Evolution of Encryption Measures

ISSN 1870-4069

Manuel Alejandro Cardona-López[1], Julieta Mazzetti-Riveros[2],
Laura Del-Rosario-González[2], Karla Denisse Taba-Díaz[2],
Juan Carlos Chimal-Eguía[1]

[1] Instituto Politécnico Nacional,
Centro de Investigación en Computación,
Mexico

[2] Instituto Politécnico Nacional,
Escuela Superior de Ingeniería Mecánica y Eléctrica,
Mexico

{mcardonal2022,chimal}@cic.ipn.mx,
{jmazzettir2200,ldelrosariog1900,ktabad2300}@alumno.ipn.mx

Abstract. The article examines the evolution of encryption measures, focusing on how results have improved over time and emphasizing recent security achievements. It discusses various metrics used to evaluate the performance of encryption algorithms, including Number of Pixel Change Rate, Unified Average Changing Intensity, correlation coefficient, information entropy, Chi-square test, and key space analysis. These metrics are crucial for ensuring the integrity and confidentiality of images, and their improvements over time are commonly aimed. Also, it is analyzed the key advancements in encryption algorithms that have led to improve these encryption metrics, from older to more recent works. The analysis focuses on the critical differences that have contributed to enhanced security. In addition, the article underscores the importance of standardizing security measures in Cryptography to enhance the comparison of robustness between different encryption systems against advanced attacks to various types of data and applications.

Keywords: Correlation, encryption, entropy, image, security

1 Introduction

The massive transfer of data, including digital images, has become a common practice, presenting significant challenges in terms of security and privacy. To address these challenges, image encryption systems have been developed. These systems employ algorithms to convert readable images, which contain clear messages, into encrypted versions. This process involves the use of a specific key to decrypt the image and restore it to its original state, thereby ensuring the confidentiality, integrity, and authenticity of the image during its transmission, reception, and storage [12, 34]. Such systems are critically applied in environments that prioritize information security, such as medical images

pp. 31–42; rec. 2024-09-11; acc. 2024-10-14

with confidential diagnoses, personal identifiers, and sensitive data in military applications [32].

The effectiveness of encryption algorithms heavily relies on their ability to withstand unauthorized decryption attempts, prompting the development of security analyses to assess their robustness and reliability across various usage scenarios [38]. Consequently, this work explores various existing analyses to verify the quality of different encryption proposals. These include evaluation metrics like NPCR (Number of Pixels Changed Rate), UACI (Unified Average Changing Intensity), correlation coefficient analysis, and histogram analysis, among others [29]. Furthermore, it details the quantifiable evolution and improvements of these analyses over recent years, emphasizing advancements in encryption techniques and their adaptation to evolving security threats in digital environments.

The paper is structured as follows. Section 2 introduces the key metrics in the field of image encryption, which are essential for tracking the evolution of reported values. This section provides a detailed explanation to underscore the importance of these metrics in evaluating encryption effectiveness. Section 3 presents the collected data on the evolution of each metric, highlighting improvements over time, with corresponding references and details of the images used for the evaluation. Section 4 outlines the main differences between older and more recent studies that have contributed to these advancements in metrics. Finally, Section 5 concludes the paper.

2 Background of Encryption Metrics

In this section, we provide a brief overview of each metric used for evaluating image encryption security. This includes the purpose of each evaluation, the equations employed, the procedures for their application, and the target values required to indicate a high level of security. The measures included, in order of appearance, are NPCR, UACI, Correlation Coefficient, Information Entropy, Chi-Square Test, and Key Space. The reported values of these measures are then collected for analysing the improvements in encryption security.

2.1 NPCR

The Number of Pixel Change Rate (NPCR) is a metric used to calculate the percentage of differing pixels D between two encrypted images C and C' whose original images differ by exactly one pixel. This metric is crucial for evaluating an encryption algorithm's resistance to differential attacks, which test the algorithm's sensitivity to the smallest changes in the plain image [27]. An NPCR value of 100% is desirable, indicating that the encryption technique is highly resistant to such attacks, as it shows that a minute change in the original image produces a total change in the encrypted image [17]. Conversely, a value of 0% means no change in the resultant encrypted pixels. NPCR is calculated using the following Equation (1), and the difference of two image is shown in Equation (2):

$$\mathrm{NPCR} = \frac{\Sigma_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{1}$$

$$D(i,j) = \begin{cases} 0 \text{ if } C(i,j) = C'(i,j) \\ 1 \text{ if } C(i,j) \neq C'(i,j) \end{cases}. \tag{2}$$

2.2 UACI

The Unified Average Changing Intensity (UACI) measures the average of the absolute intensity differences between two encrypted images corresponding to original images that differ by only a single pixel. This metric is important for evaluating how changes are distributed within the encrypted image in response to slight variations in the original image [20]. A high UACI indicates that the encryption algorithm effectively diffuses changes throughout the encrypted image, which is essential for encryption security [21]. UACI is calculated using the formula in Equation (3), with a desirable value of 33%:

$$\mathrm{UACI} = \frac{1}{M \times N}[\Sigma_{i,j} \frac{\mid C(i,j) - C'(i,j) \mid}{255}] \times 100\%. \tag{3}$$

2.3 Correlation Coefficient

The correlation coefficient (CC) in Equation (4) is a measure used to evaluate the degree of relationship between two variables x, y, in this case, the pixel values [11]. The coefficient indicates their level of similarity. The CC is defined using covariance (Cov) of Equation (5) and variance (Var) of pixel values that is the square of the deviation D in Equation (7), and the expected value E in Equation (6). All these values are for the $N \times N$ total number of pixels in an image. In an original image, the horizontal, diagonal, and vertical values of adjacent pixels are strongly correlated. An effective encryption method reduces this correlation in the encrypted image, bringing the correlation coefficient value closer to zero [28]. This reduction implies that the pixels in the encrypted image are less predictable and, therefore, more secure against statistical attacks. In contrast, a CC of 1 implies perfect correlation, meaning the pixels are linearly identical, indicating a failed encryption process. The correlation coefficient is calculated using equation, which evaluates the quality of the cryptographic system:

$$\mathrm{CC}_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4}$$

$$\mathrm{Cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{5}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2. \tag{7}$$

2.4 Information Entropy

Entropy H is a measure of the expected value or average amount of information that can be extracted from a message, in this case, an image [33]. It represents the quantity of information present and indicates the degree of uncertainty or randomness in the data. Introduced by Claude Shannon in 1949, entropy values range from 0 to 8 and should be close to 8 for an 8-bit image representation. A high entropy value of 8.0 indicates a uniform distribution of pixel values, which is desirable for an encrypted image because it reflects a high level of unpredictability and randomness [47]. This uniform distribution means each pixel has an equal probability of appearing, ensuring maximum entropy. Conversely, if the entropy of the encrypted image is significantly less than 8, it suggests the image has patterns or predictability, posing a security risk. Entropy can be calculated using Equation (8) and is based on the probabilities $p(x_i)$ of the occurrence of each pixel value x_i in an image with N pixels:

$$H(x) = -\sum_{i=0}^{N-1} P(x_i)\log_2 P(x_i). \tag{8}$$

2.5 Chi-square Test

The Chi-square χ^2 test is used to evaluate the uniformity of histograms, with the aim of determining the resistance to statistical attacks [7]. A lower Chi-square value indicates better uniformity, where the ideal value is equal to zero, suggesting the strongest resistance [48]. To confirm the uniform distribution of the resulting ciphered images more precisely, the Chi-square test is conducted, demonstrating that the encrypted image follows a uniform distribution. It is based on the expected frequency E_i of a uniform histogram and the observed o_i from the image, following the procedure of Equation (9):

$$\chi^2 = \sum_{i=1}^{255} \frac{(o_i - E_i)^2}{E_i}. \tag{9}$$

2.6 Key Space Analysis

Key Analysis (KA) is crucial in any encryption algorithm, as the algorithm's security heavily relies on the strength of the secret keys. Assessing the effectiveness of an encryption system involves analyzing the key space, where the key is a unique value used for encrypting data, ensuring only authorized parties can decrypt the information. Desirable properties of strong secret keys include a large key space. The key space depends on the size of the secret key;

Table 1. Numer of pixel change rate (NPCR).

Proposal	Publication year	Reported value	Image size	Image name
Ref. [25]	2012	99.5850	256×256	Lena
Ref. [30]	2015	99.5789	200×200	Peppers
Ref. [50]	2018	99.5697	256×256	Cameraman
Ref. [42]	2020	99.6100	512×512	Lena
Ref. [49]	2023	99.6399	256×256	Baboon
Ref. [16]	2024	99.6500	256×256	Medicine

a larger size makes it more challenging for an attacker to guess the key. An excellent image encryption algorithm requires a robust key space, indicating resistance against brute-force attacks. With a large key space, exhaustive key searches become impractical, requiring an infeasible number of operations (e.g., 2^{128} for a 128-bit key). In other words, a larger key size significantly reduces the likelihood of a brute-force attack succeeding, given the vast number of potential combinations that must be tested to find the correct key.

3 Encryption Metrics Evolution

This section presents the evolution of encryption results across eight tables. The tables compile data from various works over the years, including the measures introduced in the previous section, along with the image name and size. Over time, these measures have progressively approached optimal values, illustrating how each new cryptosystem generally enhances security outcomes. The data in each table is organized chronologically, from the oldest to the most recent publications.

3.1 NPCR

In this context, the NPCR (Number of Pixel Change Rate) aims to achieve a 100% difference in the encrypted pixels between two encrypted images that differ by only one pixel in their plain representation. Recent advancements have brought this value closer to the ideal 100%. This improvement is illustrated in Table 1.

3.2 UACI

For this metric, it is important that not only the pixels are different, but also differ so far from in its intensity levels. A value closer to 33% is the optimal, where in the recent years has been kept.

Table 2. Unified average changing intensity (UACI).

Proposal	Publication year	Reported value	Image size	Image name
Ref. [30]	2012	32.9495	200×200	Baboon
Ref. [37]	2015	33.3430	256×256	Lena
Ref. [50]	2018	33.3618	256×256	Cameraman
Ref. [41]	2020	33.4700	512×512	Cameraman
Ref. [49]	2023	33.4199	256×256	Lena
Ref. [22]	2023	33.6500	256×256	Barbara

Table 3. Correlation Coefficient (Horizontal Direction).

Proposal	Publication year	Reported value	Image size	Image name
Ref. [3]	2007	0.0308	256×256	Lena
Ref. [45]	2010	0.0036	256×256	Lena
Ref. [25]	2011	0.0068	256×256	Lena
Ref. [13]	2015	0.0273	512×512	Boat
Ref. [44]	2016	−0.0060	1024×1024	Male
Ref. [18]	2017	−0.0163	256×256	Colour Flower
Ref. [46]	2018	0.0004	256×256	Clock
Ref. [50]	2018	−0.0017	256×256	Cameraman
Ref. [1]	2024	0.0008	256×256	Lena

3.3 Correlation Coefficient

The ideal correlation coefficient is 0.0, regardless of the direction in which the correlation is measured. The values should be around this ideal, indicating no correlation. Over time, approaches have increasingly approximated this ideal. Improvements in correlation can be seen in Tables 3, 4, and 5.

3.4 Information Entropy

For pixels with 256 intensity values, the optimal entropy value is 8.0. Recently, image cryptosystems have been getting closer to this value, as shown in Table 6.

3.5 Chi-square Test

The goal of the Chi-square test is to achieve a value of 0, indicating no difference between the histogram of the encrypted image and a uniform distribution. The differences have decreased over the years, as detailed in Table 7.

Table 4. Correlation Coefficient (Vertical Direction).

Proposal	Publication year	Reported value	Image size	Image name
Ref. [3]	2007	0.0304	256×256	Lena
Ref. [45]	2010	0.0023	256×256	Lena
Ref. [25]	2011	0.0091	256×256	Lena
Ref. [13]	2015	−0.0321	512×512	Boat
Ref. [44]	2016	−0.0103	1024×1024	Male
Ref. [18]	2017	0.0185	256×256	Colour Flower
Ref. [46]	2018	−0.0054	256×256	Clock
Ref. [50]	2018	−0.0279	256×256	Cameraman
Ref. [1]	2024	−0.0003	256×256	Lena

Table 5. Correlation Coefficient (Diagonal Direction).

Proposal	Publication year	Reported value	Image size	Image name
Ref. [3]	2007	0.0317	256×256	Lena
Ref. [45]	2010	0.0039	256×256	Lena
Ref. [25]	2011	0.0063	256×256	Lena
Ref. [13]	2015	-0.0060	512×512	Boat
Ref. [44]	2016	0.0031	1024×1024	Male
Ref. [18]	2017	-0.0129	256×256	Colour Flower
Ref. [46]	2018	0.0111	256×256	Clock
Ref. [50]	2018	0.0047	256×256	Cameraman
Ref. [1]	2024	0.0002	256×256	Lena

Table 6. Information Entropy.

Proposal	Publication year	Reported value	Image size	Image name
Ref. [39]	2009	7.9970	256×256	Lena
Ref. [6]	2012	7.9890	256×256	Lena
Ref. [24]	2013	7.9881	256×256	Pepper
Ref. [26]	2015	7.9637	256×256	Cameraman
Ref. [2]	2016	7.9979	256×256	Baboon
Ref. [10]	2019	7.9992	256×256	Lena
Ref. [17]	2021	7.9994	512×512	Lena
Ref. [43]	2023	7.9998	1024×1024	Barbara
Ref. [36]	2024	7.9998	1024×1024	Male

Table 7. Chi-square test.

Proposal	Publication year	Reported value	Image size	Image name
Ref. [8]	2009	290	256×256	Lena
Ref. [9]	2013	260	128×128	Lake
Ref. [19]	2014	243	256×256	Lena
Ref. [15]	2016	251.2	256×256	Lena
Ref. [17]	2021	233.729	512×512	Lena
Ref. [43]	2023	207.445	256×256	Mountain

3.6 Key Space Analysis

The key space should be as large as possible to prevent feasible brute force attacks. The size of the key space has increased over time, enhancing security by expanding the number of possible combinations that must be tested to decrypt the image. This trend is illustrated in Table 8.

Table 8. Key Space.

Proposal	Publication year	Reported value
Ref. [35]	2005	2^{128}
Ref. [31]	2006	2^{150}
Ref. [5]	2010	2^{256}
Ref. [23]	2015	2^{299}
Ref. [40]	2018	2^{312}
Ref. [14]	2021	2^{604}
Ref. [4]	2023	2^{1658}

4 Improvements in Algorithms

The following list summarizes the advancements in encryption algorithms that have led to improved encryption metrics. These insights are drawn from the collection of papers reporting on encryption metrics. A comparative analysis of older and more recent works highlights the key differences that have contributed to enhanced security. While the fundamental concepts and features discussed have persisted over the years, their application has evolved to provide stronger security measures.

1. Chaotic systems: Although encryption procedures based on chaotic systems have been in use since the early 2000s, their properties have significantly

improved. Modern chaotic systems now feature a broader range of chaotic parameters, leading to enhanced chaotic characteristics.

2. XOR operations: XOR operations have long been a fundamental technique in encryption. While they remain crucial, they are now complemented by additional methods such as SHA functions and substitution operations, applied before or after the XOR process to create a more chaotic bit distribution.
3. DNA application: DNA sequences have been combined with chaotic maps in encryption. Recent advancements have parallelized DNA coding, reducing execution time and allowing for more encryption rounds, thereby enhancing security.
4. Permutations: Previously, only one permutation was typically applied per round, often generated from chaotic maps. Now, permutations are applied in diverse ways and derived from various sources, such as random walks within the same encryption round, which effectively reduces correlation.
5. Encryption metrics: Measuring current results is the first step toward improvement. Over time, more encryption metrics have been introduced to evaluate the chaotic distribution of encrypted data, acknowledging that while each metric is necessary, none alone is sufficient.
6. Key space: The key space has expanded significantly. Earlier encryption schemes operated with smaller key sizes due to limited computational resources. However, increasing key sizes now allows for the inclusion of additional information within the keys, contributing to better securityoutcomes.
7. Symmetric cryptography: Symmetric cryptography, a staple in both older and newer proposals, remains favored due to its efficient execution time, even that new proposals have more encryption rounds, making it more suitable than asymmetric cryptography in many contexts.
8. Histogram: Permutations are essential for breaking the relationship between pixels without altering pixel values, thus maintaining the histogram. Over time, chaos has been increasingly applied to modify pixel values to achieve a uniform histogram, not just positions. Chaos has enhanced the substitution process too.

5 Conclusion

The imperative to enhance security levels in image encryption drives this article to review the results of various encryption approaches. Currently, past proposals may appear insecure due to their results, highlighting the ongoing need for improved security outcomes. On the other hand, while older and current encryption algorithms share fundamental concepts and features, their application has evolved over the years to deliver stronger security measures. In addition, to make image cryptography more consistent and promising, it is crucial to establish robust security frameworks with consistent evaluation metrics. We reviewed the most common security metrics, displaying standardized measures that can be universally adopted. This standardization is essential for enabling reliable comparisons of different algorithms and their effectiveness over time. Such adaptability ensures that the benefits of the framework extend to specific application scenarios, guiding future research and development efforts toward improving evaluation metrics in image cryptography.

Acknowledgments. The authors would like to thank the Instituto Politécnico Nacional of México (Secretaría Académica, Comisión de Operación y Fomento de Actividades Acadé-micas COFAA, SIP, ESIME ZAC, and CIC), and the CONAHCyT for their support in the development of this work.

References

1. Abed, Q.K., Al-Jawher, W.A.M.: Optimized color image encryption using arnold transform, uruk chaotic map and gwo algorithm. Journal Port Science Research 7(3), 219–236 (2024)
2. Ahmad, J., Hwang, S.O.: A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications 75, 13951–13976 (2016)
3. Ahmed, H.E.d.H., Kalash, H.M., Allah, O.S.F.: An efficient chaos-based feedback stream cipher (ecbfsc) for image encryption and decryption. Informatica 31(1), 121–129 (2007)
4. Alexan, W., Alexan, N., Gabr, M.: Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs. Fractal and Fractional 7(4), 287 (2023)
5. Amin, M., Faragallah, O.S., Abd El-Latif, A.A.: A chaotic block cipher algorithm for image cryptosystems. Communications in Nonlinear Science and Numerical Simulation 15(11), 3484–3497 (2010)
6. Bahrami, S., Naderi, M.: Image encryption using a lightweight stream encryption algorithm. Advances in Multimedia 2012(1), 767364 (2012)
7. Budiman, F., Andono, P.N., Setiadi, M., et al.: Image encryption using double layer chaos with dynamic iteration and rotation pattern. International Journal of Intelligent Engineering & Systems 15(2) (2022)
8. Etemadi Borujeni, S., Eshghi, M.: Chaotic image encryption design using tompkins-paige algorithm. Mathematical problems in engineering 2009(1), 762652 (2009)
9. Etemadi Borujeni, S., Eshghi, M.: Chaotic image encryption system using phase-magnitude transformation and pixel substitution. Telecommunication Systems 52, 525–537 (2013)
10. Ge, R., Yang, G., Wu, J., Chen, Y., Coatrieux, G., Luo, L.: A novel chaos-based symmetric image encryption using bit-pair level process. IEEE Access 7, 99470–99480 (2019)
11. Guleria, V., Kumar, Y., Mishra, D.C.: Multiple colour image encryption using multiple parameter frdct, 3d arnold transform and rsa. Multimedia Tools and Applications 83(16), 48563–48584 (2024)
12. Haddad, S., Coatrieux, G., Moreau-Gaudry, A., Cozic, M.: Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains. IEEE Transactions on Information Forensics and Security 15, 2556–2569 (2020)

13. Hua, Z., Zhou, Y., Pun, C.M., Chen, C.P.: 2d sine logistic modulation map for image encryption. Information Sciences 297, 80–94 (2015)
14. Iqbal, N., Naqvi, R.A., Atif, M., Khan, M.A., Hanif, M., Abbas, S., Hussain, D.: On the image encryption algorithm based on the chaotic system, dna encoding, and castle. IEEE Access 9, 118253–118270 (2021)
15. Jallouli, O., El Assad, S., Chetto, M.: Robust chaos-based stream-cipher for secure public communication channels. In: Procedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST). pp. 23–26. IEEE, Barcelone, Spain (2016)
16. Jiang, D., Tsafack, N., Boulila, W., Ahmad, J., Barba-Franco, J.: Asb-cs: Adaptive sparse basis compressive sensing model and its application to medical image encryption. Expert Systems with Applications 236, 15 (2024)
17. Khairullah, M.K., Alkahtani, A.A., Bin Baharuddin, M.Z., Al-Jubari, A.M.: Designing 1d chaotic maps for fast chaotic image encryption. Electronics 10(17), 2116 (2021)
18. Khan, J.S., Ahmad, J.: Chaos based efficient selective image encryption. Multidimensional Systems and Signal Processing 30, 943–961 (2019)
19. Khanzadi, H., Eshghi, M., Borujeni, S.E.: Image encryption using random bit sequence based on chaotic maps. Arabian Journal for Science and engineering 39, 1039–1047 (2014)
20. Kumar, A., Dua, M.: Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. Multimedia tools and applications 80(18), 27785–27805 (2021)
21. Kumar, A., Dua, M.: A gru and chaos-based novel image encryption approach for transport images. Multimedia Tools and Applications 82(12), 18381–18408 (2023)
22. Kumar, S., Sharma, D.: A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. Artificial Intelligence Review 57(4), 87 (2024)
23. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. International journal of Bifurcation and Chaos 15(10), 3119–3151 (2005)
24. Liu, H., Wang, X., Kadir, A.: Color image encryption using choquet fuzzy integral and hyper chaotic system. Optik-International Journal for Light and Electron Optics 124(18), 3527–3533 (2013)
25. Loukhaoukha, K., Chouinard, J.Y., Berdai, A.: A secure image encryption algorithm based on rubik' s cube principle. Journal of Electrical and Computer Engineering 2012(1), 13 (2012)
26. Luo, Y., Du, M., Liu, J.: A symmetrical image encryption scheme in wavelet and time domain. Communications in Nonlinear Science and Numerical Simulation 20(2), 447–460 (2015)
27. Ma, Y.: Research and application of big data encryption technology based on quantum lightweight image encryption. Results in Physics 54, 107057 (2023)
28. Mali, K., Chakraborty, S., Roy, M.: A study on statistical analysis and security evaluation parameters in image encryption. entropy 34, 36 (2015)
29. Mohammad, O.F., Rahim, M.S.M., Zeebaree, S.R.M., Ahmed, F.: A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research 12(23), 13265–13280 (2017)
30. Pareek, N.K.: Design and analysis of a novel digital image encryption scheme. International Journal of Network Security & Its Applications 4(2), 13–15 (2012)
31. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image and vision computing 24(9), 926–934 (2006)

32. Patel, K.D., Belani, S.: Image encryption using different techniques: A review. International Journal of Emerging Technology and Advanced Engineering 1(1), 30–34 (2011)
33. Shen, H., Shan, X., Xu, M., Tian, Z.: A new chaotic image encryption algorithm based on transversals in a latin square. Entropy 24(11), 1574 (2022)
34. Singh, K.N., Singh, A.K.: Towards integrating image encryption with compression: A survey. ACM Transactions on Multimedia Computing, Communications, and Applications 18(3), 1–21 (2022)
35. Socek, D., Li, S., Magliveras, S.S., Furht, B.: Short paper: Enhanced 1-d chaotic key-based algorithm for image encryption. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). pp. 406–407. Athens, Greece (2005)
36. Song, W., Fu, C., Zheng, Y., Zhang, Y., Chen, J., Wang, P.: Batch image encryption using cross image permutation and diffusion. Journal of Information Security and Applications 80, 103686 (2024)
37. Stoyanov, B., Kordov, K.: Image encryption using chebyshev map and rotation equation. Entropy 17(4), 2117–2139 (2015)
38. Tiken, C., Samlı, R.: A comprehensive review about image encryption methods. Harran Üniversitesi Mühendislik Dergisi 7(1), 27–49 (2022)
39. Tong, X., Cui, M., Wang, Z.: A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator. Optics Communications 282(14), 2722–2728 (2009)
40. Ur Rehman, A., Liao, X., Ashraf, R., Ullah, S., Wang, H.: A color image encryption technique using exclusive-or with dna complementary rules based on chaos theory and sha-2. Optik 159, 348–367 (2018)
41. Xu, C., Sun, J., Wang, C.: An image encryption algorithm based on random walk and hyperchaotic systems. International Journal of Bifurcation and Chaos 30(04), 2129–2151 (2020)
42. Xue, X., Zhou, D., Zhou, C.: New insights into the existing image encryption algorithms based on dna coding. Plos one 15(10), 31 (2020)
43. Ye, G.D., Wu, H.S., Huang, X.L., Tan, S.Y.: Asymmetric image encryption algorithm based on a new three-dimensional improved logistic chaotic map. Chinese Physics B 32(3), 030504 (2023)
44. Ye, G., Zhao, H., Chai, H.: Chaotic image encryption algorithm using wave-line permutation and block diffusion. Nonlinear Dynamics 83, 2067–2077 (2016)
45. Zhang, Q., Guo, L., Wei, X.: Image encryption using dna addition combining with chaotic maps. Mathematical and Computer Modelling 52(11-12), 2028–2035 (2010)
46. Zhang, Y.: The unified image encryption algorithm based on chaos and cubic s-box. Information Sciences 450, 361–377 (2018)
47. Zhao, J., Wang, S., Zhang, L.: Block image encryption algorithm based on novel chaos and dna encoding. Information 14(3), 150 (2023)
48. Zhu, H., Dai, L., Liu, Y., Wu, L.: A three-dimensional bit-level image encryption algorithm with rubik's cube method. Mathematics and Computers in Simulation 185, 754–770 (2021)
49. Zhu, S., Deng, X., Zhang, W., Zhu, C.: Image encryption scheme based on newly designed chaotic map and parallel dna coding. Mathematics 11(1), 231 (2023)
50. Zhu, S., Zhu, C., Wang, W.: A new image encryption algorithm based on chaos and secure hash sha-256. Entropy 20(9), 716 (2018)