Chaos Based Stego Color Image Encryption

M. I. Fath Allah*[1]

[1] Assist. Prof. in Communications & Electronics Department at Delta Higher Institute, Mansoura, Egypt

Email: mismail1885@yahoo.com

Abstract

Intensive studies have been done to get robust encryption algorithms. Due to the importance of image information, image encryption has become played a vital rule in information security. Many image encryption schemes have been proposed but most of them suffer from poor robustness against severe types of attacks. In this paper two proposed techniques will be presented for color image encryption to be robust to severe attacks: composite attack. One of these approaches is represented by hybrid use of both steganography and Discrete Wavelet Transform (DWT) based encryption and the other one in which Fractional Fast Fourier Transform (FRFFT) has been used with DWT. Not only new techniques will be presented but also a new chaotic map has been used as random keys for both algorithms. After extensive comparative study with some traditional techniques, it has been found that the proposed algorithms have achieved better performance.

Keywords: Double Random Phase Encoding (DRPE); Discrete Cosine Transform (DCT); Fast Fourier Transform (FFT); Fractional Fast Fourier Transform (FRFFT); Discrete Wavelet Transform (DWT); Red-Green-Blue (RGB).

1. Introduction

Nowadays, technology has improved rapidly so security issues have become more important to protect the information. There are different approaches to transfer information in ensuring way. Transferring information from sender to receiver has needed to be very confidential so encryption has become essential [1]. Optical techniques have appeared as effective practical tools in validating and securing information [2, 3]. One of the most attractive advantages of optical systems is the possibility to provide many degrees of freedom to handle parameters such as phase, amplitude, and wavelength [4]. Image encryption techniques have attracted a growing attention since the Double Random Phase Encoding (DRPE) technique has been proposed by Refregier and Javidi [5]. On the other hand, DRPE suffers from poor performance if the transmitted image is corrupted with different types of attacks, e.g. rotation and cropping. Color images represent most practical life information, and it has been found that DRPE isn't effective for color image encryption against attacks.

In this article, two proposed methodologies for color images encryption will be provided. Both techniques are based on merging steganography with encryption using chaotic maps as random keys. One of them has depended on using only DWT with steganography and another has been used FRFFT

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

as well as DWT. The effect of different types of noise have been studied; as salt & pepper noise, Gaussian noise, and speckle noise, and hence it has been found that salt & pepper noise has had the largest effect on most of performance metrics. So, three types of attacks have been merged with each other; salt & pepper noise, rotation by 5°, and centralized cropping of size 100×100 attacks called composite attack. Our results will be compared with traditional techniques for DRPE; Fast Fourier Transform (FFT) based DRPE, Discrete Cosine Transform (DCT) based DRPE, and traditional DWT based DRPE in case of imposing plain image to composite attack. Seven performance metrics have been used for that comparative study as will be obtained later.

The outline of this paper is organized as follows; (2) presents related work, (3) introduces the proposed algorithms, (4) observes the simulation results and discussions, and (5) gives the general conclusions.

2. Related Work

In 2015, Vijayaraghavan has performed encryption and decryption of the three-color planes based on gray code effect and FFT [6]. Narayanan has presented an overview on the various encryption-based compression techniques [7]. Li has proposed a performance-enhanced image encryption schemes based on depth-conversion integral imaging and chaotic maps [8]. Liu has designed a color image encryption algorithm using Arnold transform and DCT [9]. Deng has introduced a simple color image encryption with the help of Quick Response (QR) code [10]. Mohamed has proposed a hybrid encryption-watermarking algorithm for copyright protection [11]. In 2017, Rajendran, S et al. proposed a new symmetric key based image hiding method. Pseudo random keys were generated by using 1D logistic map and those keys have been used for choosing the pixel position of cover image randomly for hiding the secret image[12]. Razzaq, M. Abdur, et al. presented a blended security algorithm for the security of digital image. It was a fusion of three security methods i.e. encryption, steganography and watermarking. Proposed technique mainly embraced three phases [13]. In 2018 Zear et al presented a novel technique for multiple watermarking based on DWT, DCT and SVD using Back Propagation Neural Network[14]. HASHIM, MOHAMMED, et al conducted a review of image steganography in spatial Domain to explore the term image steganography by reviewing, collecting, synthesizing and analyzing the challenges of different studies which related to this area published from 2014 to 2017 [15]. In 2019, Valandar, Milad Yousefi, et al. have introduced a new steganography technique based on new 3d sine chaotic map. This map has been used in embedding and extracting processes to increase the security of the proposed algorithm[16]. Bhnassy, Mohamed A., et al. have proposed a novel robust optical image encryption and watermarking technique. This symmetric cryptosystem has depended on a novel dynamic delay chaotic hopping pattern (DDCHP) combined with a double random phase encoding (DRPE) [17]. In 2020, In March 2020, M. I. Fath Allah, and M. M. Eid have introduced a novel technique for optical encryption depending on the proposed confusion and diffusion processes, the chaotic keys could efficiently encrypt the color images. To provide better shuffling effect plus increasing the unfamiliarity, image transformation using Discrete Cosine Transform (DCT) also were embedding through the proposed confusion stage with higher robustness against various types of attacks. After intensive comparative study versus traditional and related techniques, it has been found that this proposed system achieved better performance than conventional ones especially in the case of severe composite attacks [18]. Also in March 2020, L. Huang, S. Wang, J. Xiang, and Y. Sun have proposed a chaotic color image encryption scheme based on DNA-coding calculations and arithmetic over the Galois field. Firstly, three modified onedimensional (1D) chaotic maps with larger key space and better chaotic characteristics were introduced. The experimental results have shown that their chaotic intervals are not only expanded to (0, 15), but their average largest Lyapunov Exponent reached 10. They have been utilized as initial keys. Secondly, DNA coding and calculations were applied to add more permutation of the cryptosystem. Ultimately, the numeration over the Galois field ensured the effect for the diffusion of pixels. The simulation analysis showed that this proposed encryption scheme had good encryption effect, and the numerical results have verified that it has have higher

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

security than some of the latest cryptosystems [19]. In 2021, O. F. Abdel Wahab has proposed a hybrid data compression technique increased the input data to be encrypted by RSA (Rivest Shamir Adleman) cryptography technique to improve the security level and it could be used in executing both lossless and lossy compacting Steganography methods. After evaluated that algorithm on criteria such as Savings percentage,

Compression Ratio, Mean Squared Error, Bits per pixel, Compression Time, Structural Similarity Index, Peak Signal to Noise Ratio, and Compression Speed, the proposed algorithm has introduced a high-level performance and system methodology compared to other methods that used the same methodology [20]. In 2022, P. Huang, et al. have presented the idea of polymorphism to improve the traditional one-dimensional-mapping coupled lattice, and to construct a selective chaotic map. It could make one-dimensional coupled map lattices produce various pseudo-random sequences based on different chaotic maps. Additionally, the key space has been larger than the traditional onedimensional coupled map lattices. Moreover, the uneven distribution of chaotic sequences in onedimensional coupled lattices has been rearranged to produce homogeneous sequences, and the encryption effect has become better [21].

3. Proposed Algorithms

In this subsection the two proposed methods will be illustrated.

A. The First Proposed Algorithm

The main steps of the first proposed algorithm will be discussed. Firstly, the original image has been hidden in the lower pixels of the cover image to form the stego-image. After that this image has been multiplied by the first random key followed by multiplication by the second random key. Finally, DWT has been applied to get the encrypted image to be transmitted through the channel. The reverse steps could be applied to get the decrypted image as shown in Figure 1. Here, the random phase masks in other traditional techniques; FFT based DRPE, DCT based DRPE, and traditional DWT based DRPE, have been replaced by chaotic maps to get powerful randomization of an image. Also, chaotic maps give more varieties to enhance the performance by varying its parameters and initial conditions. The main equations of the new map are based on Chirikov map using tan function instead of sin function are shown as follows;

$$x_{n+1} = x_n - K \tan y_n \qquad (1)$$

$$y_{n+1} = y_n + x_{n+1} \qquad (2)$$

B. The Second Proposed Algorithm

The main flow chart of the second proposed algorithm will be demonstrated. The only difference between this proposed approach and the first one is applying FRFFT before applying DWT in the encryption process. In the decryption process, applying Inverse FRFFT (IFRFFT) has been needed after applying Inverse DWT (IDWT) as obtained in Figure 2.

4. Results & Discussions A. Data Collection

The traditional as well as proposed techniques performance has been tested using the color images obtained in table 1 providing the name, the extension, the size, and the entropy of each plain image. The original image as well as cover image will be shown in Figure 3. These images are different in their histogram as well be illustrated in the Figure 4.

Table 1: Plain Color Images Database

Image	Name	Extension	Size	Entropy
Original	My picture	JPEG	450 × 300	6.0302

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

Cover	Water lilies	JPEG	600 × 800	7.0650

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

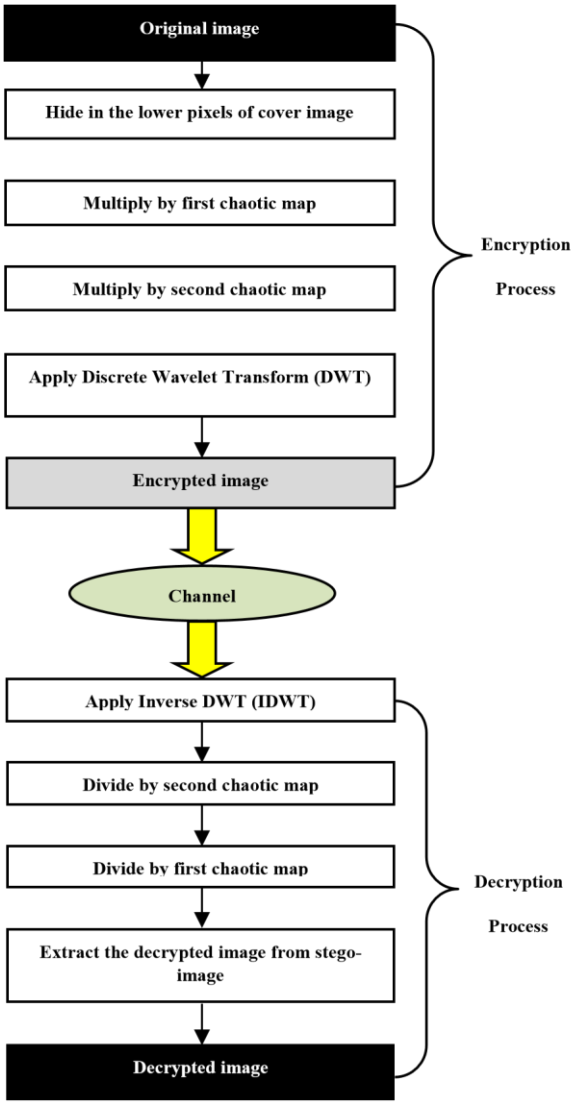


Figure 1: Flow chart of the first proposed technique

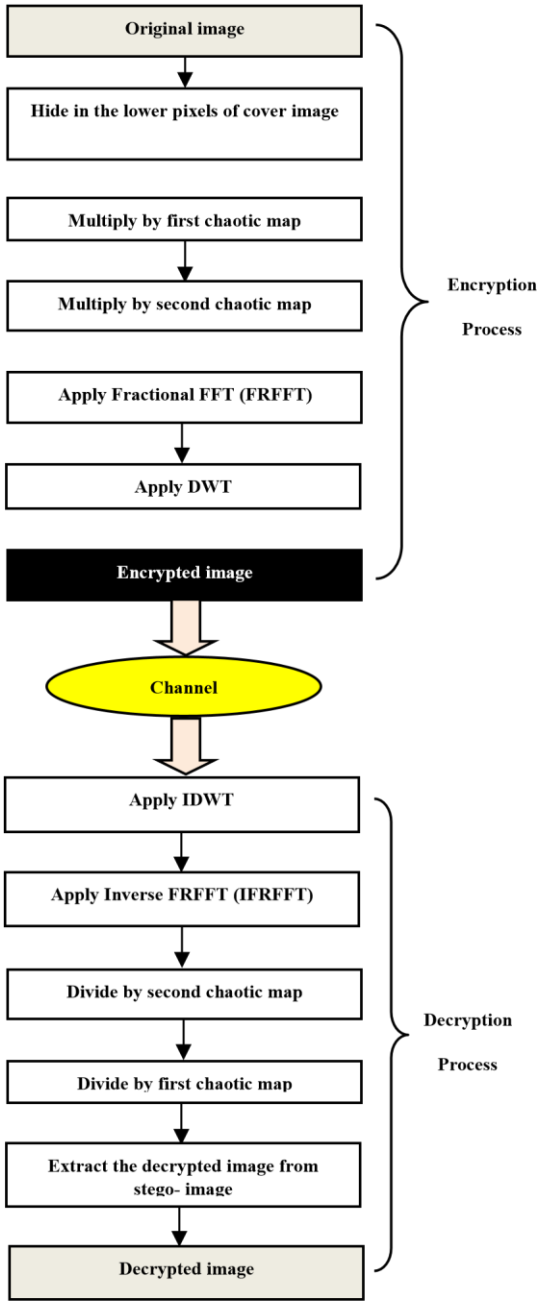


Figure 2: Flow chart of the second proposed technique.

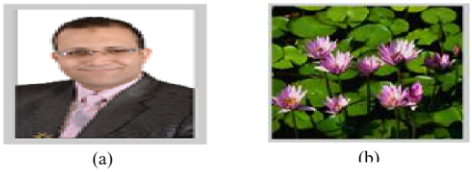


Figure 3: The color images (a) original image (1), and (b) cover image (2)

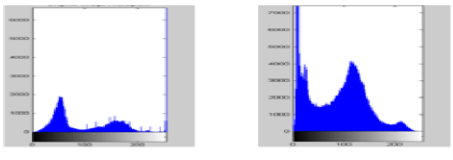


Figure 4: The color image histogram of (a) original image, and (b) cover image

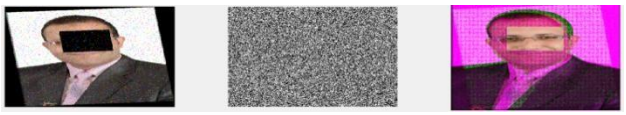
Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

B. The Performance Metrics

Seven performance metrics have been used to test the performance; elapsed time, entropy analysis, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), cross correlation coefficient (R) between original and decrypted images, Unified Average Changing Intensity (UACI), and the histogram analysis for both plain and resulted decrypted images. The basic definitions and equations for all the above performance metrics are listed in [11, 22]. Besides all of the above performance metrics, the simulation results for original, encrypted, and decrypted images for each technique will be observed.

C. Simulation Results & Discussions

The simulation results for the proposed algorithms as well as traditional ones will be discussed in this section using a personal computer with the following specifications: (i) Intel processor 3.2 GHZ Pentium-IV; (ii) 2MB cache Random Access Memory (RAM); (iii) 2 GB RAM; (iv) SATA hard disk 250GB.



(a) (b) (c)

Figure 5:The simulation results of (a) original, (b) encrypted, and (c) decrypted images for Both FFT and DCT based traditional techniques

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

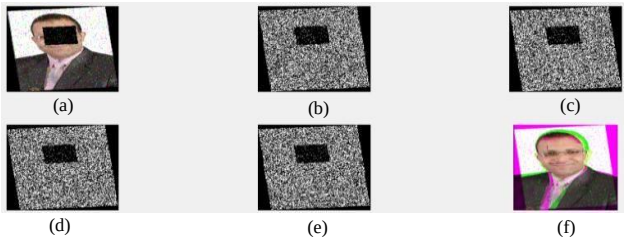


Figure 6:The simulation results of (a) original, (b) LL component, (c) LH component, (d) HL component, (e) HH component of encrypted, and (f) decrypted images for traditional DWT based technique

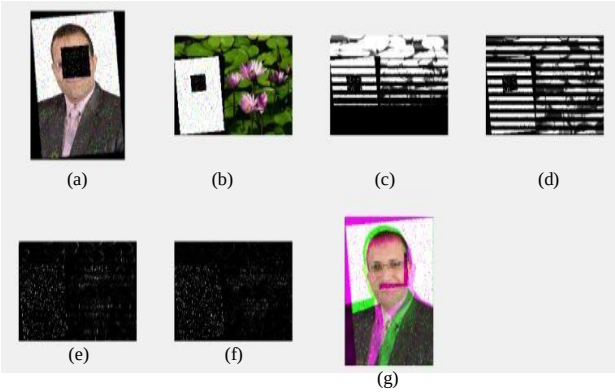


Figure 7: The simulation results of (a) original, (b) stego, (c) LL component, (d) LH component, (e) HL component, (f) HH component of encrypted, and (g) decrypted images for the first proposed technique

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

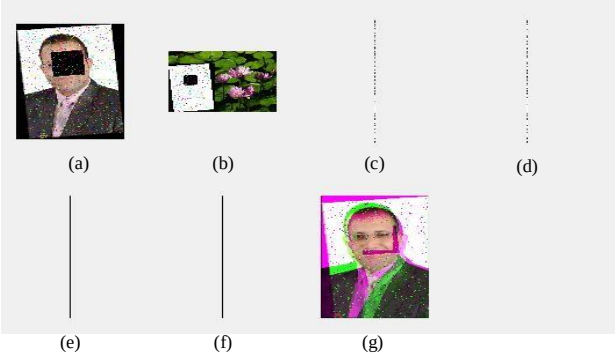


Figure 8: The simulation results of (a) original, (b) stego, (c) LL component, (d) LH component, (e) HL component, (f) HH component of encrypted, and (g) decrypted images for the second proposed technique

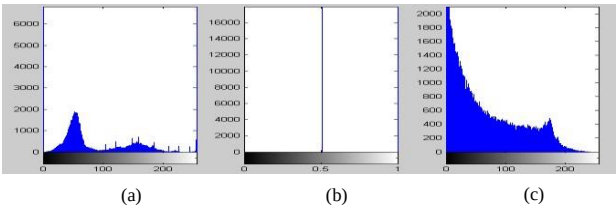


Figure 9: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for Both FFT and DCT based traditional techniques

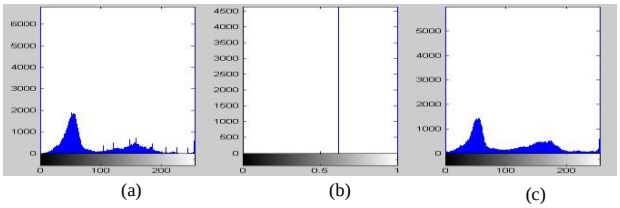


Figure 10: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for DWT based traditional technique

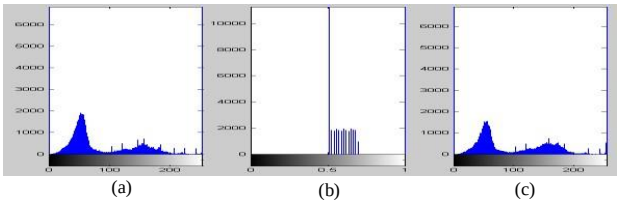
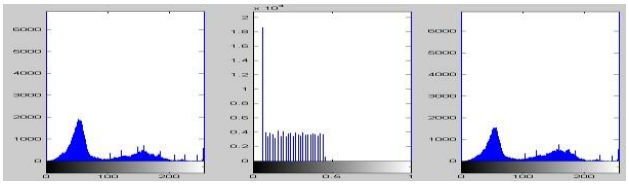


Figure 11: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for the first proposed technique

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022



(a) (b) (c)

Figure 12: The histogram analysis of (a) original, (b) encrypted, and (c) decrypted images for the second proposed technique

From all the previous figures it has been found that the proposed techniques have given more similar histogram for encrypted and decrypted images than other traditional techniques as well as realistic uniform distribution for encrypted image. Other performance metrics for all techniques will be listed in the following table.

Table 2: Performance Metrics

Metrics	FFT	DCT	DWT	Proposed Scheme (1)	Proposed Scheme (2)
Elapsed Time (Sec)	0.5007	0.7704	0.6259	0.7326	0.9310
Decrypted Image Entropy	7.2628	7.2638	5.9133	5.5161	5.5167
MSE	15828	15819	10495	10070	10101
Normalized MSE	1	0.999	0.663	0.636	0.638
PSNR (dB)	6.1365	6.1391	7.9209	8.1005	8.0871
R	0.1557	0.1545	0.4341	0.4526	0.4509
UACI	28.317	28.221	5.6079	0.8016	0.8815

From these measurements we find that the proposed algorithms have given the best performance against composite attacks. Our approach has obtained the closest entropy to that of original image listed in table 1, the least MSE, the largest PSNR, the maximum Cross correlation coefficient between original and decrypted images, and the least value for UACI. Only the elapsed time has been minimum in case of FFT based traditional technique. On the other hand, it is noticed that the difference in elapsed time between FFT based scheme and the first proposed one is only about 0.2 sec but the enhancement in other metrics that has been achieved by using our proposed schemes has been large. So, tradeoff could be done to get better performance against composite attacks. All these results are more obviously observed Figure 13.

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

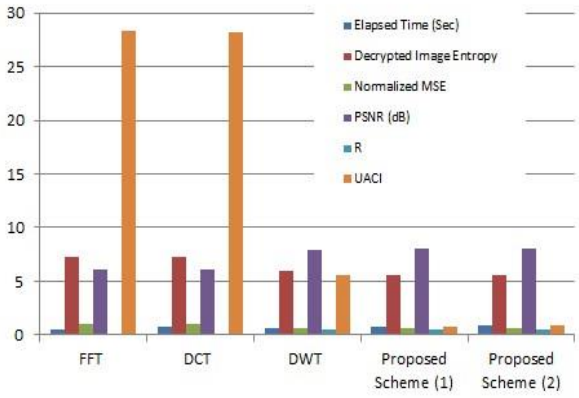


Figure 13: The performance metrics comparative presentation

5. Conclusions

In this paper two proposed encryption algorithms have been introduced. The random keys used in these techniques have been represented using a new chaotic map based on Chirikov map. The performance of these algorithms as well as a set of traditional algorithms has been studied on color images. As a result of extensive comparative study, it has been found that the proposed algorithms provided improved results with respect to traditional techniques; (i) the minimum value for MSE, (ii) the maximum value for PSNR, (iii) the largest value of R, (iv) the closest value of decrypted image entropy to those of the plain images, and (v) the minimum values for UACI. Only these techniques suffered from slightly larger values for elapsed time. The practical applications of these provided algorithms introduced the advantage of high robustness against composite-severe attacks. On the other hand, the theoretical implications of these algorithms were the increased complexity of the overall system. So, for real time applications in which low security level is needed it is recommended to use the first traditional algorithm. For high level of security, it is recommended to use one of the proposed methods especially the first one. In the future, the proposed techniques can be implemented on a reasonable hardware platform as Field Programmable Gate Array (FPGA).

Funding: "This research received no external funding"

Conflicts of Interest: "The author declares no conflict of interest."

References

[1] R. Vijayaraghavan, S. Sathya, N. R. Raajan, "Encryption for an Image Using Circular Budge on Bit-Planes" , International Journal of Applied Engineering Research, Vol. 9, No. 2, 2014, pp. 60–153.

[2] M. A. Mohamed, A.S. Samarah, M.I. Fath Allah, "Optical Encryption Techniques: An Overview", International Journal for Computer Science Issues (IJCSI), Vol. 11, No. 2, 2014, pp. 125-129.

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022

[3] F. Mosso, M. Tebaldi, "All-Optical Encrypted Movie", Optical Society of America, Vol. 19, No. 6, 2011, pp. 5706-5712.
[4] Y. Liu, J. Lin, J. Fan, N. Zhou, "Image Encryption Based on Cat Map and Fractional Fourier Transform", Journal of Computational Information Systems, Vol. 8, No. 18, 2012, pp. 7485-7492.
[5] P. R´efr´egier, B. Javidi, "Optical Image Encryption Based on Input Plane & Fourier Plane Random Encoding", Optics. Letters, Vol. 20, 1995, pp. 767-769.
[6] R. Vijayaraghavan, S. Sathya, N. R. Raajan, "Image Encryption based on the Reflected Binary Code Method with the Combination of FFT", Indian Journal of Science and Technology, Vol. 8, No. 36, 2015, pp. 1-10.
[7] C. S. Narayanan, S. A. Durai, "A Critical Study on Encryption Based Compression Techniques", Journal of Computers, Vol. 11, No. 5, 2015, pp. 380-399.
[8] X. Li, C. Li, S. T. Kim, I. K. Lee, "An Optical Image Encryption Scheme Based on Depth Conversion Integral Imaging and Chaotic Maps", arXiv: 1501. 04167v1 [cs. CR], 2015, pp. 1-18.
[9] Z. Liu, H. Chen, "Color image encryption by using Arnold Transform and Color-blend Operation in Discrete Cosine Transform Domains", Optics Communications Vol. 284, 2015, pp. 123–128.
[10] X. Deng, X. Zhu, "A Simple and Practical Color Image Encryption with the Help of QR Code", Optica Applicata, Vol.. XLV, No. 4, 2015, pp. 513-521.
[11] M. A. Mohamed, H. M. Abdel-Atty, A. M. Abutaleb, M. G. Abdel-Fattah, A. S. Samrah, "Hybrid Watermarking Scheme for Copyright Protection Using Chaotic Maps Cryptography", International Journal of Computer Applications (0975 – 8887), Vol. 128, No. 1, 2015, pp. 1:14.
[12] [Rajendran, S. and M. Doraipandian, Chaotic Map Based Random Image Steganography Using LSB Technique. IJ Network Security, 2017. 19(4): p. 593-598.
[13] Razzaq, M.A., et al., Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 2017. 8(5).
[14] Zear, A., A.K. Singh, and P. Kumar, A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia tools and applications, 2018. 77(4): p. 4863-4882.
[15] HASHIM, M., et al., A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. Journal of Theoretical & Applied Information Technology, 2018. 96(4).
[16] Valandar, M.Y., et al., An integer wavelet transform image steganography method based on 3D sine chaotic map. Multimedia Tools and Applications, 2019. 78(8): p. 9971-9989.
[17] Bhnassy, M.A., et al., Image encryption and watermarking combined dynamic chaotic hopping pattern with double random phase encoding DRPE. Optical and Quantum Electronics, 2019. 51(7): p. 246.
[18] M. I. Fath Allah, M. M. Eid, "Chaos Based 3D Color Image Encryption," Ain Shams Engineering Journal (ASEJ), Vol. 11, Issue 1, p. 67 – 75, March 2020.
[19] Huang, L., Wang, S., Xiang, J., Sun, Y., "Chaotic Color Image Encryption Scheme using Deoxyribonucleic Acid (DNA) Coding Calculations and Arithmetic over the Galois Field," Mathematical Problems in Engineering, Hindawi, Vol. 2020, ID: 3965281, https://doi.org/10.1155/2020/3965281, p. 1 – 22, March 2020.
[20] O. F. A.Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, ``Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," IEEE Access, vol. 9, pp. 31805_31815, 2021..
[21] B. Huang, et al., "A Novel Color Image Encryption Algorithm Using Coupled Map Lattice with Polymorphic Mapping," Electronics 2022, 11, 3436. https://doi.org/10.3390/electronics11213436.
[22] A. Alfalou, C. Brosseau, "Optical Image Compression and Encryption Methods", Adv. Opt. Photon, 1(00516980), 2010, pp. 589-636.

Doi : https://doi.org/10.54216/JCIM.100201
Received: May 01, 2022 Accepted: August 01, 2022