A Neoteric Image Encryption System Using Nonlinear Chaotic Strange Attractors

Suchindran Srinivasan, Varun Subramaniam, V. S. Ramya Lakshmi, and N. R. Raajan

Abstract The science of securing the message by altering the information into an uninterruptable form so that it cannot be recognized is called cryptography. Currently, a wide range of algorithms have been employed for image encryption, but chaos blended image encryption techniques are preferred due to their excellent security and speed. This scheme primarily consists of two steps: chaos-based diffusion and scrambling of the pixel locations. This paper provides a concise introduction to chaotic image encryption and then an analysis of the properties of the chaotic attractors used. The inherent properties of the attractors which are relevant to cryptography are the salient reasons for their utilization in information security applications. Here, we introduce an innovative technique to encrypt a standard RGB image using the pseudorandom numbers generated by the 3D chaotic attractors which has an advanced response to a broad range of control parameters. The unpredictability of the attractors and its sensitivity to initial conditions has enhanced the security of the image immensely. This encryption scheme involves the chaotic bit streams and the image parameters being combined over a simple logical operation, thus reducing the possibility of retrieving the original data by intruders. From the results of the variety of statistical tests conducted, we come to an inference that encryption algorithm proposed is up to the mark and can be deployed for safe transmission of information.

Keywords Cryptography · Encryption · Chaotic attractors · Diffusion

1 Introduction

A large amount of data is being relayed over the Internet and this not only includes text but also image, audio and multimedia files. With the accelerated advancement in technology, transmission of information through a safe and secure network and its storage has become a matter of great importance. It is imperative to shield the cyber-related information from illegal retrieval, copying and distribution by attackers [1].

S. Srinivasan (✉) · V. Subramaniam · V. S. Ramya Lakshmi · N. R. Raajan
SASTRA Deemed University, Thanjavur 613401, India
e-mail: 122101008@sastra.ac.in

A. Sivasubramanian et al. (eds.), *Futuristic Communication and Network Technologies*,
Lecture Notes in Electrical Engineering 792,
https://doi.org/10.1007/978-981-16-4625-6_72

Images have a lot of extensive applications ranging from telemedicine, multimedia systems to military communication [2]. The privacy of people's data is put in jeopardy due to the leakage of data while transmitting through wireless and wired media such as Wi-Fi and Ethernet [3].

Hence, it is imperative to formulate a data encryption system that is resilient and provides data integrity, authentication and confidentiality [4]. The obsolete encryption algorithms like DES, SHA, AES, RSA and elliptic curve-based cryptography are not effective for images due to its speed and its inability crack the correlation between the adjacent pixels [5–8]. Another reason why these algorithms and its variations are ineffective is because they have small keyspace and use elementary encryption operations thus, making it susceptible to attacks such as the brute force attack [6]. It is not advisable to employ these techniques in real time because of the high degree of data redundancy. Therefore, it is pivotal to design a cryptosystem that can provide excellent data security, speed and retrieval of decrypted image without loss in quality. In this context, chaos theory has turned out to be one of the most budding research fields for information security for the past few decades [9]. The robust encryption schemes that involve chaos have superseded the above-mentioned traditional algorithms and play an indispensable role in the surveillance of IT communication. Cryptography and chaos theory are closely connected and play a paramount role in the development of contemporary information security [10]. Research scholars are trying to incorporate the properties of the nonlinear chaotic attractors in secure communication. Ergodicity, unstable behavior, no periodicity, high sensitivity to system constraints and initial conditions are a few outstanding features of these chaotic systems that make it suitable for data encryption [9]. One-dimensional chaotic maps yield only single elementary chaotic paths and have average keyspace [11]. As a result, it becomes easy for the intruder to obtain the key necessary for decryption. Hence, we opt for three-dimensional chaotic attractors for securing data as incrementing the dimensions increases the nonlinearity, provides enhanced security and has greater numbers of positive exponents of Lyapunov [12, 13]. The entropy generated by the chaotic attractor produces three sets of pseudorandom sequences that can be utilized in carrying out the scrambling and diffusion process [14, 15]. In this paper, the standard 256×256 Pepper test image is encrypted using the Genesio-Tesi attractor, Lorenz attractor and the Modified Chua attractor [16–18]. The results of the proposed scheme and a detailed analysis of the various statistical tests conducted are provided toward the end of the paper.

2 Methodology

2.1 Realization of the Nonlinear Strange Attractors

The comprehensive analysis and the realization of the nonlinear chaotic attractors used to encrypt the RGB image is shown below.

Lorenz Attractor: The Lorenz nonlinear chaotic attractor is a continuous system that is represented by a family of differential equations which is notable for having chaotic solutions for a certain range of parameter values and system conditions. This chaotic attractor is an example of a strange attractor and is a deterministic system as the future values can be predicted as it changes with time when the exact starting values are known. The Lorenz system of equations is given below

$$\begin{aligned} \frac{\mathrm{d}x}{\mathrm{d}t} &= m_1(y - x) \\ \frac{\mathrm{d}y}{\mathrm{d}t} &= m_2 x - y - xz \\ \frac{\mathrm{d}z}{\mathrm{d}t} &= xy - m_3 z \end{aligned} \tag{1}$$

In this system of equations, m_1, m_2, m_3 are the system constraints and the left-hand side of the family of differential equations represent the state of the system. The terms xy and xz contribute to the nonlinearity of the chaotic system. Normally, the values of m_1, m_2, m_3 are taken to be positive. Here, in this case, we will designate the values of the constraints as $m_1 = 10$, $m_2 = 8/3$, $m_3 = 28$ and the preliminary constraints of the chaos-based system as $(x_0, y_0, z_0) = (0, 1, 0)$. The Lorenz system displays chaotic behavior for the aforementioned values and proximate values as well. The 3D view of the Lorenz attractor is displayed in Fig. 1a.

Genesio-Tesi Attractor: The Genesio-Tesi chaotic attractor is also another continuous system that is represented by a set of nonlinear differential equations shown below

$$\begin{aligned} \frac{\mathrm{d}y}{\mathrm{d}x} &= y \\ \frac{\mathrm{d}y}{\mathrm{d}x} &= z \\ \frac{\mathrm{d}z}{\mathrm{d}t} &= -p_3 x - p_2 y - p_1 z + x^2 \end{aligned} \tag{2}$$

The state variables are represented by x, y, z and p_1, p_2, p_3 are positive real system parameters such that the parameters satisfy $p_1.p_2 < p_3$. The values for the initial conditions and the system constraints are designated as ($x_0 = 0.1$, $y_0 = 0.1$, $z_0 = 0.1$) and $p_1 = 1, p_2 = 3.03, p_3 = 5.55$ so that chaotic system displays the anticipated chaotic behavior. The plot of the Genesio-Tesi attractor is shown in Fig. 1b.

Modified Chua Attractor: The Modified Chua chaotic attractor system is a multi-scroll attractor with system parameters $b_1 = 10.82$, $b_2 = 0.11$, $b_3 = 14.286$, $e = 1.3$, $d = 0$ and initial conditions ($x_0 = 1$, $y_0 = 1$, $z_0 = 0$). The system of equations representing the Modified Chua attractor is shown below

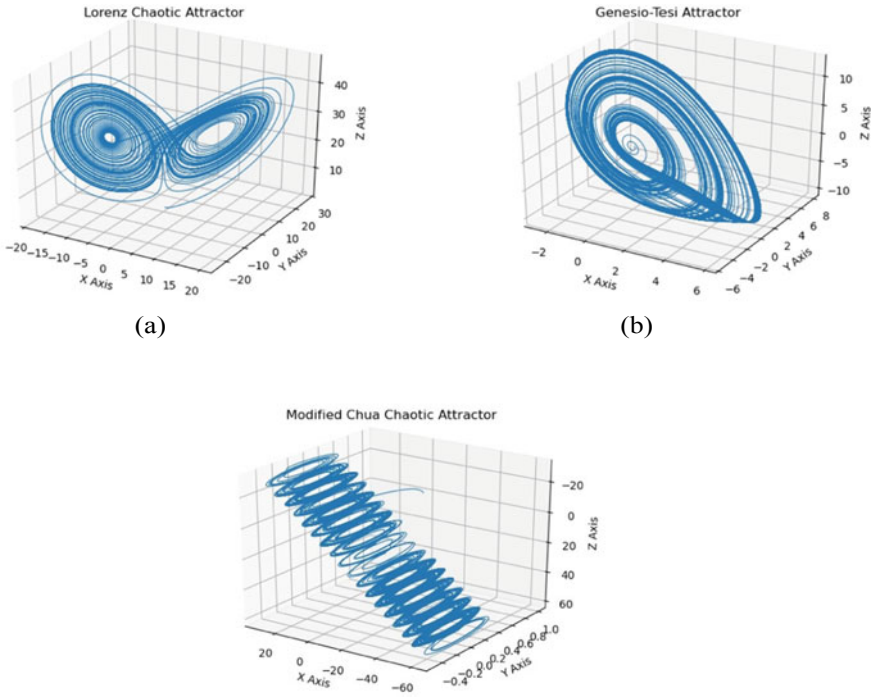

Fig. 1 **a** Lorenz chaotic attractor, **b** Genesio-Tesi chaotic attractor, **c** Modified Chua chaotic attractor

$$\begin{aligned} \frac{\mathrm{d}x}{\mathrm{d}t} &= b_1(y + b_2(\sin(\frac{\pi x}{2e} + d))) \\ \frac{\mathrm{d}y}{\mathrm{d}t} &= x - y + z \\ \frac{\mathrm{d}z}{\mathrm{d}t} &= -b_3 y \end{aligned} \tag{3}$$

The 3D graph of the Modified Chua attractor is shown in Fig. 1c.

2.2 Implementation of the Proposed Encryption Scheme

Discretization of the continuous Lorenz, Genesio-Tesi and Modified Chua system based on Runge–Kutta technique: A broad range of techniques can be harnessed to acquire the numerical results of the system of nonlinear differential equations. Difference equations are obtained after the differential equations undergo discretization. In this case, the function is performed with the aid of Runge–Kutta

4th numerical technique. An approximate value of x is estimated for a known value of t. The limitation of Runge–Kutta technique is that it is applicable only differential equations of the first order. The formula used for the mentioned operation is shown below

$$\begin{aligned} m_1 &= \text{if}(t_n, x_n) \\ m_2 &= \text{if}\left(t_n + \frac{i}{2}, x_n + \frac{m_1}{2}\right) \\ m_3 &= \text{if}\left(t_n + \frac{i}{2}, x_n + \frac{m_2}{2}\right) \\ m_4 &= if(t_n + i, x_n + m_3) \\ x_{n+1} &= x_n + \frac{m_1}{6} + \frac{m_2}{3} + \frac{m_3}{3} + \frac{m_4}{6} \end{aligned} \tag{4}$$

The formula given above is used to determine the next value of x, i.e., x_{n+1} from x_n. The variable i is the increment size and $t_{n+1} = t_n + i$. The increment size is set to a very small value for greater accuracy. We fix the increment value to $i = 0.001$ and the initial conditions and subsequently, the three sets of pseudorandom numbers namely X, Y, Z discrete series of the three attractors are obtained.

Proposed Encryption Scheme: The standard 256×256 Pepper RGB image is taken and processed. The image is transformed into a two-dimensional matrix of 3 different layers, i.e., R, G, B planes. The planes are further converted into one-dimensional arrays. The diffusion process is implemented by performing bit-wise XOR operation between the X, Y, Z pseudorandom sequences and the one dimensional R, G, B plane 8-bit values respectively.

This is followed by a scrambling process where the same random number sequences are used to shuffle the location of the matrix elements. This is used to produce indiscernible 1D array to increase the ambiguity of the enciphered image and the complexity of the encryption key. The encrypted information is transformed back into a 2D matrix, thus producing the encrypted image. This algorithm involves three layers of scrambling and diffusion to boost the security of the data. The entire process of encryption is shown as a block diagram in Fig. 2. The original test image can be obtained by performing the inverse operation of encryption, i.e., decryption. The diffused image, final encrypted image along with the decrypted image are shown in Fig. 3. From Fig. 3c, we can clearly observe that the process of securing the given test image is efficient and successful as the details of the plain test image cannot be retrieved from the enciphered image by an unintended recipient without the key.

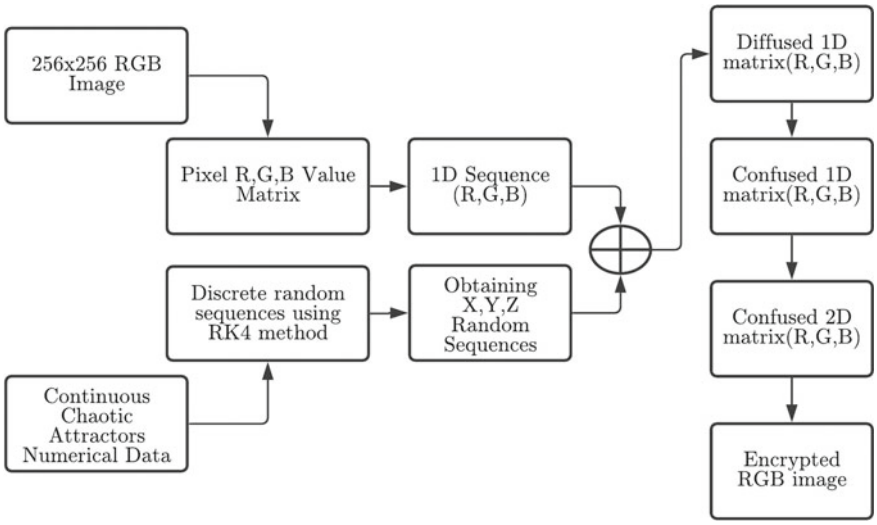

Fig. 2 Proposed encryption scheme

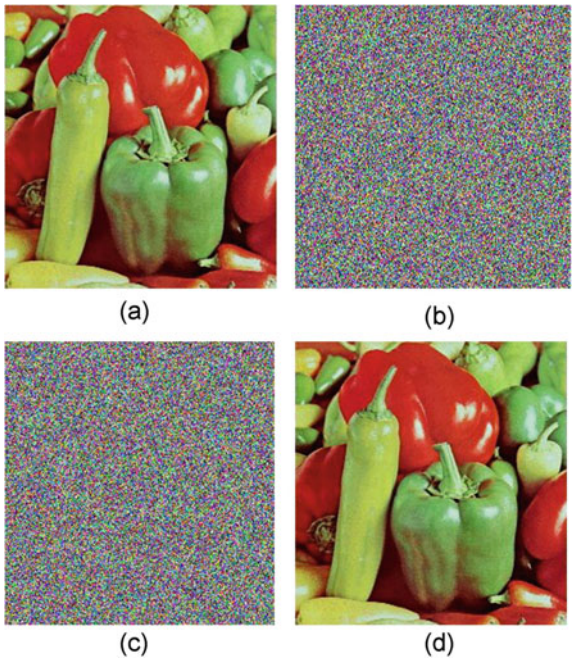

Fig. 3 **a** 256 × 256 Pepper test image, **b** Diffused image, **c** Final encrypted image, **d** Decrypted image

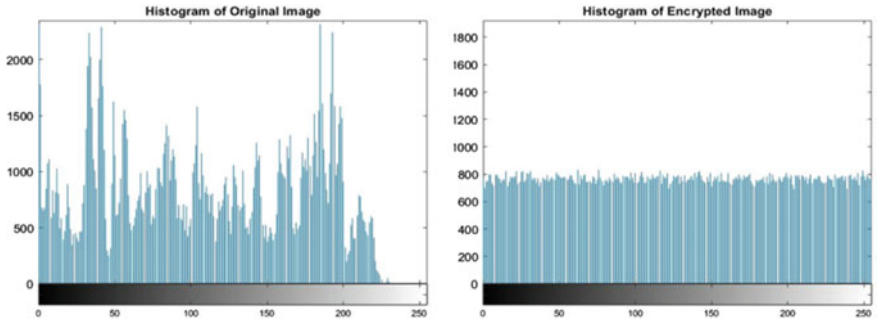

Fig. 4 **a** Histogram plot of test image, **b** Histogram plot of ciphered data

3 Results and Discussion

3.1 Histogram Plot Analysis

The quantity of pixels in an image for different intensity values present in an image is given by the histogram plot. It is indicative of how the tones are distributed in an image. The histogram plot of the original test image along with the encrypted image are displayed in Fig. 4a and b. From the figure, it is observed that the histogram plot of the original data comprises of irregular rise and falls whereas the cipher data has a fairly consistent tonal distribution. The histogram plot of the encrypted data substantiates that the suggested cryptosystem is extremely effective against statistical attacks.

3.2 Entropy Analysis

Entropy analysis is one of the most primary metrics to estimate the degree of randomness in the image and evaluate the effectiveness of the scrambling and diffusion technique. The entropy of the digital image increases with the increase in the distribution of the R, G, B values in the image. The most suitable value of the entropy for an 8-bit encrypted image is 8.000. The entropy values for the enciphered image are clearly shown in Table 1.

Table 1 Comparison between the entropy of the test image and the enciphered image

Image	R	G	B	Total
Original pepper	7.1730	7.2192	7.0244	7.6271
Encrypted pepper	7.9977	7.9975	7.9976	7.9991

Table 2 Analysis of the correlation coefficients of the encrypted image and original image

Image	Horizontal	Vertical	Diagonal
Plain pepper	0.9615	0.9659	0.9435
Enciphered pepper	−0.0000	−0.0019	−0.0019

Table 3 Comparison of the UACI and NPCR values

Image		NPCR	UACI
Pepper	R	99.6735	28.5168
	G	99.6735	28.5168
	B	99.6735	28.5168

3.3 Correlation Coefficient Analysis

The relationship between two proximate pixels in a digital image is given by the coefficient of correlation. It is the measure of resemblance between two pixels.

The value of the coefficient varies from −1 to +1. For a cipher image, the correlation coefficient values should be very low and should be high for plain image. With the aim of testing the correlation of the proximate pixels of the enciphered image, 3000 pixels are randomly selected from the image and their correlation coefficients are estimated. The horizontal, diagonal and vertical coefficients of correlation are listed in Table 2.

3.4 NPCR and UACI Analysis

The NPCR value is indicative of the rate at which the number of pixels changes in the enciphered image, when a certain pixel value of the test image is altered and the UACI value is indicatory of the mean intensity of differences between the test data and the enciphered data. These values are directly proportional to the ability of the system to withstand differential invasions. The NPCR and UACI values for the suggested cryptosystem are listed in Table 3.

3.5 PSNR Analysis

The quantitative mathematical relationship between peak strength of a signal and the strength of noise that degrades the characteristics of the signal rendition is given by the peak signal-to-noise ratio (PSNR) [19, 20]. The PSNR is a direct indicator of the features of the image obtained. It is proportional to the quality of the image [21, 22]. PSNR and MSE is a very beneficial performance evaluation test to assess the quality of reconstruction of encryption codes. The average of errors raised to the second

Table 4 PSNR and MSE values of the image

Image		PSNR	MSE
Pepper	R	9.2636	7.7041e + 03
	G	7.6610	1.1142e + 04
	B	7.5478	1.1437e + 04

Table 5 Comparative study of the statistical tests

Images	NPCR			UACI			Entropy
	R	G	B	R	G	B	
Ref. [3]	99.64	99.64	99.64	33.49	33.56	33.50	7.9992
Ref. [23]	99.45	99.43	99.41	29.58	29.65	29.43	7.7036
Ref. [24]	99.6216	99.6307	99.6017	34.2633	34.0188	34.1718	7.9993
Ref. [25]	99.6357	99.6158	99.6247	33.4570	33.4705	33.4423	7.9991
Our algorithm	99.6735	99.6735	99.6735	28.5168	28.5168	28.5168	7.9991

degree between the plain test image and the image with noise is given by the MSE. The error is denotative of the amount by which the values of the plain test image differ from the depreciated image. The PSNR values obtained using the suggested algorithm is shown below in Table 4.

3.6 Comparative Study of the Encryption Technique

With a plethora of research papers being published on information security throughout the year, it is essential to compare the results of the encryption standard put forth with the already existing novel cryptosystems. The comparative study of various statistical tests conducted for the encryption scheme proposed in this paper and the reference papers are shown clearly in Table 5.

4 Conclusion

In this paper, an innovative and robust approach has been implemented in securing digital images by making use of nonlinear chaotic iterative attractors. The proposed scheme is efficient due to the use of three-dimensional chaotic attractors as they have more keyspace and it becomes very hard for the unintended recipient to obtain the original data from the cipher image. It is corroborated that the scheme proposed masks the original data effectively and the decrypted image obtained has no loss in quality. This efficiency of the cryptosystem is validated by the results of the various

statistical tests conducted. This algorithm can be extended to encrypt other forms of data as well such as audio and video. This cryptosystem has been executed using software without any major obstacles and forms a solid groundwork for hardware implementation. The encryption method validated by this paper can be used in real-time communication and chaos theory has a splendid future in cryptography and information security.

References

1. Abinaya Kumari, Akshaya B, Umamaheswari B, Thenmozhi K, Rengarajan Amirtharajan, Padmapriya Praveenkumar (2018) 3D Lorenz map governs DNA rule in encrypting DICOM images. Biomed Pharmacol J 11(2):897–906
2. AlRababah A (2017) Digital image encryption implementations based on AES algorithm. VAWKUM Trans Comput Sci 13(1):1–9
3. Khan M, Masood F, Alghafis A, Amin M, Naqvi SIB (2019) A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. PLoS ONE 14(12):e0225031
4. Al-Haj A (2015) Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. J Digit Imaging 28(2):179–187
5. Sheela SJ, Suresh KV, Tandur D (2017) A novel audio cryptosystem using chaotic maps and DNA encoding. J Comput Netw Commun 2017
6. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8(4):37
7. Patil P, Narayankar P, Narayan DG, Md Meena S (2016) A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comput Sci 78(1):617–624
8. Na Su, Zhang Y, Mingyue Li (2019) Research on data encryption standard based on aes algorithm in internet of things environment. In: 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC). IEEE, pp 2071–2075
9. Alvarez G, Li S (2003) Cryptographic requirements for chaotic secure communications. arXiv preprint arXiv:nlin/0311039
10. Mainardi F, Pagnini G, Gorenflo R (2007) Some aspects of frac- tional diffusion equations of single and distributed order. Appl Math Comput 187(1):295–305
11. Xiao S, Yu Z, Deng Y (2020) Design and analysis of a novel chaos-based image encryption algorithm via switch control mechanism. Secur Commun Netw 2020
12. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
13. Essaid M, Akharraz I, Saaidi A, Mouhib A (2019) A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system. In: 2019 International conference on wireless technologies, embedded and intelligent systems (WITS). IEEE, pp 1–6
14. Jeong Y-S, Oh K, Cho C-K, Choi H-J (2018) Pseudo random number generation using LSTMs and irrational numbers. In 2018 IEEE international conference on big data and smart computing (BigComp). IEEE, pp 541–544
15. Wang X, Su Y, Luo C, Wang C (2020) A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling. PLoS ONE 15(7):e0236015
16. Sambas A, Vaidyanathan S, Mamat M, Sanjaya WSM, Prastio RP (2016) Design, analysis of the Genesio-Tesi chaotic system and its electronic experimental implementation. Int J Control Theory Appl 9(1):141–149
17. Arpacı B, Kurt E, Çelik K (2020) A new algorithm for the colored image encryption via the modified Chua's circuit. Eng Sci Technol Int J 23(3):595–604

18. Patel S, Muthu RK (2020) Image encryption decryption using chaotic logistic mapping and dna encoding. arXiv preprint arXiv:2003.06616
19. Choudhary R, Arun JB (2014) Secure image transmission and evaluation of image encryption. Int J Innov Sci Eng Technol 1(2):65–69
20. Goyal M, Lather Y, Lather V (2015) Analytical relation comparison of PSNR and SSIM on babbon image and human eye perception using matlab. Int J Adv Res Eng Appl Sci 4(5):108–119
21. Patil VP, Gohatre UB, Sonawane RB (2017) An enhancing PSNR, payload capacity and security of image using bits difference base on most significant bit techniques. Int J Adv Electron Commun Syst
22. Hore A, Ziou D (2010) Image quality metrics: PSNR vs. SSIM. In: 2010 20th international conference on pattern recognition. IEEE, pp 2366–2369
23. Suryanto Y, Ramli K (2017) A new image encryption using color scrambling based on chaotic permutation multiple circular shrinking and expanding. Multimed Tools Appl 76(15):16831–16854
24. Guesmi R, Farah MAB, Kachouri A, Samet M (2016) A novel chaos-based image encryption using DNA sequence operation and secure Hash algorithm SHA-2. Nonlinear Dyn 83(3):1123–1136
25. Niyat AY, Moattar MH, Tor-shiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237