Hybrid chaotic map with L-shaped fractal Tromino for image encryption and decryption

Sharon Rose Victor Juvvanapudi[1], Pullakura Rajesh Kumar[2], Konala Veera Venkata Satyanarayana Reddy[2]
[1]Electronics and Communication Engineering Department, Pragati Engineering College, Surampalem, India
[2]Electronics and Communication Engineering Department, Andhra University, Visakhapatnam, India

Article Info

Article history:

Received May 25, 2023
Revised Aug 2, 2023
Accepted Sep 6, 2023

Keywords:

Decryption
Encryption
Hybrid chaotic map with L-shaped fractal Tromino
Integer wavelet transform and hybrid discrete cosine transform
Linear transformation
Watermarking approach

ABSTRACT

Insecure communication in digital image security and image storing are considered as important challenges. Moreover, the existing approaches face problems related to improper security at the time of image encryption and decryption. In this research work, a wavelet environment is obtained by transforming the cover image utilizing integer wavelet transform (IWT) and hybrid discrete cosine transform (DCT) to completely prevent false errors. Then the proposed hybrid chaotic map with L-shaped fractal Tromino offers better security to maintain image secrecy by means of encryption and decryption. The proposed work uses fractal encryption with the combination of L-shaped Tromino theorem for enhancement of information hiding. The regions of L-shaped fractal Tromino are sensitive to variations, thus are embedded in the watermark based on a visual watermarking technique known as reversible watermarking. The experimental results showed that the proposed method obtained peak signal-to-noise ratio (PSNR) value of 56.82dB which is comparatively higher than the existing methods that are, Beddington, Free, and Lawton (BFL) map with PSNR value of 8.10 dB, permutation substitution, and Boolean operation with PSNR value of 21.19 dB and deoxyribonucleic acid (DNA) level permutation-based logistic map with PSNR value of 21.27 dB.

Corresponding Author:

Sharon Rose Victor Juvvanapudi
Electronics and Communication Engineering Department, Pragati Engineering College
Surampalem, India
Email: jsr.victor@gmail.com

1. INTRODUCTION

The rapid development of digital applications and enhanced technologies has simultaneously created a huge demand in the security industry also [1], [2]. Security is one of the most vital parameters required for successfully transmitting information via the network, but is greatly impacted by increase in illegal activities pertaining to information misuse such as copying, editing [3]. The watermarking method is used for converting the image information to keep it confidential, hence making it difficult to be recognized by unauthorized persons [4], [5]. The watermarking method is known for its capability in retrieving the actual information without losing the significant data in it [6], [7]. The encrypted secret data is sent via internet or wireless networks to fulfill the need of securing the route of data transmission over distinct communication channels [8], [9]. Moreover, encryption of secret information prevents unapproved access, data destruction, and adjustment of data in data exchange [10], [11]. The existing researches are based on chaos image encryption technique which has robust properties with independent conditions [12], [13]. Computational systems based on internet, act as a lead for diversified watermarking techniques [14], [15]. The image encryption technique based on chaos approach is robust due to its furcating behavior [16], [17]. The deterministic conditions in chaos, specify the randomized behavior with deterministic system [18]. The existing encryption approaches are based on pixel transformation of digital images and random sequences [19]. There are different algorithms used in digital image encryption techniques that involve image compression coding, random sequence, pixel transformation, and image key [20], [21]. It is challenging to interpret the image encryption methodology due to its quality of randomness which makes it more reliable for digital image encryption applications [22]. The high dimension space-based chaos encryption technology has issues in uniformity of pixel encryption, possesses low efficiency and poor processing. The literature review of various methodologies involved in image encryption is described as follows.

Rani *et al.* [23] developed an image encryption model concerning individual colored and grayscale images using a novel fused magic cube. This developed fused magic cube was having both diffusion phases and confusion phases for performing image encryption that eliminated additional components. The visual inspection of the encrypted images through the human eye showed that the original image’s information was not present. Patro and Acharya [24] suggested an effective model known as dual layer cross-coupled chaotic map for performing encryption of images. The suggested approach varied from the image encryption schemes and it was based on two layered chaotic maps that operate on permutations and diffusions. However, the suggested approach was complex while evaluating it with existing approaches.

Zefreh *et al.* [25] introduced a hybridized approach which comprised of deoxyribonucleic acid (DNA) computation, chaotic systems and hash functions, utilized in the process of encrypting the images. The suggested approach accomplished the mapping function which was on the basis of logistic map that helped to create randomized images. However, the suggested approach achieved better security in image encryption schemes. Ali and Ali [26] deployed a Chaos based image encryption technique which was comprised with Boolean operation and permutation substitution. The developed phase was considered the first performed permutation process for the digital image using the chaotic map. However, the model does not consider the security while encrypting real time images. De *et al.* [27] developed three different chaotic maps for the process of secure image encryption. The image encryption distinctly captured the required position for providing multimedia data security. However, the developed model needed improvement in terms of verification. The major contributions of this research are listed as follows: i) to propose a hybrid chaotic encryption with an L-fractal Tromino module for encrypting the images using hybrid mapping-based chaos encryption which consists of logistic and Henon maps and ii) to perform direct and indirect recursions by integrating the chaos map with an L-fractal Tromino-based encryption technique. The remaining of the manuscript is organized in the following way: The proposed methodology of this research paper is deliberated in Section 2. The results obtained through analysis of the proposed approach is listed in Section 3 and the overall conclusion of this research is listed in Section 4 of the manuscript.

2. PROPOSED METHOD

Usually, for experimental investigation, two types of images are considered in image watermarking, namely, cover and secret images. The cover image is used to maintain the secret image without any noise so that it appears like the original image. The flow diagram of the collected grey scale as well as color sample images are represented in Figure 1. Generally, the cover image is employed for implantation of the secret message (text or image), as it needs to be noiseless and similar to the original image. For instance, the various methods involved in the encryption process include peppers, baboon, Monalisa, and Saturn.

2.1. Pre-processing

After the stage of collecting the digital images, the secret image is encrypted with the help of logistic and Henon maps. The proposed hybrid chaotic encryption is applied on the secret image to embed it with a cover image and convert it into transform domain. Chaos encryption with hyper chaotic fractal encryption is used for mapping, which prevent information loss and provide assurance of data safety, offer low computation complexity and enhances the security and efficiency of the information transmission.

2.2. Encryption and decryption using proposed hybrid chaotic mapping with L-shaped fractal Tromino

After collecting the pre-processed images, hybrid mapping is performed to encrypt the secret image by a chaos encryption process. At present, researchers show enormous interest in chaos encryption because of its inherent features. Commonly, a chaotic image possesses two stages, namely, permutation and diffusion. During diffusion, all individual pixel values are modified by the application of chaos sequences. For every stage of permutation, without altering the values of the image pixel, the scrambled pixels over the entire image are positioned and considered for pixel permutation. In this study, the stages of permutation and diffusion are carried out by the usage of invoked keys k_i, and logistic map value along with Henon map. The most primitive chaotic maps in chaos encryption are Henon and logistic maps that are mentioned in (1) and (2). One of the polynomial maps that display chaotic behavior is the logistic map. One such map is provided in (1).

$$l_{map} = \mu x_n(1 - x_{n-1}) \tag{1}$$

where, x_n denotes a chaos sequence between the range [0, 1], and μ denotes the control parameter of the range $\mu \in (3.57,4)$. As the parameter approaches four, sensitivity towards initial conditions by the chaotic system improves. With correspondence to a logistic map, Henon map is a non-linear one that is reversible and two-dimensional by nature that iterates point (x_n, y_n), as indicated in (2).

$$h_{map} = 1 - ax_n^2 + y_n,\ y_{n+1} = bx_n \tag{2}$$

where, $a \in (0,1.4),\ b \in (0.2, 0.314)$ denote controlled parameters. Henon map works depending on parametric values obtained from hybrid maps with generated keys represented as K_i. As the next step, the chaotic orbit is sorted and permutated to attain plain or diffused images using (3) and (4).

$$x_{n+1} = l_{map} + h_{map} \tag{3}$$

$$mim(i) = permut \oplus K_i\big(x_{n+1}\ p(i)\big), i = 1,2,3, \dots .p \times q \tag{4}$$

where, q and p represent the height and width of the plain image respectively, $p(i)$ indicates the value of actual image pixels, and $mim(i)$ represents the value of the minimal image pixel. Finally, for the permuted image, a cipher key is generated and by using a hybrid chaotic orbit, diffusion of the permuted image is performed. Thus, the output obtained at the diffusion stage is cipher image $c(i)$ which is shown in (5).

$$c(i) = mim(i)\ , i = 1,2,3, \dots p \times q \tag{5}$$

The generated output images now undergo fractal Tromino operations for enhancing the image encryption. The module functions are designed based on direct and indirect recursions combined with a dividing-conquering strategy to encrypt and decrypt the applications of colorful images.

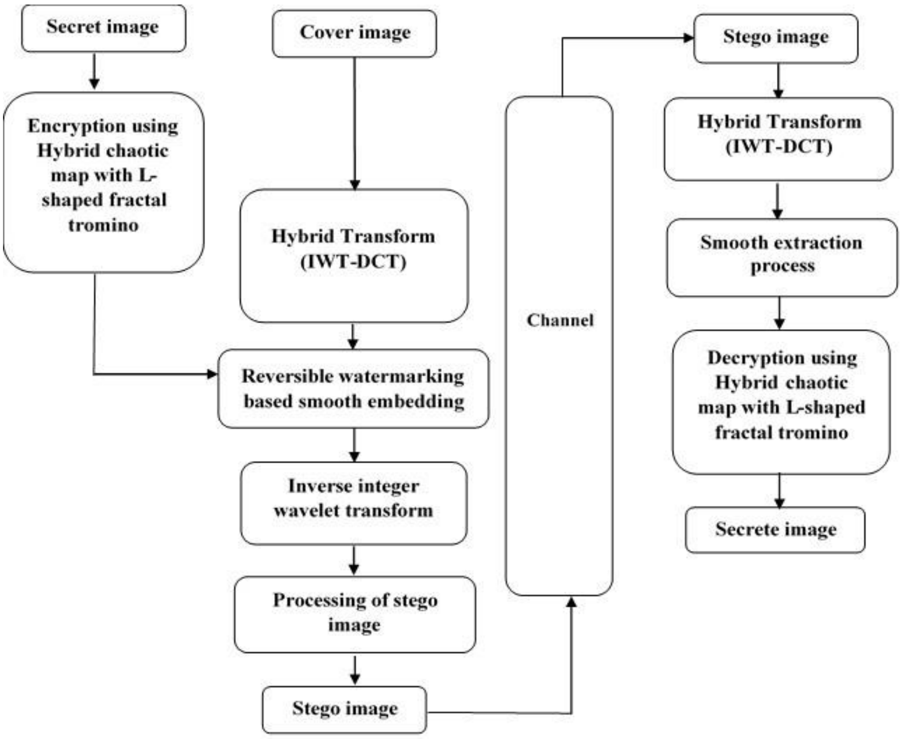
Secret image
Encryption using Hybrid chaotic map with L-shaped fractal tromino
Cover image
Hybrid Transform (IWT-DCT)
Reversible watermarking based smooth embedding
Inverse integer wavelet transform
Processing of stego image
Stego image
Channel
Stego image
Hybrid Transform (IWT-DCT)
Smooth extraction process
Decryption using Hybrid chaotic map with L-shaped fractal tromino
Secrete image

Figure 1. Flow diagram for the proposed hybrid chaotic with fractal Tromino model

The Figure 2 exhibits the overall process involved in embedding the secret image in the cover image. Initially, in Figure 2(a) the cover image is obtained as input and the secret image in Figure 2(b) is selected. In Figure 2(c), encryption of Figure 2(b) is performed to encrypt the color image and the fractal Tromino is obtained from encrypted color image presented in Figure 2(d). Figure 2(d) is a fractal chessboard covering algorithm for any size chessboard that includes a special random initial grid. Then the fractal Tromino of the secret image is embedded into input cover image to obtain stego image in Figure 2(e) and finally, the secret image is reconstructed from the stego image, and is presented in Figure 2(f).

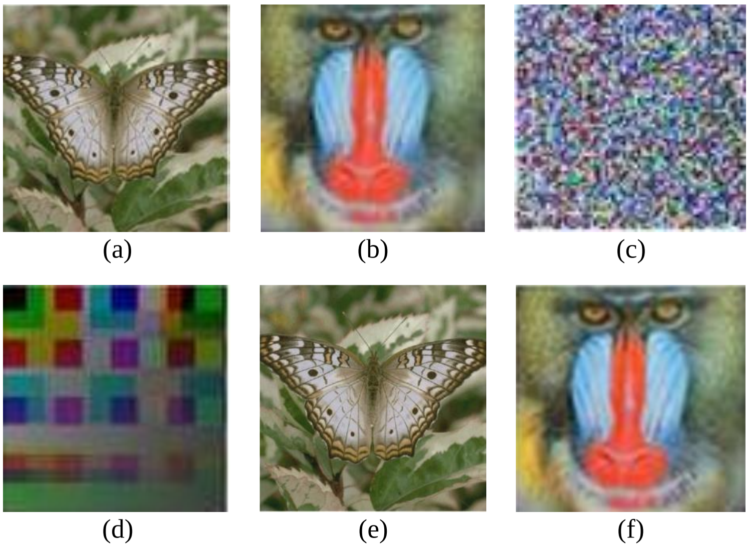

Figure 2. Sample of (a) input image which is used as cover image and (b) secret image which is to be embedded in cover image, (c) the color image obtained through encryption of secret image, (d) fractal Tromino of the encrypted secret image, (e) stego image where the fractal Tromino is embedded and (f) reconstructed secret image

Generation of fractal Tromino using the following steps:

Step 1: An R-dimensional is created with dimensions $M \times 3\,N$ where $M \times N \times 3$ are the plain image's dimensions and 3 refers to red, green, blue (RGB) channels

Step 2: Two 8-bit long random keys k_1 and k_2 are generated.

Step 3: The Matrix values generated above are updated by applying (6) and its rule:

$$R(i,j) = \begin{cases} mod(j,f) & if\ mod(i,k_2 \times c) < k_1 \times c \\ mod(i,f) & if\ mod(j,k_2 \times c) > k_1 \times c \\ mod(c-i,c) & otherwise \end{cases} \tag{6}$$

from (6) c is calculated by using (7).

$$c = \sqrt{(255-m) \times m} \tag{7}$$

The value of c is wrapped off to the closest digit, where m is the mean of the matrix in (7) spawned in the first step.

Step 4: The matrix modified in step 3 is reshaped to the dimension $M \times N \times 3$. This is the pled fractal Tromino. The obtained fractal image is shown in Figure 2(d) which shows the image of exclusive-OR(XOR) of the fractal as shown in (8).

$$fractal\ Tromino\ (image) = mim(i)\ \oplus R(i,j) \tag{8}$$

2.3. Hybrid transform (IWT-DCT)

In the present research work, IWT and DCT are combined to form a hybrid model for the process of encryption. Utilizing integer wavelet transform (IWT) approach [3] the image is converted into an integer transform domain. In general, there are four levels of sub-bands in IWT known as low-low (LL), high-high (HH), low-high (LH), and high-low (HL). In the given four sub-bands, the LL sub-band looks closely related to the original image and is hence considered. The algorithm is used for JPEG standards and is based on two dimensions with 8×8 DCT blocks that are robust for compression and also for performing filtering process. The shortcoming of DCT is its main features that are used for image conversion from the spatial domain towards the frequency domain which gives diminished time-frequency properties to an image. To overcome this, inverse discrete cosine transforms (IDCT) [16] is used to reconstruct a sequence by using the coefficients of its discrete cosine transform (DCT). IDCT plays the counterpart of the function which helps the embedding process to perform extraction using reversible watermarking.

2.4. Embedding process and extraction process using reversible watermarking

The present research work utilizes a watermarking system that contains pseudo-random sequence having M real numbers $X = f_{x_1}, f_{x_2}$wherein each of them has a value x_i which is a random number with standard distribution. The process of watermarking is seen as process communication with two steps. Firstly, watermark casting is done and the signal is represented with the watermark. An actual image acts as an intentional attack and the image distortion represents noises in the signals that are transmitted among the channels. The image distortion is represented as the channel noises and when the watermark is detected, the signal is obtained and extracted from the corrupted image.

2.4.1. Watermark casting

The watermark casting has 8×8 DCT with an 8×8 image I and the coefficients generated from the DCT are recognized as the zig-zag scan. This is done by compressing the selected co-efficients and generating vector $T = \{t_1, t_2, \dots, t_L, t_{L+1}, \dots., t_{L+M}\}$. Obtaining a trade-off among the invisibility and robustness of an image demands the use of image processing techniques and skipping the L coefficients with a watermark $X = x_1, x_2, , \dots., x_M$. 1000 pseudo-random sequences are chosen and embedded in M numbers resulting in a new vector $T' = \{t_1,\ t_2, \dots, t_L, t'_{L+M}\}$ that follows the rule as shown in (9).

$$T'_{L+i} = t_{L+i} + \propto |t_{L+i}| x_i \tag{9}$$

where $i = 1,2, \dots, M$. The vector T' is further inserted back in the zig-zag scan. Then the inverse DCT algorithm is applied to deliver the watermarked image I'.

2.4.2. Visual masking

For enhancement of the watermark's robustness, human visual system (HVS) characteristics are exploited to adapt the watermark for the image's signature. Actual image$I$ and the watermarked one I_0 are combined through individual pixels by weighted factor to obtain a new watermarked one$I$. The characteristics of HVS are taken into account by the weighting factor j so that diminishing of the watermark does not occur in characterized regions of low noise sensitivity. The simplest step is to choose and describe each of the pixels in the square block having the size as$R$. The calculated sample variance is normalized with the block variances that are maximum in number. Through the normalized factor $\beta_{i,j}$, variance is calculated with the pixel value as $y_{i,j}$. Thus, the visual masking of the parameter is exploited and the (1) is computed as the value of an image used for weighting by the factor $\beta_{i,j}$ without visible image conversion.

2.4.3. Watermark detection

In this, the image is possibly present with noise as I and $N \times N$ in the DCT is applied for I^*. The DCT coefficients are re-ordered for the scan and the coefficients are selected in the range $(L+1)^{th}$-$(L+M)^{th}$ for generating T^* as a vector. The value of the possible different mark Y is expressed as shown in (10).

$$z = \frac{Y \cdot T^*}{M} = \frac{1}{M} \sum_{i=1}^{M} y_i\, t^*_{L+i} \tag{10}$$

In the correlation comparison, the threshold is defined as z and it is important to define if the mark is present or absent. The application of water mark detection approach evaluates the threshold value S_z of the marked image in a direct manner. The threshold value of the image based on watermark detection is evaluated using (11):

$$S_z = \frac{\overline{\alpha}}{3M} \sum_{i=1}^{M} |t^*_i| \tag{11}$$

3. RESULTS AND DISCUSSION

The performance metrics of the proposed method are evaluated in this section and the proposed method is simulated using MATLAB R2018a. The section describes various performance measures utilized for evaluating the proposed method. The performance is evaluated by computing peak-signal to noise ratio (PSNR), mean square error (MSE), unified average changing intensity (UACI), structural similarity (SSIM) and normalized cross correlation (NCC).

3.1. Quantitative analysis

The results evaluated using the aforementioned methods are in terms of PSNR, SSIM, UACI, entropy, and NCC metrics. The gray and color images both have secret and cover images while processing their results and evaluating them. The secret image obtained Inf for the PSNR (dB) for the color images and gray images. For color image analysis, the value of SSIM obtained for the secret image is ‘1’ and the SSIM value for cover image is 0.996. As per gray image analysis, ‘1’ is the SSIM for the secret image and 0.988 SSIM is for the cover image. For the color image, the UACI performance metric is measured at 33.46 for the secret image and 33.46 for the cover image as well. Also, for the grey image the UACI obtained for the secret image is 33.46 and 33.46 for the cover image. The entropy value is obtained as 7.38 for the secret image and 7.73 for the cover image with respect to the color image. The secret image obtained an entropy value of 6.90 and the cover image obtained 7.33 with respect to the gray image. The value of NCC is obtained as 1 for the secret and cover images in the color image. For the gray image, the value of entropy is obtained as 1 in both secret image and the cover image. The results obtained from the proposed hybrid chaotic with L-shaped fractal Tromino encryption algorithm for the color as well as gray image is represented in Table 1 and Table 2 respectively.

Table 1. Results obtained for the proposed hybrid chaotic with L-shaped fractal Tromino encryption algorithm to the color image

Color image	PSNR	SSIM	UACI	Entropy	NCC
Secret image	Inf	1	33.46	7.38	1
Cover image	56.9	0.996	33.46	7.73	1

Table 2. Results obtained for the proposed hybrid chaotic with L-shaped fractal Tromino encryption algorithm with respect to the gray image

Gray image	PSNR	SSIM	UACI	Entropy	NCC
Secret image	Inf	1	33.46	6.90	1
Cover image	56.9	0.988	33.46	7.33	1

Table 3 displays the statistics of the performance analysis of the proposed hybrid chaotic with L-fractal Tromino which attained better performances in terms of PSNR, SSIM, UACI, entropy, and NCC. The proposed method obtained a PSNR value of 5.97 for the logistic algorithm, 5.97 for Henon, the hybrid chaotic model which has a combination of logistic and Henon obtained PSNR of 54.47, L-fractal Tromino obtained 6.94 for the PSNR values with respect to the secret image of color type image. Whereas, the proposed hybrid chaotic with L-fractal Tromino obtained inf in terms of PSNR values. The value of SSIM is -0.031 for the logistic algorithm, -0.031 for the Henon chaotic map generated negative values which is caused because of the covariance of the two images as it would generate negative values. Whereas the proposed hybrid chaotic map obtained 0.998 of SSIM value and the proposed hybrid chaotic with L-fractal Tromino obtained 1 as the SSIM value.

The results obtained while evaluating the proposed approach hybrid chaotic with L-fractal Tromino for gray secret image is presented in Table 4. The Table 5 depicted below shows the results obtained while evaluating the proposed approach based on color cover image. Finally, the results obtained while evaluating the proposed approach based on covered gray image is presented in Table 6.

Table 3. Qualitative results for color secret image

Secret image (Color)	PSNR	SSIM	UACI	Entropy	NCC
Hybrid Chaotic	54.47	0.99	33.46	7.95	1
Logistic	5.97	0	33.46	7.38	0.11
Henon	5.97	-0.031	33.35	7.38	0.39
L-fractal Tromino	6.94	-0.0009	33.46	7.69	0.40
Hybrid Chaotic with L-fractal Tromino	Inf	1	33.46	7.38	1

Table 4. Qualitative results for gray secret image

Secret Image (gray)	PSNR	SSIM	UACI	Entropy	NCC
Hybrid Chaotic	54.76	0.925	33.46	7.6	1
Logistic	7.45	0.007	33.46	7.45	0.46
Henon	14.28	0.003	33.46	6.43	0.50
L-fractal Tromino	Inf	1	33.46	6.90	1
Hybrid chaotic with L-fractal Tromino	Inf	1	33.46	6.90	1

Table 5. Qualitative results for color cover image

Cover Image	PSNR	SSIM	UACI	Entropy	NCC
Hybrid Chaotic	54.47	0.99	33.46	7.95	1
Logistic	56.79	0.39	33.42	7.73	0.12
Henon	56.80	0.39	33.43	7.71	0.23
L-fractal Tromino	56.81	0.33	33.45	7.70	0.56
Hybrid chaotic with L-fractal Tromino	56.82	0.99	33.46	7.69	1

Table 6. Qualitative results for gray cover image

Cover Image	PSNR	SSIM	UACI	Entropy	NCC
Hybrid Chaotic	54.76	0.92	33.46	7.59	1
Logistic	56.80	0.95	33.47	7.33	0.99
Henon	56.81	0.96	33.48	7.33	0.99
L-fractal Tromino	56.82	0.97	33.49	7.33	0.99
Hybrid chaotic with L-fractal Tromino	56.83	0.98	33.5	7.33	1

The results from Tables 4, 5, and 6 show that the proposed approach gives better results for overall metrics. For example, the qualitative result of the proposed approach for gray scale image is considered. The PSNR value of proposed approach is 56.83 whereas the same for the existing hybrid chaotic, logistic map, Henon map and L-fractal Tromino is 56.82. These results show the effectiveness of the proposed method when compared with existing ones. The graphical representation of PSNR value for the proposed hybrid chaotic with L-fractal Tromino model with other methods are represented in Figure 3.

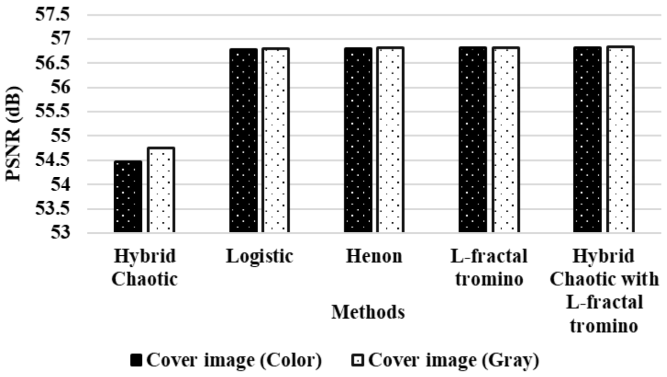

Figure 3. Graph obtained for the proposed hybrid chaotic with L-fractal Tromino model evaluated in terms of PSNR

3.2. Comparative analysis

In this section, the comparative results of proposed with existing approaches are analyzed in terms of PSNR, number of pixels change rate (NPCR), UACI, and entropy. The existing approaches are incapable in obtaining the original information as it displays lowered accuracy values. The visual inspection of the encrypted images proved that the image's original information was absent. The complexity of the developed model is minimized which helps to enhance the performance of encryption. The developed model provided security at its best which showed better image encryption and faster processing. The Table 7 depicts the comparative analysis of the proposed approach when compared with existing approaches listed in related works.

The results from the Table 7 show that the proposed hybrid chaotic with L-fractal Tromino has achieved better results in terms of PSNR, UACI, NPCR, and entropy. For example, the entropy of proposed method is achieved at a minimum value of 7.33 whereas the existing fused magic cube encryption approach, dual-layer and cross-coupled chaotic map, DNA level permutation-based logistic map, permutation substitution and Boolean operation and BFL map, all achieved their respective entropies of 7.97, 7.99, 7.35, 8, and 8. As the entropy value gets increased, randomization occurs which spreads the data beyond the limit and diminishes the accuracy of retrieving the secret image. So, the proposed approach utilized fractal encryption with the combination of the L-shaped Tromino theorem for enhancement of information hiding and helps to obtain the secret image without affecting the information.

Table 7. Comparative analysis

Authors	Method	PSNR (dB)	UACI	NPCR	Entropy
Rani *et al.* [23]	Fused magic cube encryption approach	-	33.83	99.59	7.97
Patro and Achary [24]	Dual-layer and cross-coupled chaotic map	-	33.47	99.62	7.99
Zefreh [25]	DNA level permutation-based logistic map	21.27	33.51	99.61	7.35
Ali and Ali [26]	Permutation substitution and Boolean operation	21.19	33.46	99.61	8
De *et al.* [27]	Beddington, free and Lawton (BFL) map	8.10	33.48	99.61	8
Proposed method	Hybrid chaotic with L-fractal Tromino	56.82	34.02	99.99	7.33

4. CONCLUSION

This research focuses on the enhancement of security in networks of real-world applications. In this proposed research, hybrid mapping is implemented to ensure that the secret image is private and integrated. Also, hybrid chaotic encryption with an L-fractal Tromino module is used for encrypting the images through chaos encryption which involves a hybrid mapping method, consisting of logistic and Henon maps. Further improvements can be made by combining the direct and indirect recursion with the proposed approach. The proposed approach effectively worked for huge images with less time complexity when compared with the existing approaches. The simulation results show that the proposed method improved efficiency and increase image encryption in terms of security. The proposed method obtained PSNR of 1, UACI of 0.23, a NPCR of 0.99, and entropy of 0.56. Thus, the proposed method is reliable and efficient for providing security for the images. In the future, the efficiency of the proposed methodology can be analyzed with deep learning techniques.

REFERENCES

[1] A. K. Sahu, M. Hassaballah, R. S. Rao, and G. Suresh, "Logistic-map based fragile image watermarking scheme for tamper detection and localization," *Multimedia Tools and Applications*, vol. 82, no. 16, pp. 24069–24100, Dec. 2023, doi: 10.1007/s11042-022-13630-4.

[2] F. Deeba, S. Kun, F. A. Dharejo, and H. Memon, "Digital image watermarking based on ANN and least significant bit," *Information Security Journal*, vol. 29, no. 1, pp. 30–39, Jan. 2020, doi: 10.1080/19393555.2020.1717684.

[3] G. Gambhir and J. K. Mandal, "Multicore implementation and performance analysis of a chaos based LSB steganography technique," *Microsystem Technologies*, vol. 27, no. 11, pp. 4015–4025, Feb. 2021, doi: 10.1007/s00542-020-04762-4.

[4] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, Art. no. 170316, Feb. 2023, doi: 10.1016/j.ijleo.2022.170316.

[5] P. Singh, K. J. Devi, H. K. Thakkar, and J. Santamaría, "Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness," *Entropy*, vol. 23, no. 12, p. 1650, Dec. 2021, doi: 10.3390/e23121650.

[6] J. Y. Wu, W. L. Huang, W. M. Xia-Hou, W. P. Zou, and L. H. Gong, "Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition," *Multimedia Tools and Applications*, vol. 79, no. 31–32, pp. 22727–22747, May 2020, doi: 10.1007/s11042-020-08987-3.

[7] S. Sharma, J. J. Zou, and G. Fang, "A novel multipurpose watermarking scheme capable of protecting and authenticating images with tamper detection and localisation abilities," *IEEE Access*, vol. 10, pp. 85677–85700, 2022, doi: 10.1109/ACCESS.2022.3198963.

[8] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 6, pp. 2951–2963, Jun. 2022, doi: 10.1016/j.jksuci.2019.04.008.

[9] W. Chen, N. Ren, C. Zhu, A. Keskinarkaus, T. Seppänen, and Q. Zhou, "Joint image encryption and screen-cam robust two watermarking scheme," *Sensors (Switzerland)*, vol. 21, no. 3, pp. 1–28, Jan. 2021, doi: 10.3390/s21030701.

[10] S. Mansoor and S. A. Parah, "HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing," *Multimedia Tools and Applications*, vol. 82, no. 19, pp. 28769–28796, Feb. 2023, doi: 10.1007/s11042-023-14542-7.

[11] R. Wang, H. Shaocheng, P. Zhang, M. Yue, Z. Cheng, and Y. Zhang, "A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain," *IEEE Access*, vol. 8, pp. 182391–182411, 2020, doi: 10.1109/ACCESS.2020.3004841.

[12] M. Khan, A. S. Alanazi, L. S. Khan, and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex and Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, Jul. 2021, doi: 10.1007/s40747-021-00460-4.

[13] J. S. Khan *et al.*, "Dynamic S-Box and PWLCM-based robust watermarking scheme," *Wireless Personal Communications*, vol. 125, no. 1, pp. 513–530, Feb. 2022, doi: 10.1007/s11277-022-09562-9.

[14] Y. Alghamdi, A. Munir, and J. Ahmad, "A lightweight image encryption algorithm based on chaotic map and random substitution," *Entropy*, vol. 24, no. 10, p. 1344, Sep. 2022, doi: 10.3390/e24101344.

[15] Attaullah, T. Shah, and S. S. Jamal, "An improved chaotic cryptosystem for image encryption and digital watermarking," *Wireless Personal Communications*, vol. 110, no. 3, pp. 1429–1442, Sep. 2020, doi: 10.1007/s11277-019-06793-1.

[16] A. M. Abdelhakim and M. Abdelhakim, “A time-efficient optimization for robust image watermarking using machine learning,” *Expert Systems with Applications*, vol. 100, pp. 197–210, Jun. 2018, doi: 10.1016/j.eswa.2018.02.002.

[17] W. H. Alshoura, Z. Zainol, J. Sen Teh, and M. Alawida, “A new chaotic image watermarking scheme based on SVD and IWT,” *IEEE Access*, vol. 8, pp. 43391–43406, 2020, doi: 10.1109/ACCESS.2020.2978186.

[18] D. Sravanthi, K. A. K. Patro, B. Acharya, and M. Prasanth Jagapathi Babu, “Simple permutation and diffusion operation based image encryption using various one-dimensional chaotic maps: A comparative analysis on security,” in *Lecture Notes in Networks and Systems*, vol. 94, Springer Singapore, 2020, pp. 81–96. doi: 10.1007/978-981-15-0694-9_9.

[19] M. Begum, J. Ferdush, and M. S. Uddin, “A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5856–5867, Sep. 2022, doi: 10.1016/j.jksuci.2021.07.012.

[20] Y. Luo, X. Ouyang, J. Liu, L. Cao, and Y. Zou, “An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system,” *Soft Computing*, vol. 26, no. 11, pp. 5409–5435, Jan. 2022, doi: 10.1007/s00500-021-06554-y.

[21] D. Liu, Z. Yuan, and Q. Su, “A blind color image watermarking scheme with variable steps based on Schur decomposition,” *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 7491–7513, Dec. 2020, doi: 10.1007/s11042-019-08423-1.

[22] P. V. Sanivarapu, K. N. V. P. S. Rajesh, K. M. Hosny, and M. M. Fouda, “Digital watermarking system for copyright protection and authentication of images using cryptographic techniques,” *Applied Sciences (Switzerland)*, vol. 12, no. 17, Art. no. 8724, Aug. 2022, doi: 10.3390/app12178724.

[23] N. Rani, S. R. Sharma, and V. Mishra, “Grayscale and colored image encryption model using a novel fused magic cube,” *Nonlinear Dynamics*, vol. 108, no. 2, pp. 1773–1796, Feb. 2022, doi: 10.1007/s11071-022-07276-y.

[24] K. A. K. Patro and B. Acharya, “An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption system,” *Nonlinear Dynamics*, vol. 104, no. 3, pp. 2759–2805, Apr. 2021, doi: 10.1007/s11071-021-06409-z.

[25] E. Z. Zefreh, “An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions,” *Multimedia Tools and Applications*, vol. 79, no. 33–34, pp. 24993–25022, Jun. 2020, doi: 10.1007/s11042-020-09111-1.

[26] T. S. Ali and R. Ali, “A new chaos based color image encryption algorithm using permutation substitution and Boolean operation,” *Multimedia Tools and Applications*, vol. 79, no. 27–28, pp. 19853–19873, Mar. 2020, doi: 10.1007/s11042-020-08850-5.

[27] S. De, J. Bhaumik, and D. Giri, “A secure image encryption scheme based on three different chaotic maps,” *Multimedia Tools and Applications*, vol. 81, no. 4, pp. 5485–5514, Dec. 2022, doi: 10.1007/s11042-021-11696-0.

BIOGRAPHIES OF AUTHORS

Sharon Rose Victor Juvvanapudi is presently associate professor of ECE in Pragati Engineering College, Surampalem. She graduated in electronics and communication engineering from MVSREC affiliated to Osmania University, Hyderabad in 2000. She received her M.Tech in digital systems and computer electronics from JNT University, Ananthapur in 2003. She has 16 years of teaching experience. She is Ph.D. at Andhra University College of Engineering, Visakhapatnam, India. She is a member of ISTE, IAENG. Her research interests are in the area of image processing, signal processing, and machine learning. She can be contacted at email: jsr.victor@gmail.com.

Pullakura Rajesh Kumar is presently professor and head of the Department of Electronics and Communication Engineering, Andhra University College of Engineering (Autonomous), Visakhapatnam. He graduated from CBIT affiliated to Osmania University, Hyderabad. He received his ME and Ph.D from Andhra University, Visakhapatnam. Earlier he worked in Bapatla Engineering College, GVP College of Engineering, GITAM College of Engineering, Shri Vishnu Engineering College for Women. He joined as associate professor in Andhra University in the year 2006. He has 25 years of teaching experience and guided many students for their thesis work. He has published more than 90 research papers in various national and International Journals/Conferences. Presently he is guiding 18 research scholars. He is member of IEEE, IETE, ISTE, EMCE(I) and Instrument Society of India. He was vice chairman, secretary and presently chairman, IETE Visakhapatnam Centre. His research interests are radar signal processing, image processing and bio-medical signal processing. He can be contacted at email: rajeshauce@gmail.com.

Konala Veera Venkata Satyanarayana Reddy is presently honorary professor and formerly professor of electronics and communication engineering in Andhra University College of Engineering, Visakhapatnam. He has published more than 80 journal and conference papers. He has 36 years of experience in teaching and research besides possessing 3 years of industrial experience. He is a Fellow of Institute of Electronics and Telecommunication Engineers (FIETE) and Life Member Society for EMI/EMC Engineers, India. He has produced more than 15 Ph.D. He has guided more than 70 M.E and M.Tech projects. His areas of research interest are communication systems, signal processing and satellite communications. He can be contacted at email: konalavs51@yahoo.com.