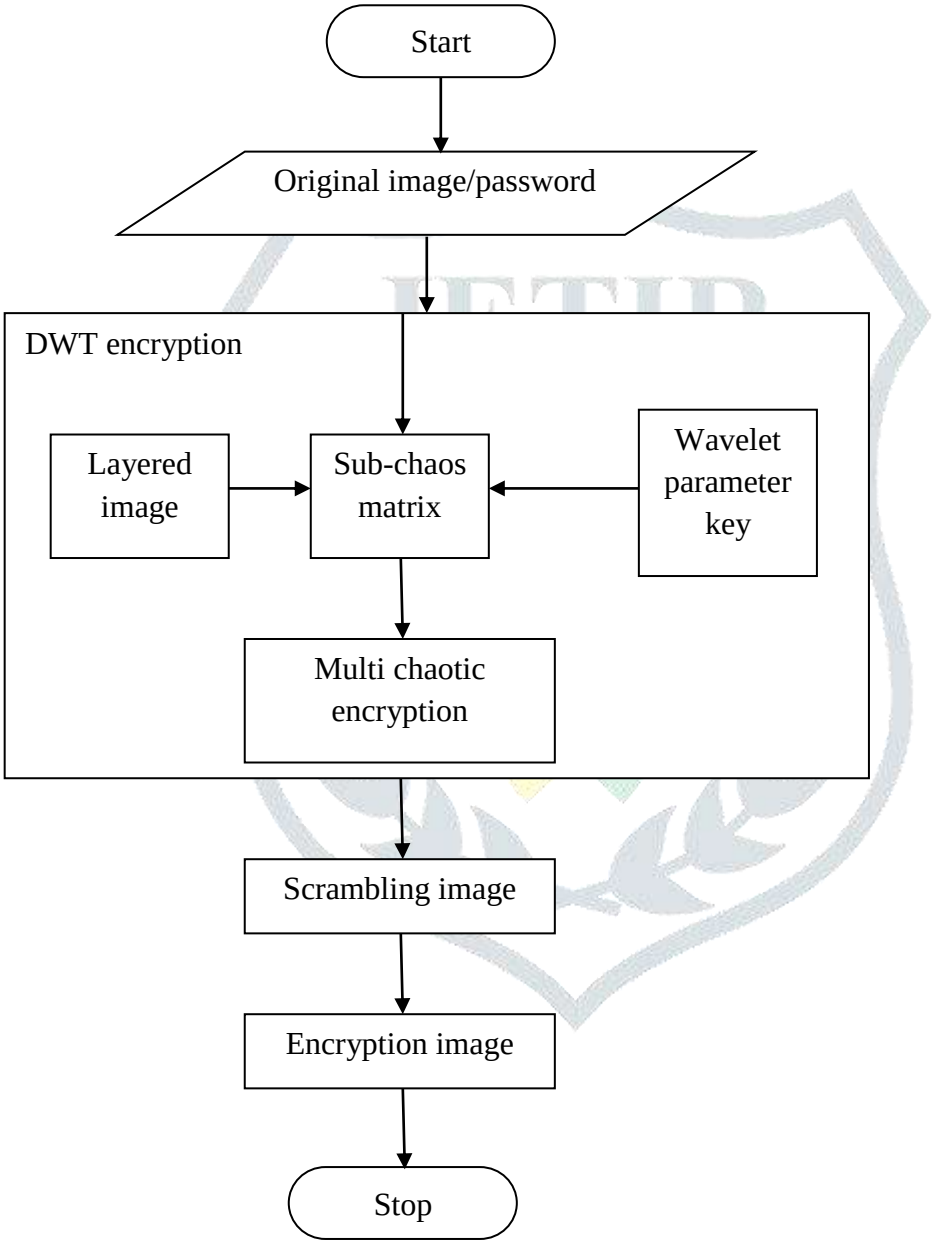


Figure 1: Flow chart for DWT encryption standard

Most traditional DWT based delicate or semi-delicate watermarking plans announced in the writing have three deficiencies(Deb.K et al., 2012):

(1) Insecurity. The plans utilized just a single wavelet base to play out the DWT. When the calculation was taken by an assailant, the covered-up data bits might be uncovered or changed without any problem.

(2) Low strength to JPEG.

(3) High computational multifaceted nature. Contrasted with DCT (discrete cosine change), customary DWT has a less computational cost.

Finally, the instance of an image having a huge size, it is as yet difficult when DWT applied to an entire picture.

A possible strategy to improve security is to pick a wavelet base from a lot of wavelet bases by parameters. In the event that the parameter space is sufficiently huge, it is outlandish for the aggressor to get the helpful data in this way ensures additional security. Be that as it may, his plan is still in view of ordinary DWT. A lifting plan is a compelling technique to improve the preparing pace of DWT (sivanantham kalimuthu, 2021).

The general design of the tumultuous based picture encryption frameworks normally comprises of the cycle of two stages (I) change and (ii) distribution. The variation is accomplished by scrambling all the pixels all in all utilizing 2D disorderly maps. In the distribution stage, the pixel esteems are modified successively and the change made to a specific pixel relies upon the amassed impact of the entire past pixel values. In any case, the same number of rounds of stage and dissemination or emphases should be taken; the general encryption speed is moderate (Wang.Y et al., 2011).

Literature review

A brief review of the literature based encryption plans is given. To stand up to brute-force assaults the keyspace is expanded by utilizing various tumultuous maps. Sam et al., (2012) proposedimage encryption dependent on intertwining disorderly maps to upgrade security and key length. They proposed a symmetric encryption plot dependent on a cyclic elliptic bend and disorderly framework, which encodes 256-piece of the plainimage to 256-piece of cipherimage inside eight 32 piece registers. Ye and Wong (2012) proposed image encryption conspire with summed up Arnold map, as the keystream relies upon the handled picture the strategy can oppose known-and picked plain content assaults. Inventors proposed a gray level encryption plan to dispose of picture diagrams and to upset the distributional qualities of the dim level.

In, the computational time is diminished by scrambling huge information in the spatial area and inconsequential information in wavelet space. Huang (2012) proposed encryption conspire dependent on tumultuous Chebyshev generator with various changes to upgrade the decorrelation. They proposed image encryption with a circle map and are safe against differential attacks. In, anencryption order of 2-D piecewise nonlinear chaotic maps with an invariant measure is presented. In, an encryption plot in light of enormous pseudorandom change is proposed, which is combinatorially created from little change lattices in light of chaotic maps.

The author's kalimuthu et al (2021) explained, DWT is considered for an enhancement to break down an image and combine the hypothesis of an image sharing to reproduce the change coefficients, and afterward, utilize the networks for encryption produced by a tumultuous framework with the nonlinear component. The encryption frameworks are delicate to the underlying state and framework parameters with factual qualities of background noise, Fouda et al., (2014) randomness and interim ergodic property, which are truly reasonable to image encryption, Jolfaei and Mirghadri (2010).

System design

By discrete wavelet transform of the unique picture, separate the low recurrence part as installed space; utilize the created chaotic arrangement to encode the encryptedimage, at that point wavelet change the scrambled picture and concentrate the low recurrence; at long last, insert the removed low recurrence of the encrypted image into the low recurrence of the first picture. So the image encryption handling is finished. HereChaos encryption of originalimage is done and by the inserting of the encoded watermarking image, a twofold encryption is accomplished. Irrespective of whether the code breaker can extract the original image with respect of the encoded key.

Initially, the original image is converted processed to DWT decomposition to generate the LL_1, LH_1, HL_1 and HH_1. Then, displace the LL_1 level multiplying with the co-efficient, (LL_1=LL_1 * LH_1 * HL_1*HH_1). Later, the second level DWT decompositions are applied over LL_1 in order to generateLL_2, LH_2, HL_2, HH_2 coefficients. Then, displace the LL_2 level multiplying with the co-efficient, (LL_2=LL_2 * LH_2 * HL_2*HH_2). The process of approximating the DWT coefficients by dividing the image dimension, LL_2 = LL_2/(M*N). The reverse process of the above levels will be resulted as (-LH_2, -HL2, -HH2). With the help of displacing second coefficient HH_2 with LL_2 and HL_2 with LH_2. Repeat the above steps until it reaches the secure key generation. The obtained processes are again reflected by using Inverse DWT and do multiplication with a chaotic matrix to form an encrypted image.

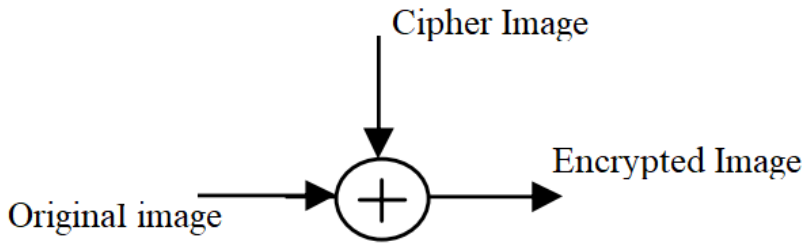


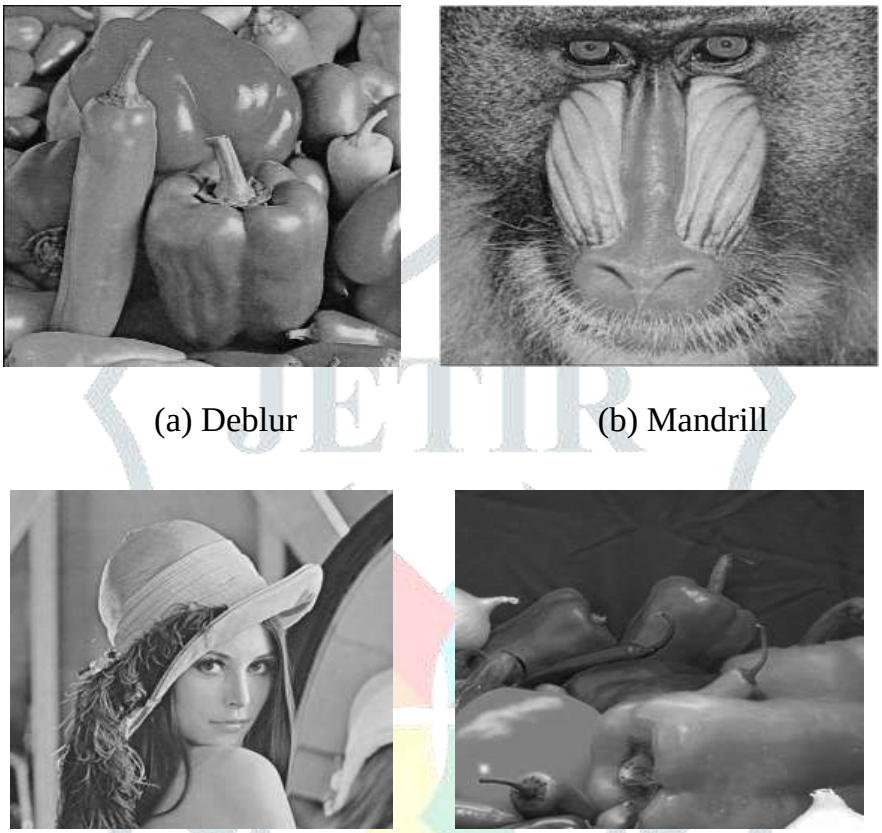
Figure 2 Encryption frame for the proposed method

The Binary Grey Scale Image is processed with the XOR-logic of cipher image to form an encryption image. Gong et al., (2016) stated that the quantum image encryption process is framed based on the XOR operations. Its essential acceptability is that it is easy to execute and that the XOR activity is computationally cheap. A directrepeating XOR (for example utilizing a similar key for XORprocess overall information) figure is in this way once in a while utilized for concealing data in situations where no specific security is required. Figure 2 explain proposed method Encryption frame.

The main motive of the research is to hide the practice of concealing messages or information in image format. In this proposed method, the Binary Greyscale image in the modified discrete wavelet domain is adopted for securing the image from the attackers. The adoption of the crystal payload concept is because of its granular control over the source. This will help in providing the encryption and decryption of an image. The storage of the management cannot read the original payload data. Without the key, it is very difficult to decrypt the original image hence it is more efficient. Inverse rearrange the positions of image pixels: Transformed the encrypted binary image into 1-D sequence, used the same keys for encryption to generate the chaotic sequence, performed inverse rearrange the positions of image pixels. Inverse bit-level permutation: According to the principle of bit-level permutation to inverse diffuse the values of image pixels, get a bits matrix

Result and discussion

To execute and check the performance of an encryption algorithm, this research used MATLAB to simulate this algorithm. Considered four binary grayscale images as experimental images, they were the binary images of Deblur, Mandrill, Lena, and peppers. Figure 3 represents the Grayscale input image standard**.**



(a) Deblur (b) Mandrill

(c) Lena (d) peppers

Figure 3 Binary Grayscale input image-standard

The histogram replicates the image statistical distribution. This will help in analyzing the statistics analysis attack. As shown in Figure 4.8, the histograms of the original image are encrypted and retrieved back the original image. It will be helpful in differentiating those two images. From Fig. 4, the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the histogram of the original image. Therefore, the encrypted image does not provide any clue to those attackers/hackers on the proposed image encryption procedure. The proposed MDWT in encryption makes statistical attacks more difficult.

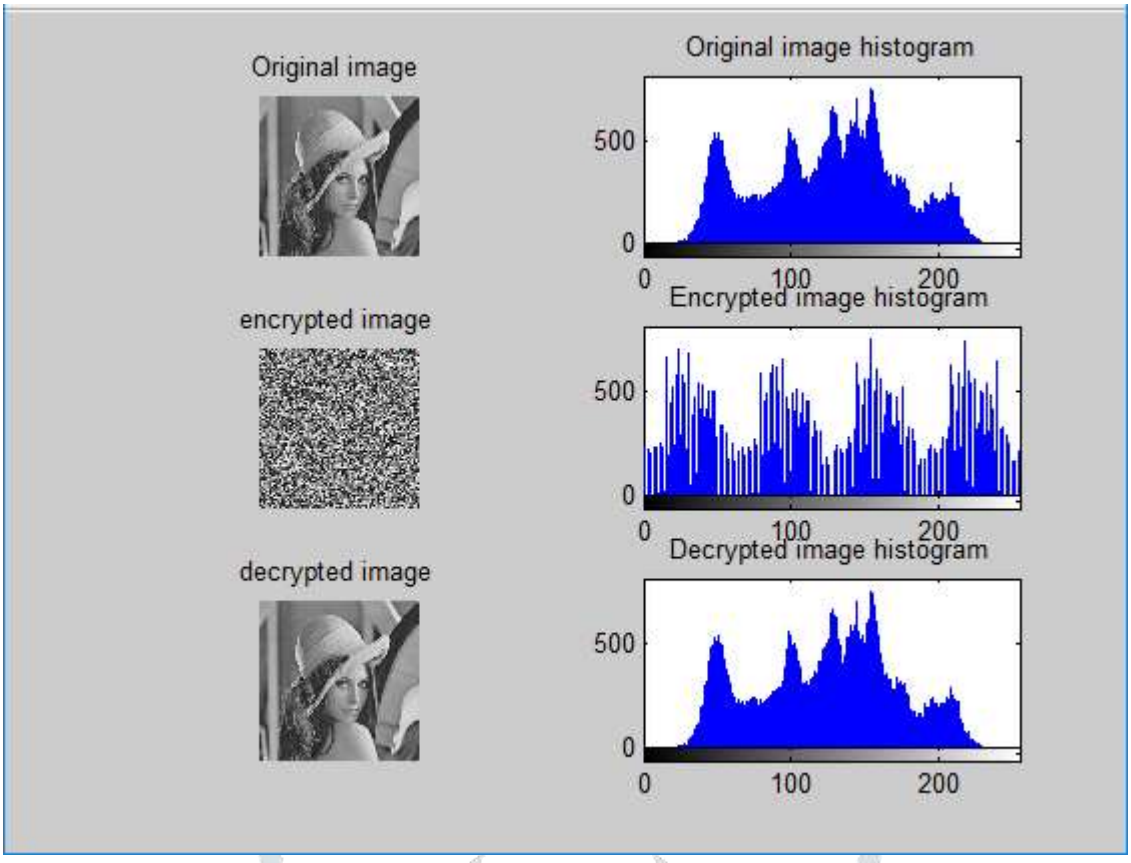


Figure 4 Original image, encrypted image and decrypted images of Lena

From the experimental results, the encrypted images have completely changed the characteristics of the original images, and there is no difference between the decrypted images and the original images in the visual, the purpose of image encryption has been achieved. Each stage of the encryption and decryption process are shown in Figures 5 and 6 for Lena's image respectively. The Secret-key level of the encrypted image can be accomplished since the algorithm has eightlevels of transformation.

Figure 5 Different levels of Lena image encryption

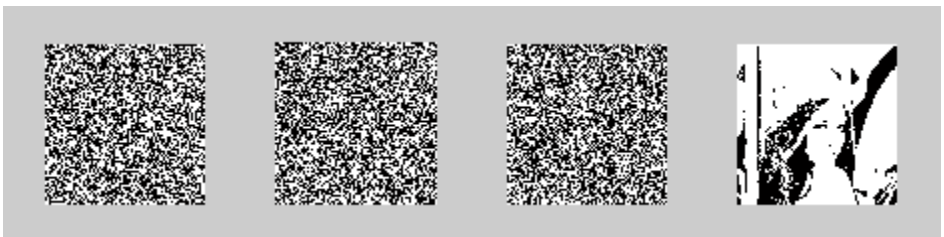


Figure 6 Different levels of Lena image Decryption

The encryption and decryption process of the Mandrill grayscale image is shown in Figure 4.12 and 4.13. Based on the encrypted image, the decrypted images will be retrieved. Since, it may contain the visual information of the original binary image even though they contain noises. The investigational result demonstrates that the encryption strategy shows greater execution within the sight of noise assaults. The encoded images can be recovered when exposed to noisy situations. The encryption must be separatedwith a Secret sharing, which is a method in which the keys of cryptographic results are divided into several subsets without increasing any confidentiality risks.

Comparing the results of figure 4, it is found that the histogram of the encrypted image obtained by MDWT is fairly uniform and is significantly different from that of the original and the encrypted image produced. The encryption algorithm MDWT has covered up all the security key of the grayscale image and has complex the statistical relationship between the grayscale image and the cipher version. Thus the encrypted images produced by MDWT transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attack. The information and entropy analysis observations are displayed in Table 1.

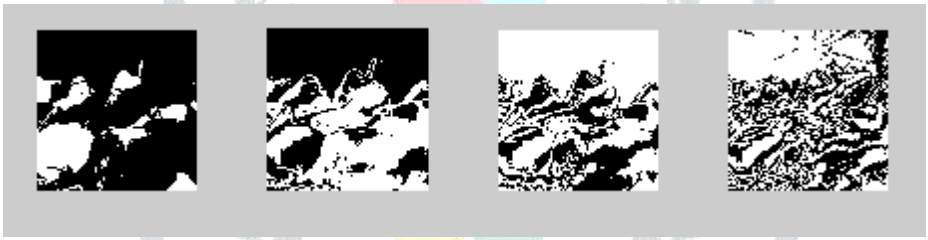


Figure 7 Peppers encryption process

Table 1 Information and Entropy Analysis

Deblu1		**Mandril1**		**Lena1**		**Peppe1**	
Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
6.810	7.33	6.99	7.68	7.108	7.591	7.0545	7.98

Table 2 Entropy Analysis of Image

Parameters	Deblu1	Mandril1	Lena1	Peppe1
NPCR (%)	99.50	99.55	99.56	99.55
UACI (%)	31.518	31.52	31.54	31.50

The NPCR and UACI are the two most significant quantities that quantify the strength of encryption algorithms. The NPCR determines the measure of a total number of pixels change rate and UACI calculates the average change of color intensities between two images when the change in one image is subtle.

Conclusion

The proposed Modified Discrete Wavelet Transform (MDWT) algorithm in this paper encrypts image pixel values and pixel locations according to the basic idea of image encryption. The binary grayscale image is processed by multichaos and pixel scrambling that utilized the Discrete Wavelet Transform (DWT) for pixel encryption. The main objective of the research is matched through the image sparsity and multi-resolution property of the wavelet transform. The proposed MDWT helps in hiding the property of the image and increases the security features. The overall merits of this implementation is achieved and tested by observing the Entropy of each image. The experimental outcome showed that the Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) is high, and then it is not visible to that of the encrypted image. Hence, it is inferred as high resistance to differential attacks and maintains security.

References

1. Kalimuthu, S., Naït-Abdesselam, F., & Jaishankar, B. (2021). Multimedia Data Protection Using Hybridized Crystal Payload Algorithm With Chicken Swarm Optimization. In *Multidisciplinary Approach to Modern Digital Steganography* (pp. 235-257). IGI Global.
2. Kalimuthu, S. (2021). Sentiment Analysis on Social Media for Emotional Prediction During COVID-19 Pandemic Using Efficient Machine Learning Approach. *Computational Intelligence and Healthcare Informatics*, 215.
3. Sam, I. S., Devaraj, P., & Bhuvaneswaran, R. S. (2012). An intertwining chaotic maps based image encryption scheme. Nonlinear Dynamics, 69(4), 1995-2007.
4. Ye, G., & Wong, K. W. (2012). An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear dynamics, 69(4), 2079-2087.
5. Huang, X. (2012). Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dynamics, 67(4), 2411-2417.

6. Fouda, J. A. E., Effa, J. Y., Sabat, S. L., & Ali, M. (2014). A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation, 19(3), 578-588.
7. Jolfaei, A., & Mirghadri, A. (2010). An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology, 19(2), 117-125.
8. Mallat, S. G. (1989). A theory for multiresolution signal decomposition: the wavelet representation. IEEE transactions on pattern analysis and machine intelligence, 11(7), 674-693.
9. Gong, L. H., He, X. T., Cheng, S., Hua, T. X., & Zhou, N. R. (2016). Quantum image encryption algorithm based on quantum image XOR operations. International Journal of Theoretical Physics, 55(7), 3234-3250.
10. Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. Journal of computer science, 3(9), 740-746.
11. Lagzian, S., Soryani, M., &Fathy, M. (2011, June). Robust watermarking scheme based on RDWT-SVD: Embedding Data in All subbands. In Artificial Intelligence and Signal Processing (AISP), 2011 International Symposium on (pp. 48-52). IEEE.
12. Deb, K., Al-Seraj, M. S., Hoque, M. M., & Sarkar, M. I. H. (2012, December). Combined DWT-DCT based digital image watermarking technique for copyright protection. In Electrical & Computer Engineering (ICECE), 2012 7th International Conference on (pp. 458-461). IEEE.
13. Wang, Y. R., Lin, W. H., & Yang, L. (2011). An intelligent watermarking method based on particle swarm optimization. Expert Systems with Applications, 38(7), 8024-8029.