SINAI International Scientific Journal (SISJ)

Vol.1 Issue 1, July 2024

DWT versus DCT Based Hybrid Steganography and Watermarking Technique for Color Image Encryption

Essam Abdellatef ^{*1} and M. I. Fath Allah^{2}

[1]Electrical Engineering Department, Faculty of Engineering, Sinai University, El-Arish, Egypt.
[1]Electrical Engineering Department, Faculty of Engineering, Suez University, Suez, Egypt.
**Corresponding author*

Correspondence:

Essam Abdellatef
essam.abdellatef@su.edu.eg

Citation:

Abdellatef, E. and Fath Allah, M. A. “DWT versus DCT Based Hybrid Steganography and Watermarking Technique for Color Image Encryption", SINAI International Scientific Journal (SISJ), vol. 1, pp. 33-57, 2024

Received: 20 April 2024

Accepted: 21 July 2024

ABSTRACT

Comprehensive studies have been done to develop strong encryption technology, which plays a vital role in multimedia transmission and communications. High robustness against various types of attacks is the main requirement of any encryption method. Many algorithms have been suggested for encryption, but most of them suffer from weak efficiency. In this paper, two proposed algorithms for color image encryption will be provided to get high robustness against composite attacks with improved performance. The composite attacks might be in one of two different forms: friendly or hard. Encryption techniques could be represented by hybrid of steganography and watermarking. Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) have been used for image transformation with the proposed techniques. After intensive comparative studies with some traditional methods, it has been got that the new algorithms have given better performance over that of the traditional ones.

KEYWORDS: Image encryption, Steganography, and Watermarking.

1. INTRODUCTION

In today's rapidly advancing technological landscape, ensuring the security of information has become paramount. With various methods available for data transfer, encryption has emerged as a critical component in safeguarding sensitive information [1]. Encryption techniques have proven to be effective means of validation and data protection [2, 3]. Steganography, a scientific method within the realm of information security, offers another layer of protection. Additionally, watermarking can be integrated with steganography to further validate and secure data. In watermarking, a signature is embedded within a digital image, either visibly or invisibly. On the other hand, steganography involves concealing the original image within a cover image to thwart potential hackers, resulting in what is known as a stego image [4 – 21].

This paper proposes two techniques for color image encryption, both leveraging a combination of steganography and watermarking using chaotic maps as random keys. Six different chaotic maps are employed, each with varying parameters, to establish robust data encryption. Performance evaluation against composite attacks is conducted using eight metrics. In one method, two chaotic maps of the same type are used to multiply the original color image. The proposed techniques employ Discrete Wavelet Transform (DWT) in one approach and Discrete Cosine Transform (DCT) in the other.

The primary contribution of this research lies in offering a resilient image encryption solution capable of withstanding diverse attacks. Subsequent sections will delve into the literature review, the proposed encryption methods, simulation results and discussions, and finally, the conclusion.

2. RELATED WORKS

In 2013, Roy and colleagues introduced an edge adaptive image steganography method known for its high fidelity and effective imperceptibility against steganalysis attacks [22]. The following year, a secure LSB technique is provided for image steganography utilizing the concept of non-linear dynamic systems (chaos) [23]. In the same year, B. Muhamed, et al. focused on Zerosteganography, a technique imperceptibly embedding data without altering the cover image, thus bypassing steganalysis [24]. Hussain, in 2014, proposed an optical image encryption algorithm by embedding a secret image into a cover image to create a stego-image, subsequently encrypted using DRPE and chaotic substitution box transformation [2].

In 2015, Benrhouma et al. introduced a semi-fragile watermarking and encryption scheme for digital images [25]. Aziz, M. et al., in the same year, presented a robust, efficient, and high-capacity steganographic algorithm capable of embedding grayscale and color images into a color image [5]. Zear et al. in 2016 devised a novel multiple watermarking method based on DWT, DCT, and SVD, employing Back Propagation Neural Network [26]. Rajendran, S et al. reviewed a symmetric key-based image hiding technique in 2016, utilizing pseudo-random keys generated from a 1D logistic map to choose pixel positions for hiding secret images [27].

In 2017, M. Abdur, et al. proposed a blended security technique for digital image security, integrating encryption, steganography, and watermarking in three phases [28]. H. Muhamed, et al. conducted a comprehensive review of image steganography in the spatial domain in 2018, analyzing studies from 2014 to 2017 to explore challenges in the field [29]. V. Yosef, et al. introduced a new steganography technique in 2018 based on a 3D sine chaotic map to enhance algorithmic security [30]. Finally, in 2019, A. Muhamed, et al. proposed an optical image encryption relying on DDCHP and DRPE [31].

3. THE PROPOSED TECNIQUES

This section delves into the key stages of a hybrid watermarking and steganography approach. Initially, to create the stego image, the original image is concealed within the lower pixel range of the cover image. Subsequently, the image undergoes multiplication by two sequential chaotic maps. Following this, either Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT), depicted in Fig. (1) and (2) respectively, is applied to generate the encrypted image by the conclusion of the encryption process. Lastly, the encrypted image is embedded to produce the encrypted watermarked image. The reversal of these steps, as depicted in Figures (1) and (2), enables the retrieval of the decrypted image. The equation of DWT could be expressed as:

$$W_{j,k} = \sum_{n=0}^{N-1} x[n] ¥_{j,k}[n] \tag{1}$$

Where $W_{j,k}$ are the wavelet coefficients, *x[n]* is the original image, and $¥_{j,k}[n]$ are the discrete wavelet functions

In addition, the equation of DCT could be expressed as:

$$X[k] = a(k) \sum_{n=0}^{N-1} x[n] \cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right) k\right] \quad (2)$$

Where, *X[k]* is the DCT coefficient at index *k*, *x[n]* is the original image, and *a(k)* is the normalization factor.

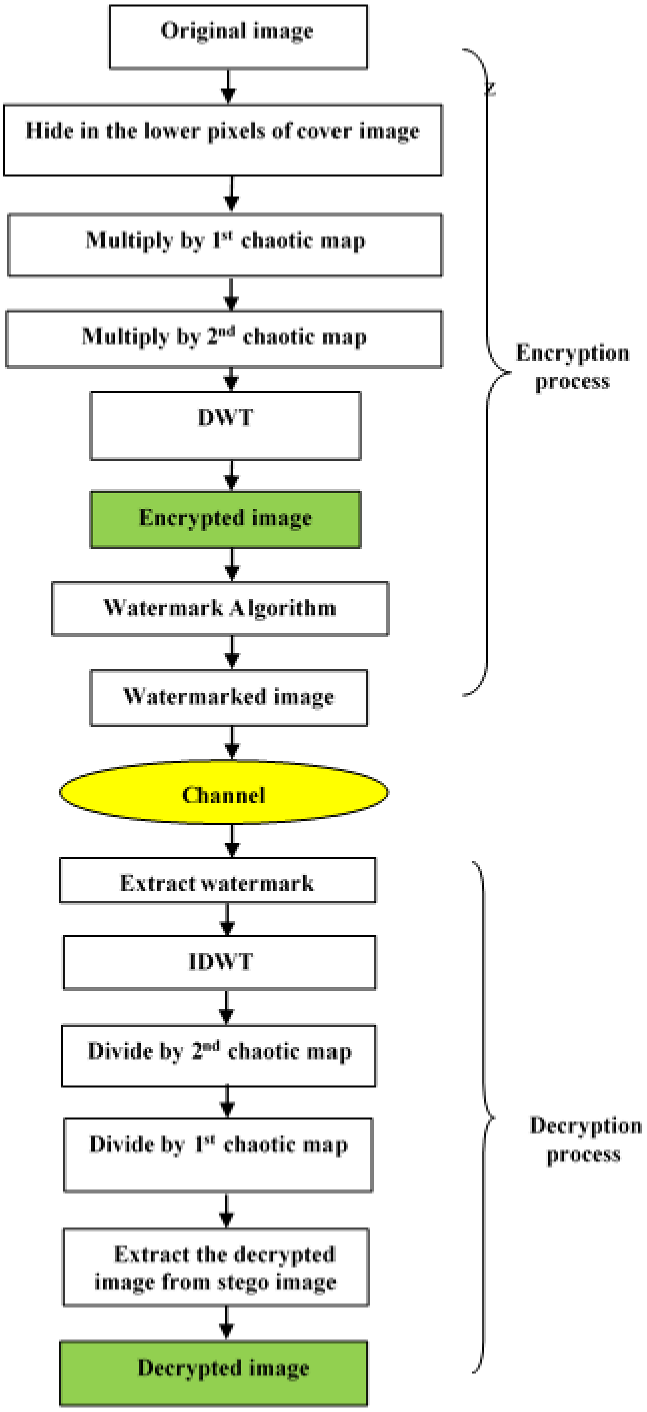

Original image
Hide in the lower pixels of cover image
Multiply by 1st chaotic map
Multiply by 2nd chaotic map
DWT
Encrypted image
Watermark Algorithm
Watermarked image
Encryption process
Channel
Extract watermark
IDWT
Divide by 2nd chaotic map
Divide by 1st chaotic map
Extract the decrypted image from stego image
Decrypted image
Decryption process

Fig. 1: Block diagram of DWT based proposed technique.

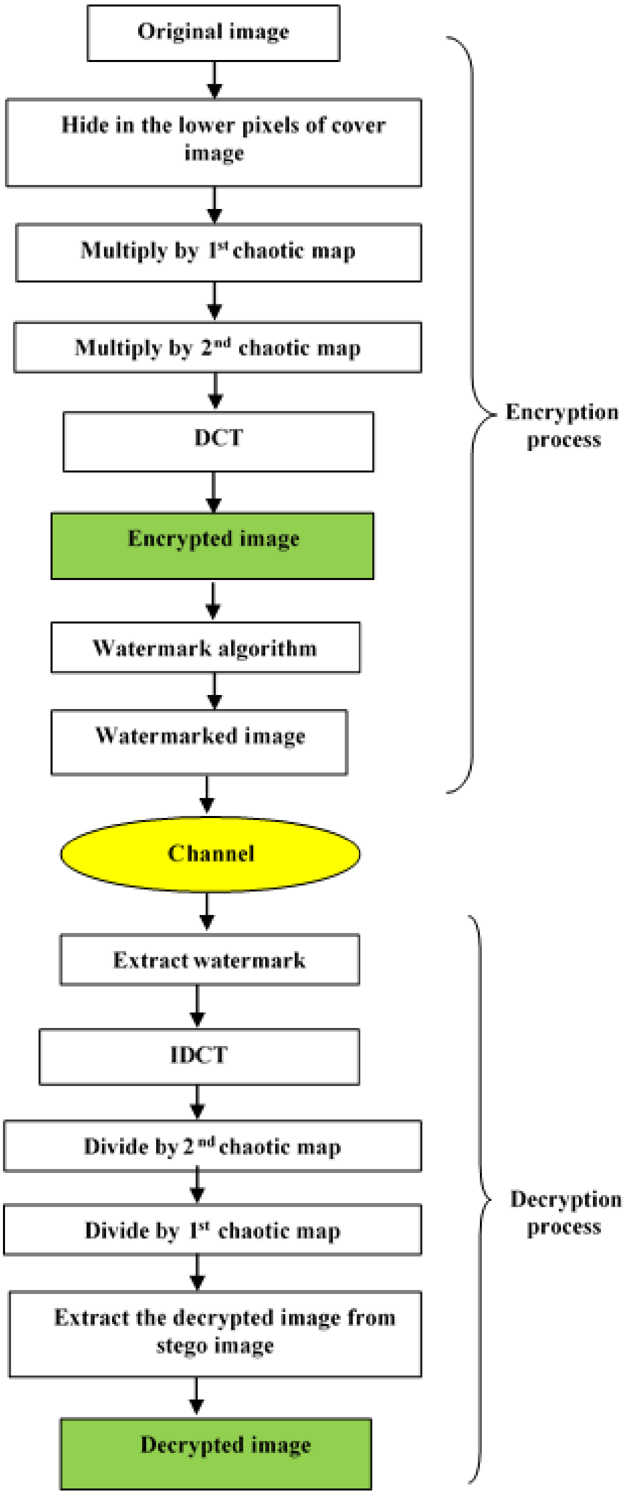
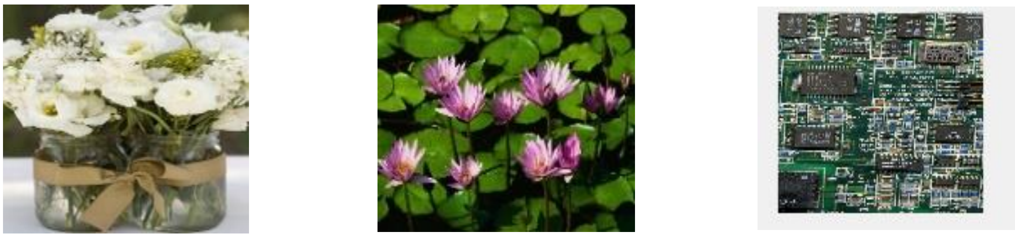

Original image
Hide in the lower pixels of cover image
Multiply by 1st chaotic map
Multiply by 2nd chaotic map
DCT
Encrypted image
Watermark algorithm
Watermarked image
Encryption process
Channel
Extract watermark
IDCT
Divide by 2nd chaotic map
Divide by 1st chaotic map
Extract the decrypted image from stego image
Decrypted image
Decryption process

Fig. 2: Block diagram of DCT based proposed technique.

4. RESULTS AND DISCUSSIONs

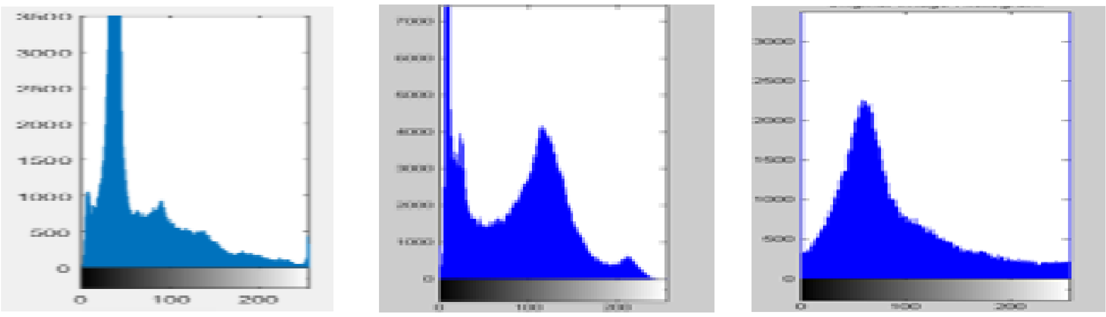
4.1. Data Collection

The effectiveness of the suggested techniques has been evaluated using an original color image, a cover image, and a host image. These images are depicted in Fig. (3), while their corresponding histograms are presented in Fig. (4).



(a) (b) (c)

Fig. 3: (a) Original Image, (b) Cover Image, and (c) Host Image..



(a) (b) (c)

Fig. 4: Image Histogram for; (a) Original Image (1), (b) Cover image (2), and (c) Board Image.

4.2. Performance Metrics

The performance is evaluated using various metrics; elapsed time, MSE, CC, PSNR, NPCR, UACI, Entropy, and histogram analysis [32].

4.3. Simulation Results and Discussions

In this section, the simulation results of the proposed hybrid steganography and watermarking based encryption technique will be discussed. All experiments have been performed using the same computer and our computer most of the time has been connected to the internet.

4.3.1 Friendly Attacks

Friendly type of attacks could be represented by imposing attacks to the encrypted image. All results have been demonstrated in case of Gaussian noise because it has been more serious than other types of noise such as; salt & pepper noise and speckle noise. In this subsection the performance measurements and the simulation results will be presented in two phases; (a) by adding host image (board image) to the original color image to make the data more secure from hacker attacks and to get high robustness against composite attacks, and (b) without adding host image.

- *By Adding Host Image*

Figs. (5-8) illustrate that the proposed technique achieves a uniform distribution of histograms for encrypted images when utilizing the Chirikov map as an encryption key compared to other methods. It is recommended to employ the Chirikov map, particularly in scenarios involving Gaussian noise, when combining the host image with the original one to mitigate friendly composite attacks. While the study primarily focuses on Gaussian noise, it also encompasses various noise types, including salt and pepper as well as speckle noise, for comprehensive evaluation. Notably, the assessment reveals that the DCT based technique yields superior results compared to the DWT based approach, ensuring fair judgment across different noise scenarios.

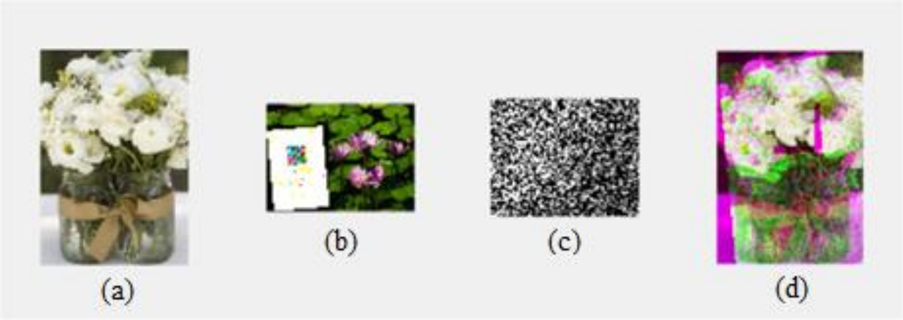
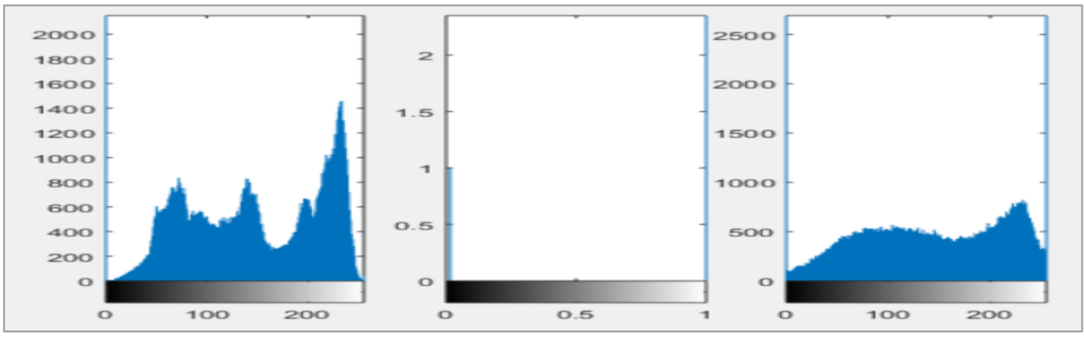


Fig. 5: Image Histogram for; (a) Original Image (1), (b) Cover image (2), and (c) Board Image.



(a) **(b)** **(c)**

Fig. 6: The histogram of (a) original (b) encrypted and (c) decrypted images for DCT based technique.

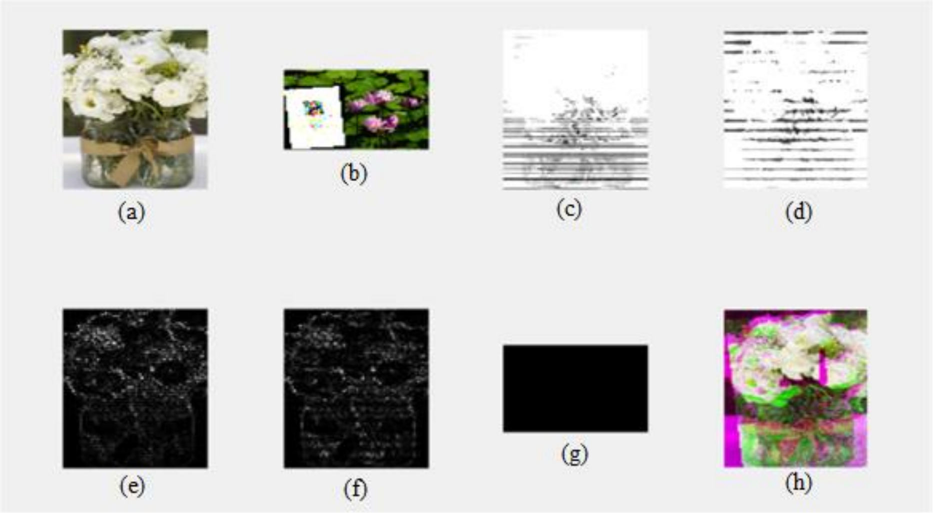


Fig. 7: (a) original, (b) stego (c) LL, (d) LH, (e) HL, (f) HH of encrypted, (g) watermarked image, and (h) decrypted image for DWT based technique.

From these measurements shown in Figs. (9-12), we found that the Chirikov Map has provided minimum Elapsed time for DCT-based method, Quadratic map has given the closer value to one for cross correlation coefficient, the least MSE and closer value for UACI to practical value of 33% and Henon map has achieved the largest PSNR.

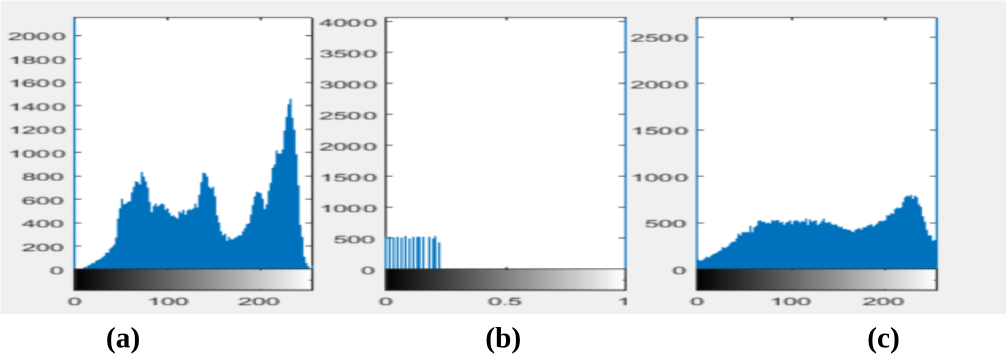


Fig. 8: The histogram of (a) original, (b) encrypted, and (c) decrypted image for DWT based technique.

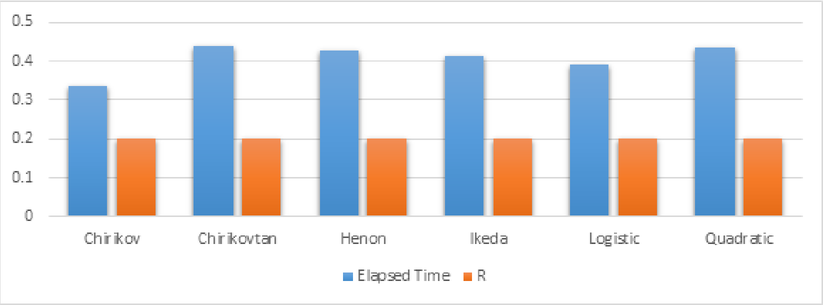


Fig. 9: Time and CC measurements for DCT based technique.

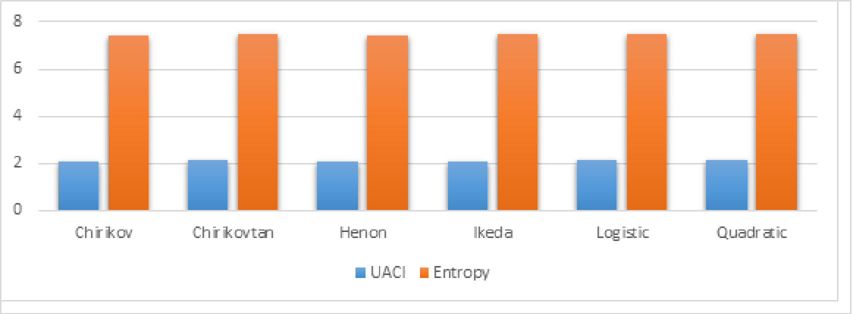


Fig. 10: UACI and Entropy measurements for DCT based technique.

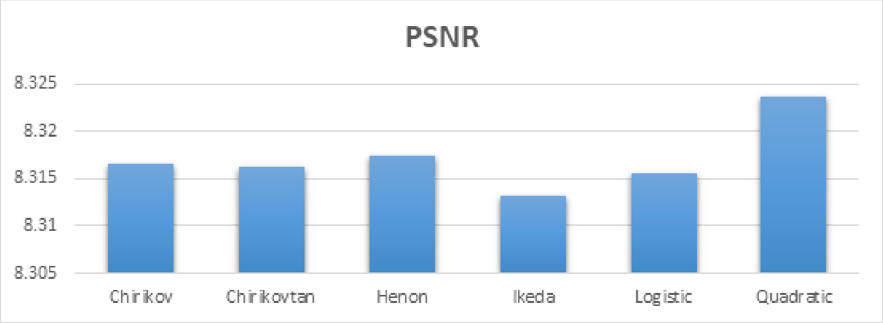


Fig. 11: PSNR for DCT based technique.

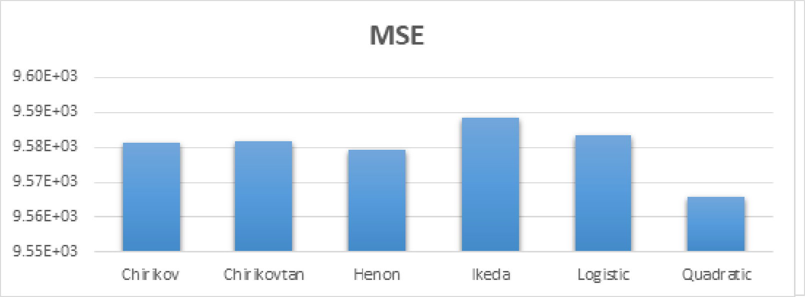


Fig. 12: MSE measurements for DCT based technique.

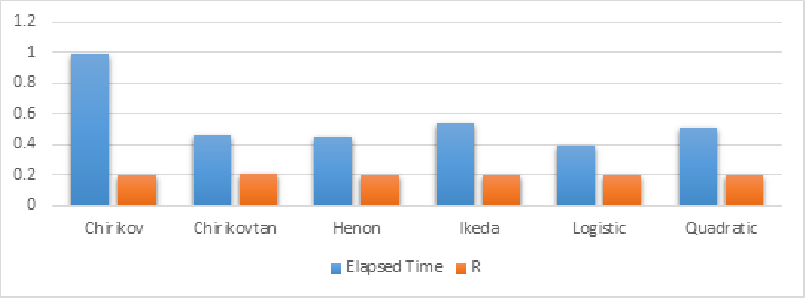


Fig. 13: Time and CC measurements for DWT based technique.

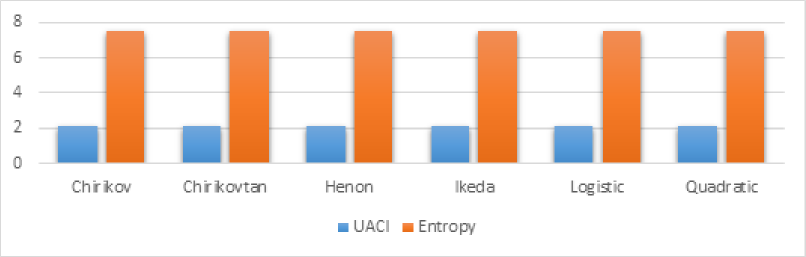


Fig. 14: UACI and Entropy measurements for DWT based technique.

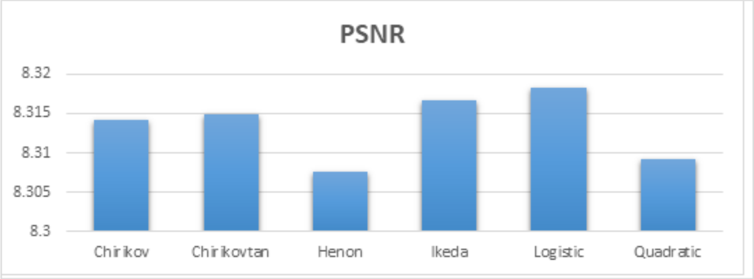


Fig. 15: PSNR for DWT based technique.

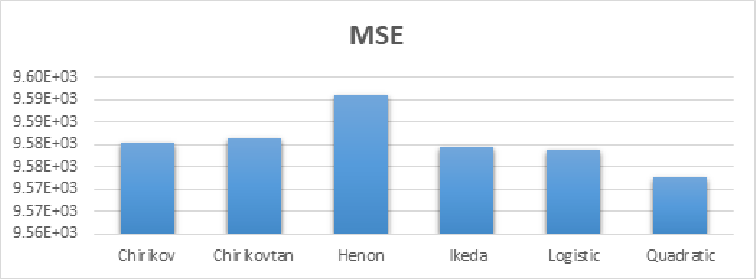


Fig. 16: MSE measurements for DWT based technique.

From measurements shown in Figs. (13-16), we found that Logistic map has provided minimum elapsed time and largest PSNR for DWT-based method, Chirikovtan map has given the closer value to one for cross correlation coefficient, Ikeda has achieved the least MSE and Henon map has provided the closer value for UACI to practical value of 33%.

- *Without Adding Host Image*

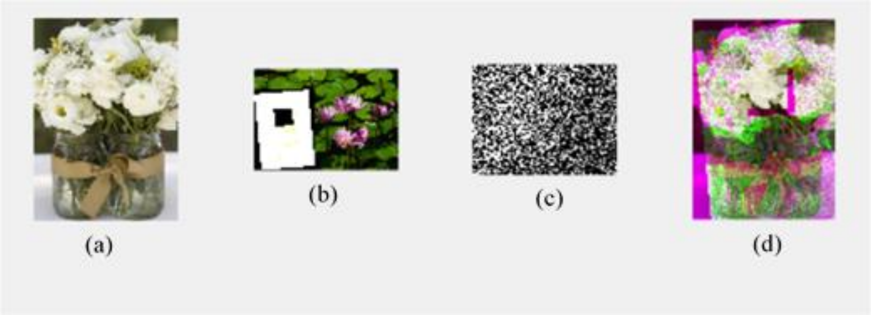
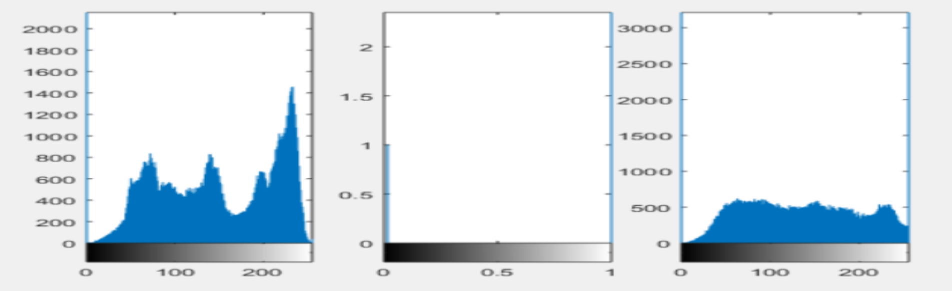


Fig. 17: (a) original, (b) stego, and (c) watermarked image (d) decrypted image for DCT based technique.



(a) (b) (c)

Fig. 18: The histogram of; (a) original (b) encrypted and (c) decrypted images for DCT based technique.

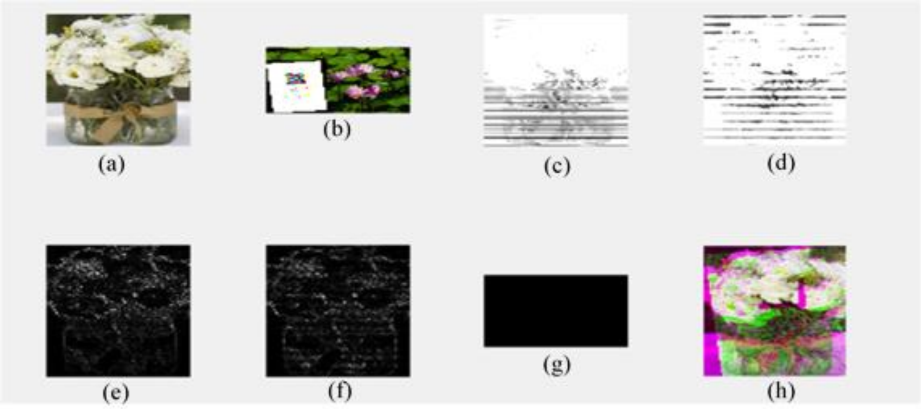


Fig. 19: (a) original (b) stego (c) LL, (d) LH, (e) HL, (f) HH of encrypted, (g) watermarked image, and (h) decrypted images for DWT based technique.

Figs (17-20) reveal that the proposed technique achieves a more uniform histogram distribution for encrypted images using the Chirikov Map, regardless of whether DCT or DWT based techniques are employed, effectively countering friendly composite attacks. Given the consistent uniformity in histogram distribution, it is recommended to utilize the Chirikov Map as a defense against friendly composite attacks, particularly in scenarios involving Gaussian noise, for both DCT and DWT based methods. Additionally, it is noteworthy that the DCT based technique outperforms the DWT based technique even without the inclusion of a host image.

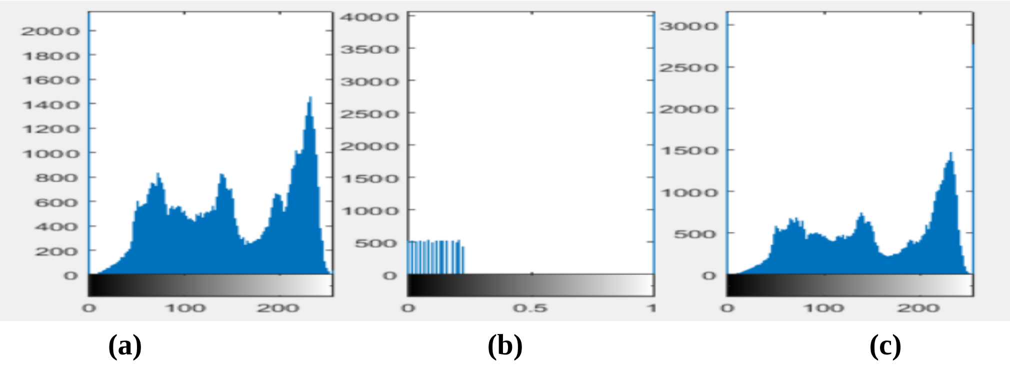


Fig. 20: The histogram of; (a) original, (b) encrypted, and (c) decrypted images for DWT based technique.

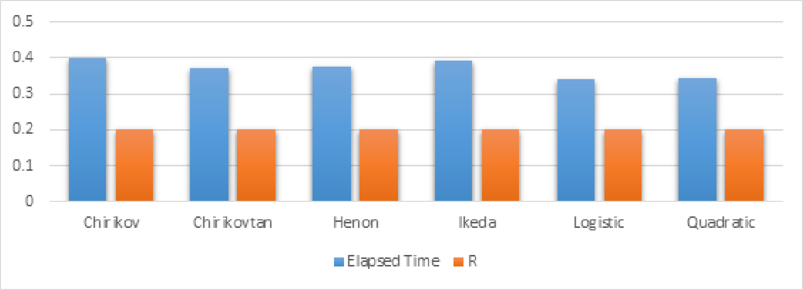


Fig. 21: Time and CC measurements for DCT based technique.

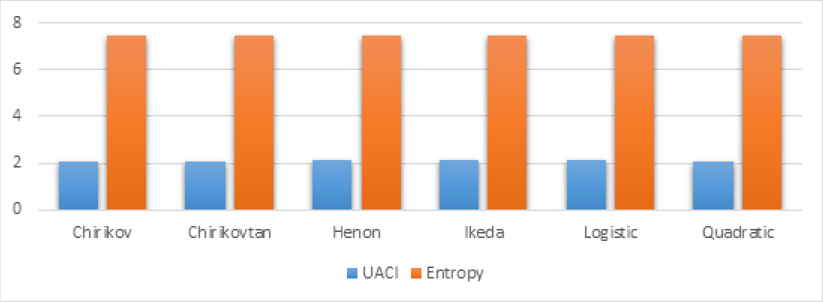


Fig. 22: UACI and Entropy measurements for DCT based technique.

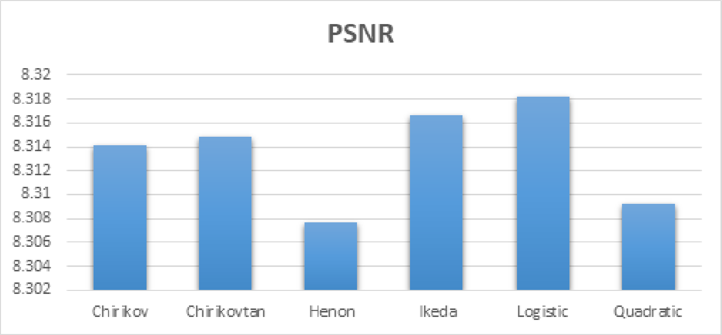


Fig. 23: PSNR for DCT based technique.

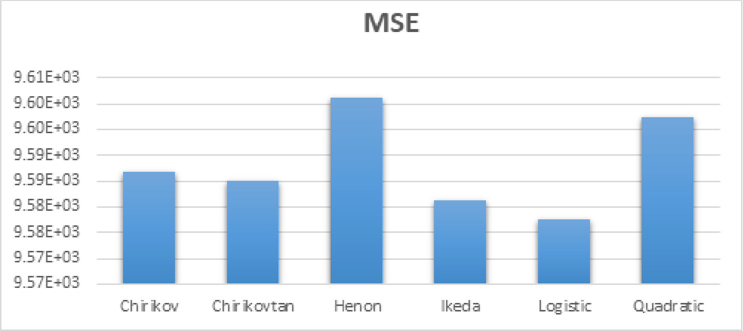


Fig. 24: MSE measurements for DCT based technique..

From measurements shown in Figs. (21-24), it has been found that Logistic map has provided minimum elapsed time for DCT-based method, the largest PSNR and the least MSE and Henon map has given the closer value to one for cross correlation coefficient and the closer value for UACI to practical value of 33%.

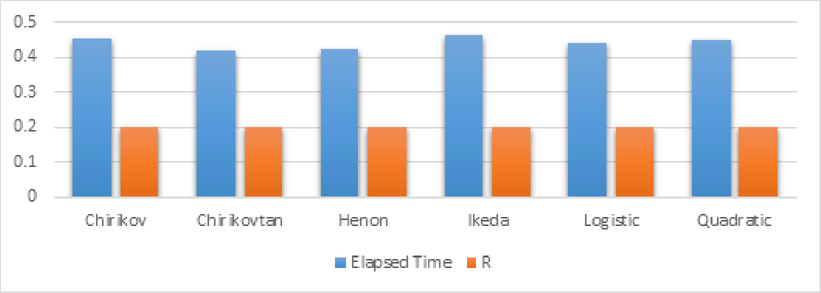


Fig. 25: Time and CC measurements for DWT based technique.

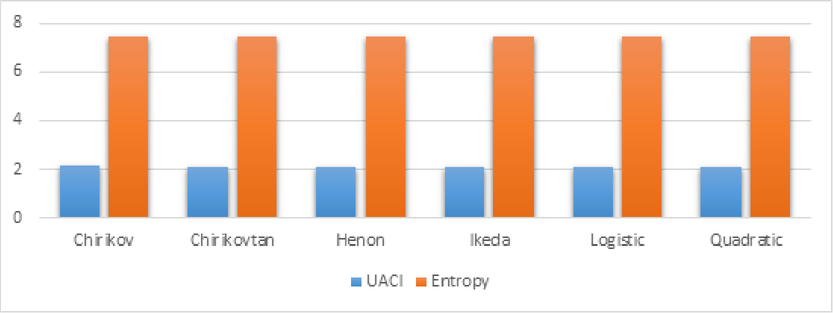


Fig. 26: UACI and Entropy measurements for DWT based technique.

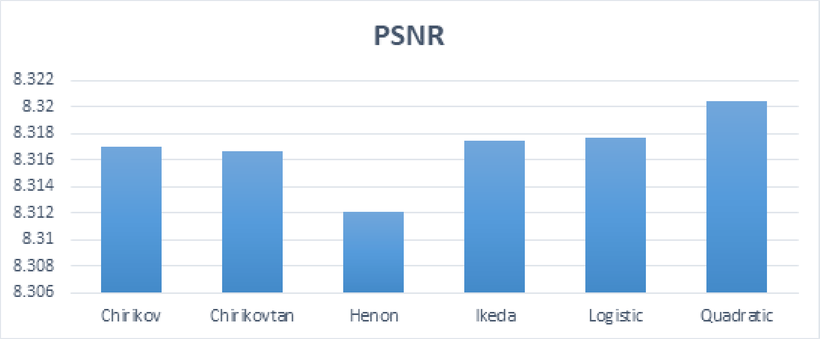


Fig. 27: PSNR for DCT based technique.

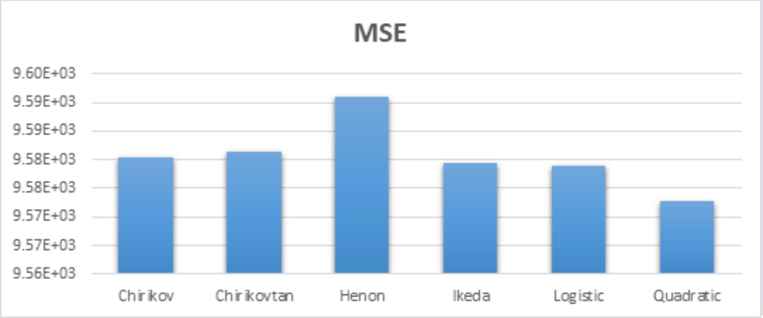


Fig. 28: MSE measurements for DWT based technique.

As depicted in Figs. (25-28), various maps exhibit distinct performance metrics within the context of DWT-based method: Chirikovtan map demonstrates minimal elapsed time, Logistic map approaches a correlation coefficient closer to one, Chirikov achieves a UACI value closer to the practical benchmark of 33%, and Quadratic map yields the highest PSNR alongside the lowest MSE. Both DCT and DWT based techniques demonstrate enhancement ratios compared to traditional methods. Specifically, concerning the Chirikov map, the DCT-based approach showcases approximately a 39.4% improvement in MSE, a 35% enhancement in PSNR, and approximately a 92.6% improvement in UACI. Conversely, the DWT based technique with the Chirikov Map yields enhancement ratios of 39% in MSE, 4.9% in PSNR, and 61.8% in UACI.

4.3.2. Hard Attacks

- *By adding Host image*

In this section the performance measurements and the simulation results will be presented in two ways; (a) by adding host image to make the data more secure from hacker attacks and to get high robustness against composite attacks, and (b) without adding host image.

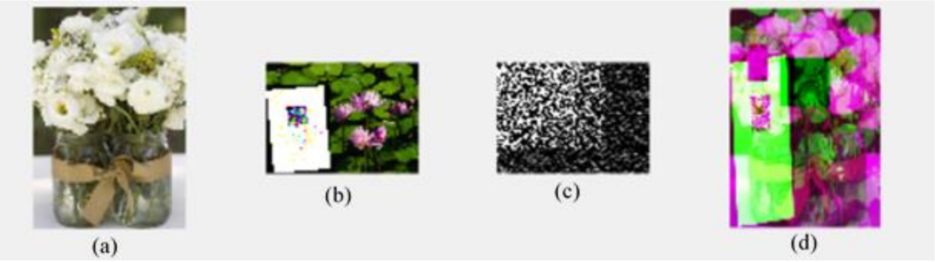
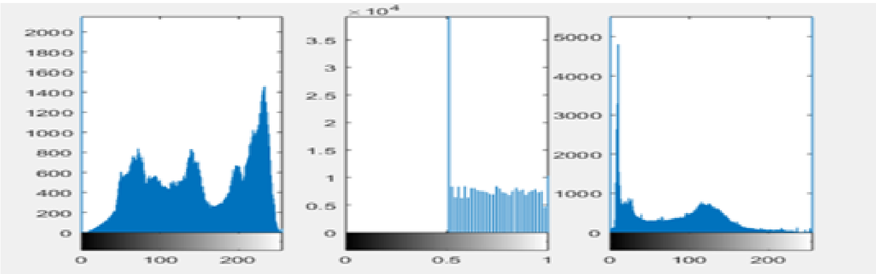


Fig. 29: (a) original, (b) stego, and (c) watermarked image (d) decrypted images for DCT based technique.



(a) **(b)** **(c)**

Fig. 30: The histogram of; (a) original (b) encrypted, and (c) decrypted images for DCT based technique.

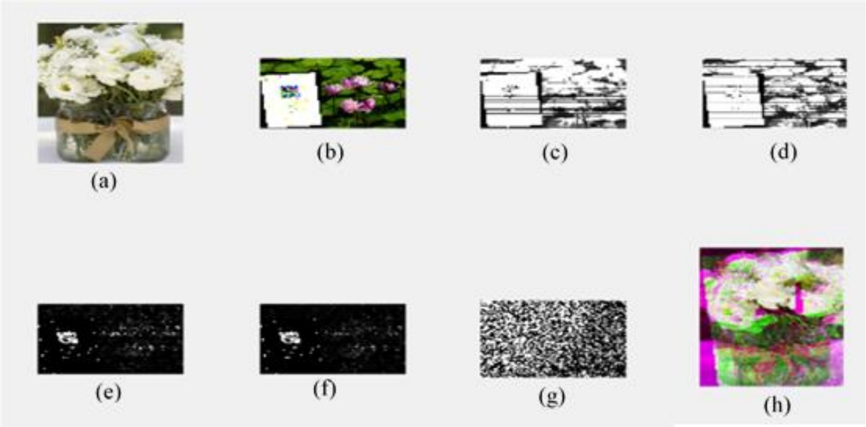
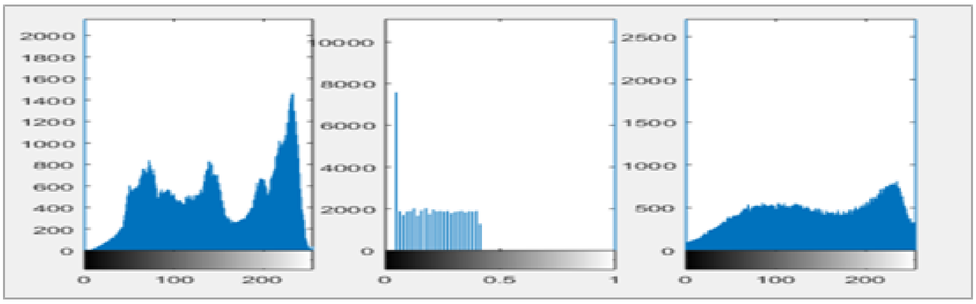


Fig. 31: (a) original, (b) stego (c) LL, (d) LH, (e) HL, (f) HH of encrypted, (g) watermarked image, and (h) decrypted images for DWT based technique.



(a) (b) (c)

Fig. 32: The histogram of; (a) original (b) encrypted, and (c) decrypted images for DWT based technique.

The analysis of Figs (29-32) reveals that both DCT and DWT-based methods offer a more uniform histogram distribution for encrypted images when employing the Chirikov map, effectively countering hard composite attacks. Furthermore, in the comparison between DCT and DWT-based methods against hard composite attacks, it was observed that the DCT-based technique exhibited superior performance compared to the DWT-based approach

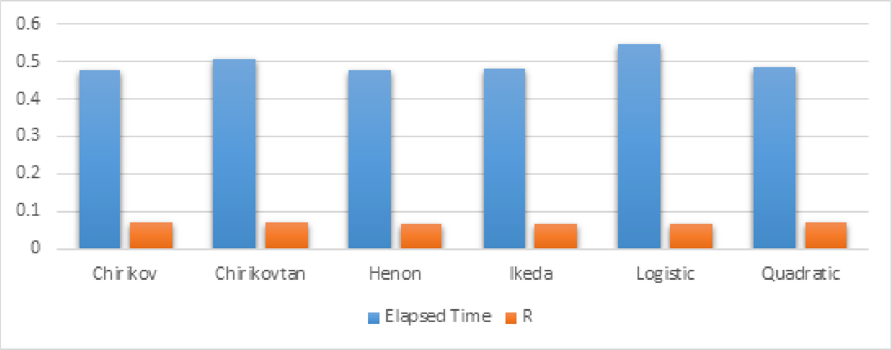


Fig. 33: Time and CC measurements for DCT based technique.

From measurements shown in Figs. (33-36) it has been found that Chirikov map has provided minimum elapsed time for DCT-based method, while Quadratic map has given the closer value to one for cross correlation coefficient, the largest PSNR and the least MSE, Logistic map has given the closer value for UACI to practical value of 33%.

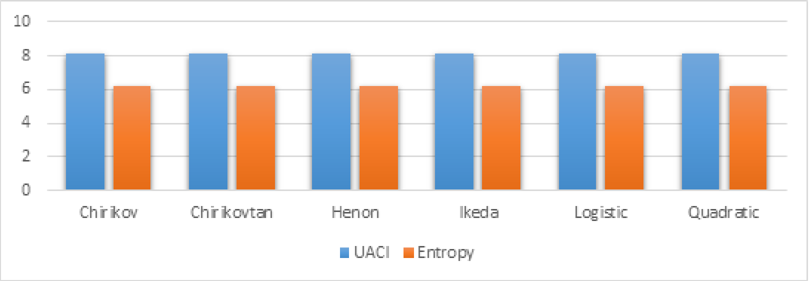


Fig. 34: UACI and Entropy measurements for DCT based technique.

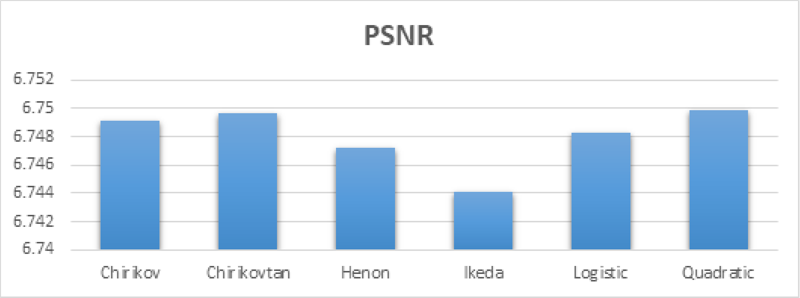


Fig. 35: PSNR for DCT based technique.

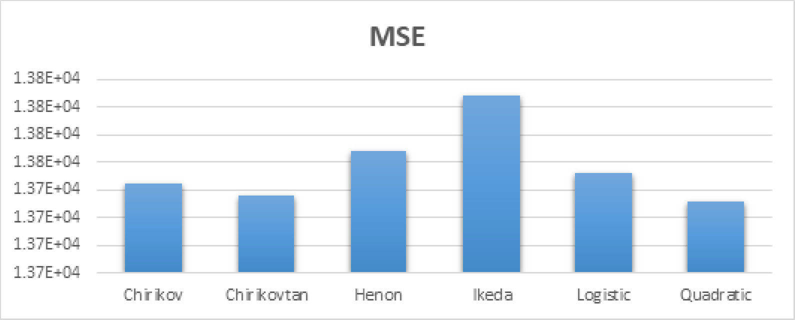


Fig. 36: MSE measurements for DCT based technique.

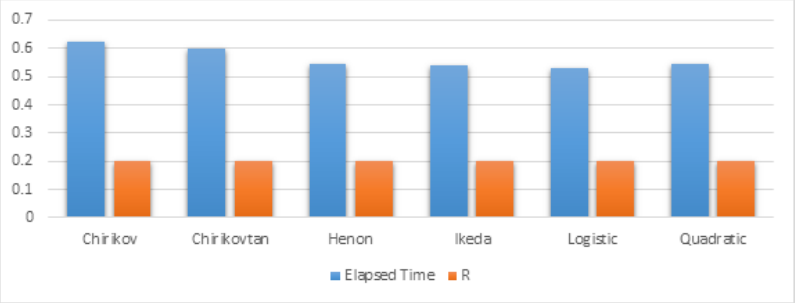


Fig. 37: Time and CC measurements for DWT based technique.

Based on the measurements illustrated in Figs. (37–40), the DWT-based method exhibits superior timing characteristics and closer cross-correlation coefficients. The Chirikov map demonstrates the highest PSNR and the lowest MSE, while the Henon map approaches a UACI value closer to the practical benchmark of 33%. Notably, under rigorous attack scenarios, the proposed technique outperforms traditional methods across most efficiency metrics, except for R. The utilization of this proposed technique consistently yields enhancement ratios across various performance metrics. Specifically, for the Chirikov map, the DCT-based approach shows approximately 13% improvement in MSE, a 9.9% enhancement in PSNR, and around a 71% improvement in UACI. Conversely, the DWT-based technique for the Chirikov map achieves enhancement ratios of approximately 8.78% in MSE, 5% in PSNR, and 62.8% in UACI.

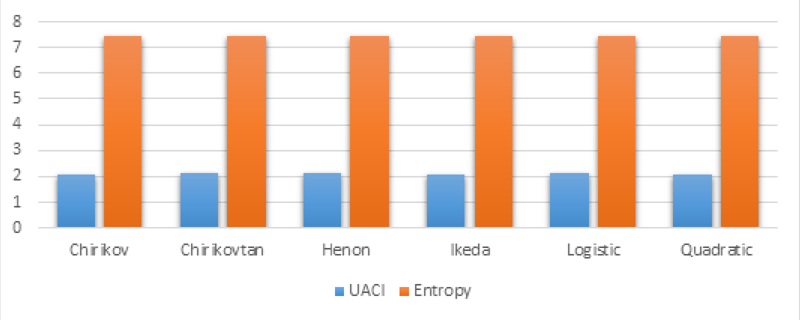


Fig. 38: UACI and Entropy measurements for DWT based technique..

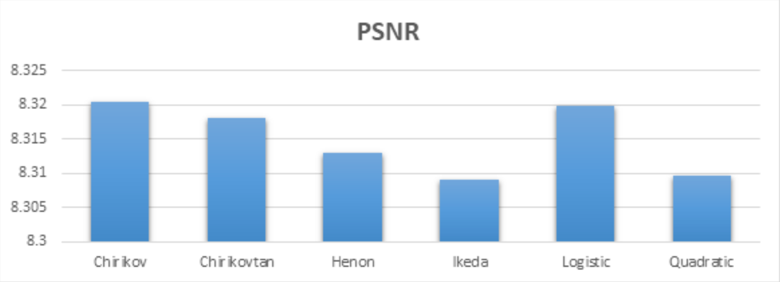


Fig. 39: PSNR for DWT based technique.

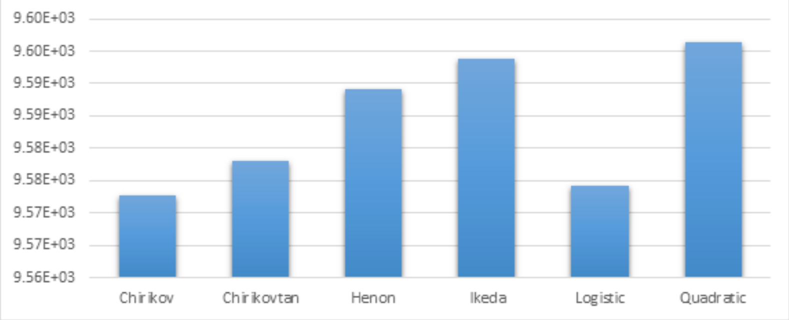


Fig. 40: MSE measurements for DWT based technique.

- *Without adding host image*

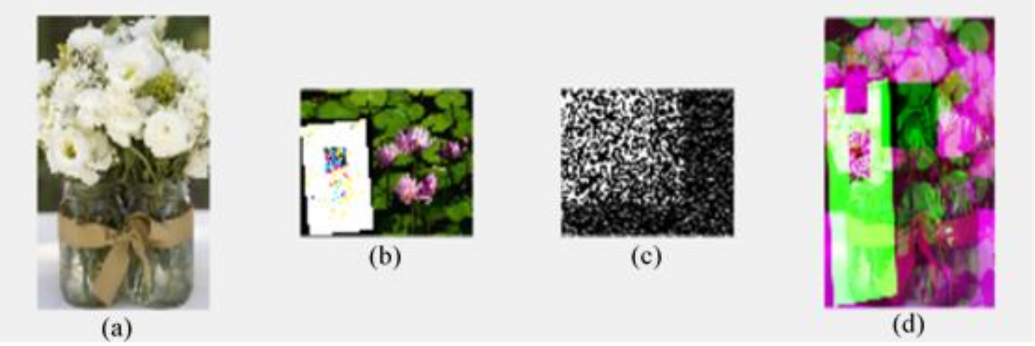
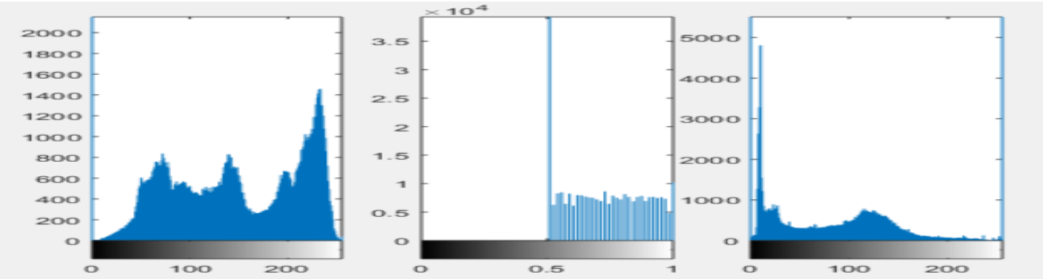


Fig. 41: (a) original, (b) stego, and (c) watermarked image (d) decrypted images for DCT based technique.



(a) (b) (c)

Fig. 42: The histogram of; (a) original (b) encrypted, and (c) decrypted images for DCT based technique.

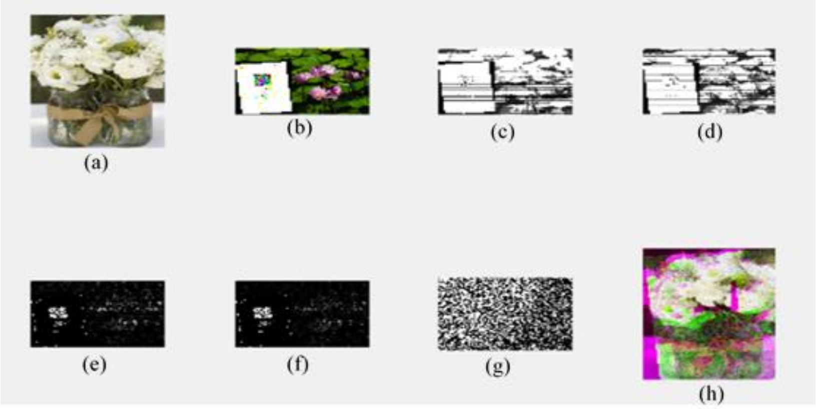
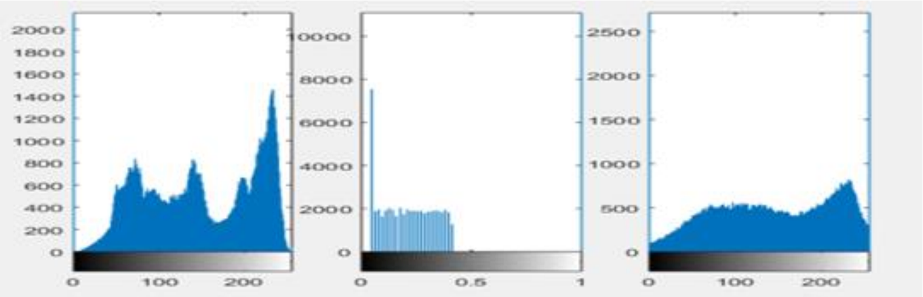


Fig. 43: (a) original, (b) stego (c) LL, (d) LH, (e) HL, (f) HH of encrypted, (g) watermarked image, and (h) decrypted images for DWT based technique.



(a) (b) (c)

Fig. 44: The histogram of (a) original (b) encrypted, and (c) decrypted images for DWT based technique.

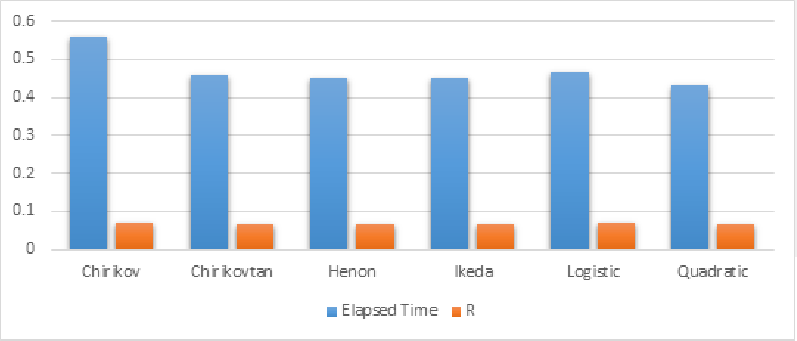


Fig. 45: Time and CC measurements for DCT based technique.

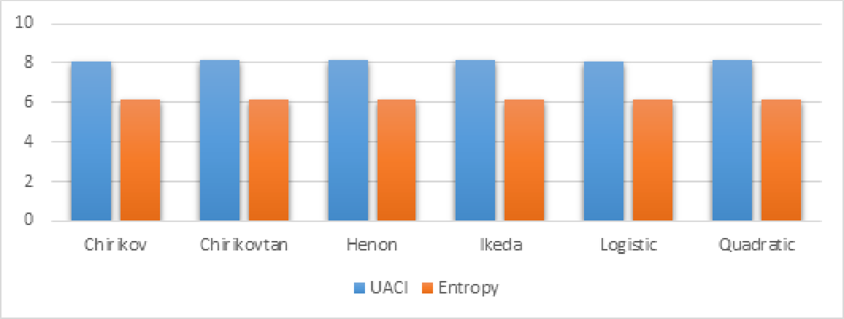


Fig. 46: UACI and Entropy measurements for DCT based technique.

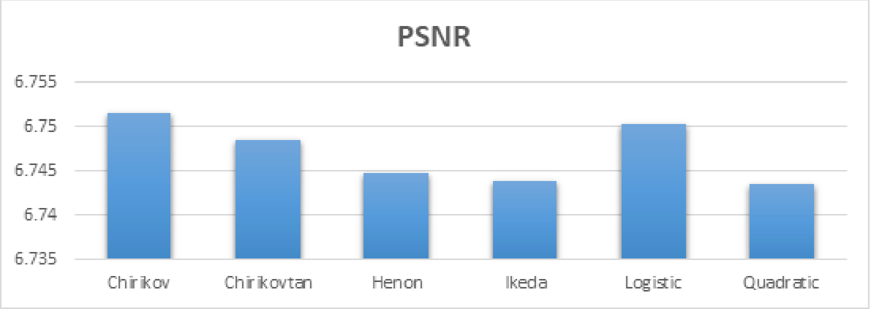


Fig. 47: PSNR for DCT based technique.

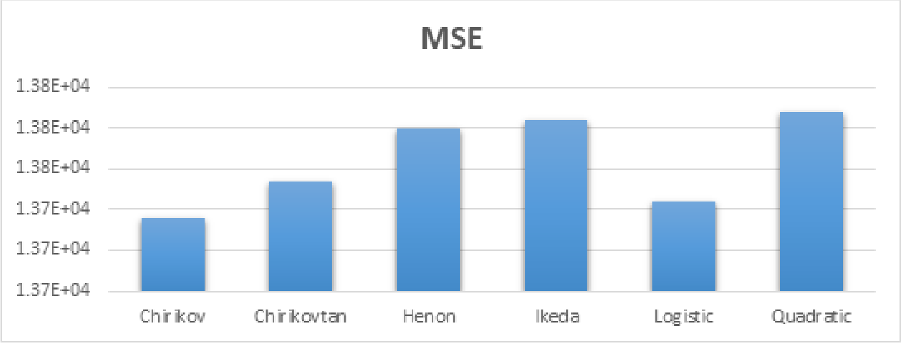


Fig. 48: MSE measurements for DCT based technique.

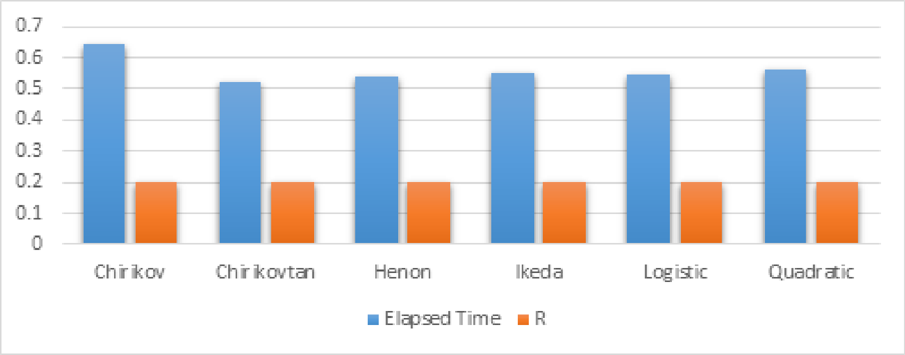


Fig. 49: Time and CC measurements for DWT based technique.

From measurements shown in figures (45-48) it has been found that Quadratic map has provided minimum elapsed time for DCT-based method, Chirikov map has given the closer value to one for cross correlation coefficient, the largest PSNR and the least MSE and Ikeda map has given the closer value for UACI to practical value of 33%.

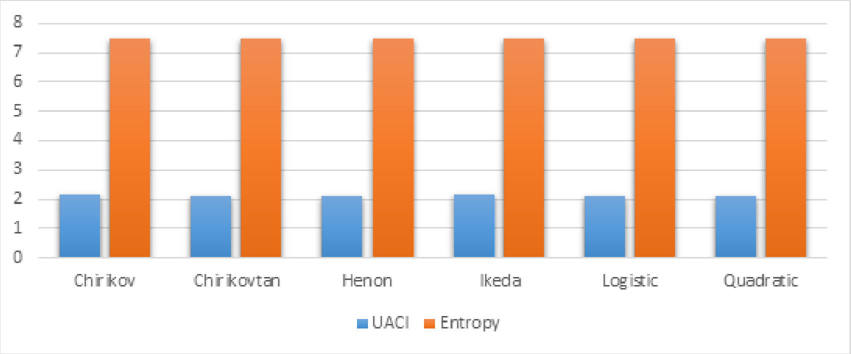


Fig. 50: UACI and Entropy measurements for DWT based technique.

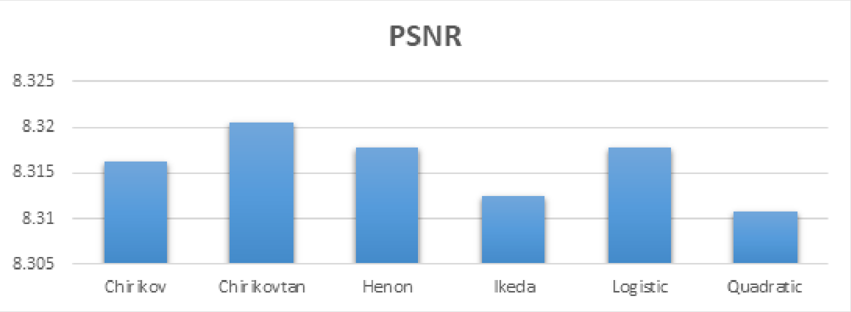


Fig. 51: PSNR for DWT based technique.

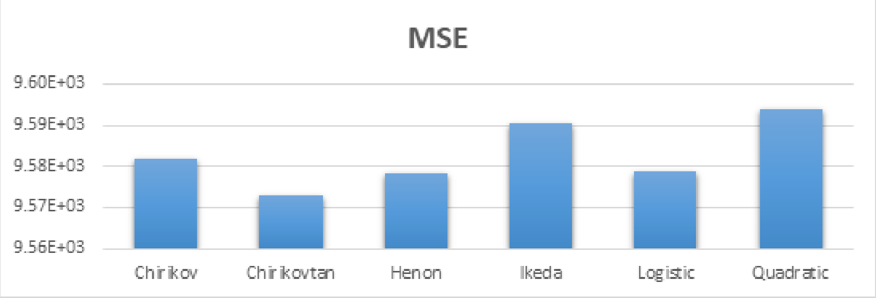


Fig. 52: MSE measurements for DWT based technique.

Analysis of measurements presented in figures (49-52) indicates notable performance attributes of the Chirikovtan map within the DWT-based method. Specifically, it demonstrates minimal elapsed time, a correlation coefficient closer to one, the highest PSNR, and the lowest MSE. Additionally, when utilizing the Chirikov map, it achieves a UACI value closer to the practical benchmark of 33%. Overall, both DCT and DWT based techniques exhibit enhanced performance ratios compared to traditional methods. For instance, with the Chirikov map, the DCT-based approach demonstrates approximately a 91% improvement in MSE, a 9.9% enhancement in PSNR, and about a 71% improvement in UACI. Conversely, the DWT-based technique with the Chirikov Map yields enhancement ratios of 8.7% in MSE, 5% in PSNR, and 61.7% in UACI.

5. CONCLUSION AND FUTURE SCOPE

With the continuous proliferation of information technology, safeguarding data during transmission from unauthorized access has emerged as a crucial concern. Consequently, the development of techniques capable of securing data and defending against various forms of attacks has become imperative. This paper introduces a proposed technique that combines steganography and watermarking for digital color images. The randomness inherent in these techniques is achieved through the use of six different chaotic maps for generating random keys. These chaotic maps significantly enhance the randomness of the keys compared to traditional random keys, making the proposed methods suitable for applications requiring high levels of authentication, such as federal government agencies and medical imagery. After a thorough investigation, it was determined that the three proposed techniques outperformed traditional methods in several aspects: (i) achieving the minimum MSE value, (ii) obtaining a larger cross-correlation coefficient value, (iii) maximizing PSNR, (iv) closely approximating the practical value of UACI to 33%, and (v) maintaining the entropy value of the decrypted image close to the original. These algorithms demonstrated high robustness against severe composite attacks, although they introduced increased complexity to the security system. Simulation results of hybrid watermarking and steganography, particularly with the DCT method, showed a UACI value closer to the practical benchmark of 33%, suitable for applications such as retail stores and federal government agencies. Conversely, the DWT-based method exhibited a decrypted image histogram closer to the original, making it applicable in political and governmental contexts. Thus, the proposed algorithm is recommended for real-time applications where high levels of security are necessary. Future directions for research include exploring hybrid combinations of chaotic maps with different parameters for generating keys, implementing the proposed methods on hardware platforms such as Field

Programmable Gate Arrays (FPGAs) and microcontrollers, and extending the techniques to digital color videos.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1.] A.A. Abbasi et al., Evolutionary-based image encryption using biomolecules and non-coupled map lattice, Optics and Laser Technology, (2021), https://doi.org/10.1016/j.optlastec.2021.106974

[2.] Hussain, I., N.A. Azam, and T. Shah, Stego optical encryption based on chaotic S-box transformation. Optics & Laser Technology, 61: p. 50-56, (2014), https://doi.org/10.1016/j.optlastec.2014.01.018

[3.] U. Erkan et al., 2D hyperchaotic system based on Schaffer function for image encryption, Expert Systems with Applications, (2023), https://doi.org/10.1016/j.eswa.2022.119076

[4.] Anees, A., et al., A technique for digital steganography using chaotic maps. Nonlinear Dynamics, 75(4): p. 807-816, (2014), DOI: 10.1007/s11071-013-1105-3

[5.] Aziz, M., M.H. Tayarani-N, and M. Afsar, A cycling chaos-based cryptic-free algorithm for image steganography. Nonlinear Dynamics, 80 (3): p. 1271-1290, (2015), DOI: 10.1007/s11071-015-1943-2

[6.] DeIlinger, T.M., et al., Glycogen storage disease and von Willebrand's disease implications for dental treatment: Dental management of a pediatric patient. Special Care in Dentistry, 18(6): p. 243-246, (1998), doi: 10.1111/j.1754-4505.1998.tb01641.x.

[7.] Priyanka et al., Yolo-based roi selection for joint encryption and compression of medical images with reconstruction through super-resolution network, Future Gener Comput Syst, (2024), https://doi.org/10.1016/j.future.2023.08.018

[8.] QinM. et al., Expanded multi-scroll attractor system analysis and application for remote sensing image encryption, Appl Math Model, (2024), https://doi.org/10.1016/j.apm.2023.08.021

[9.] ChaiX. et al., Combining improved genetic algorithm and matrix semi-tensor product (stp) in color image encryption, Signal Process, (2021), https://doi.org/10.1016/j.sigpro.2021.108041

[10.] BhowmikS. et al., Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm, J Inf Secur Appl, (2023), https://doi.org/10.1016/j.jisa.2022.103391

[11.] LinH. et al., Memristor-coupled asymmetric neural networks: Bionic modeling, chaotic dynamics analysis and encryption application, Chaos Solitons Fractals, (2023), https://doi.org/10.1016/j.chaos.2022.112905

[12.] HaoW. et al., Corrigendum to a hybrid neqr image encryption cryptosystem using two-dimensional quantum walks and quantum coding signal processing, 205, 108890, Signal Process, (2023), https://doi.org/10.1016/j.sigpro.2023.109012

[13.] LaiQ. et al., Design and realization of discrete memristive hyperchaotic map with application in image encryption, Chaos Solitons Fractals, (2022), https://doi.org/10.1016/j.chaos.2022.112781

[14.] LiuH. et al., Mutil-medical image encryption by a new spatiotemporal chaos model and

DNA new computing for information security, Expert Syst Appl, (2024), https://doi.org/10.1016/j.eswa.2023.121090

[15.] ManZ. et al., Research on cloud data encryption algorithm based on bidirectional activation neural network, Inform Sci, (2023), https://doi.org/10.1016/j.ins.2022.11.089

[16.] JamalS.S. et al., Region of interest-based medical image encryption technique based on chaotic s-boxes, Expert Syst Appl, (2024), https://doi.org/10.1016/j.eswa.2023.122030

[17.] NairA. et al., Colour image encryption algorithm using rubik's cube scrambling with bitmap shuffling and frame rotation, Cyber Secur Appl, (2024), https://doi.org/10.1016/j.csa.2023.100030

[18.] BibanG. et al., Image encryption based on 8d hyperchaotic system using fibonacci q-matrix, Chaos Solitons Fractals, (2023), https://doi.org/10.1016/j.chaos.2023.113396

[19.] WinarnoE. et al., Integrated dual hyperchaotic and josephus traversing based 3d confusion-diffusion pattern for image encryption, J King Saud Univ Comput Inf Sci, (2023), DOI: 10.1016/j.jksuci.2023.101790

[20.] KongX. et al., A class of 2n+1 dimensional simplest hamiltonian conservative chaotic systems and fast image encryption schemes, Appl Math Model, (2024), https://doi.org/10.1016/j.apm.2023.10.004

[21.] ToktasA. et al., A robust bit-level image encryption based on bessel map, Appl Math Comput, (2024), https://doi.org/10.1016/j.amc.2023.128340

[22.] Roy, R., A. Sarkar, and S. Changder, Chaos based edge adaptive image steganography. Procedia Technology, 10: p. 138-146, (2013), https://doi.org/10.1016/j.protcy.2013.12.346

[23.] Bandyopadhyay, D., et al., A novel secure image steganography method based on chaos theory in spatial domain, International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1): p. 11-22, (2014), DOI : 10.5121/ijsptm.2014.3102

[24.] Bilal, M., et al., Chaos based Zero-steganography algorithm, Multimedia tools and applications, 72(2): p. 1073-1092, (2014), DOI: 10.1007/s11042-013-1415-y

[25.] Benrhouma, O., O. Mannai, and H. Hermassi. Digital images watermarking and partial encryption based on DWT transformation and chaotic maps. In 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15), (2015), DOI: 10.1109/SSD.2015.7348112

[26.] 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, 77 (4): p. 4863-4882, (2018), DOI: 10.1007/s11042-016-3862-8

[27.] Rajendran, S. and M. Doraipandian, Chaotic Map Based Random Image Steganography Using LSB Technique. IJ Network Security, 19(4): p. 593-598, (2017), DOI: 10.6633/IJNS.201707.19(4).12

[28.] Razzaq, M.A., et al., Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 8 (5), (2017), DOI: 10.14569/IJACSA.2017.080528

[29.] HASHIM, M., et al., A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN. Journal of Theoretical & Applied Information Technology, 96 (4), (2018)

[30.] Valandar, M.Y., et al., An integer wavelet transform image steganography method based on 3D sine chaotic map. Multimedia Tools and Applications, 78 (8): p. 9971-9989, (2019), https://doi.org/10.1007/s11042-018-6584-2

[31.] Bhnassy, M.A., et al., Image encryption and watermarking combined dynamic chaotic hopping pattern with double random phase encoding DRPE, Optical and Quantum Electronics, 51 (7), (2019), https://doi.org/10.1007/s11082-019-1961-2

[32.] S. Gao et al., A 3D model encryption scheme based on a cascaded chaotic system, Signal Processing, (2023), https://doi.org/10.1016/j.sigpro.2022.108745