Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

Research on Image Encryption Algorithms Based on Matrix Scrambling and Matrix Product Transformations

Shu Qin[1)], Chunming Xu[2)]*
[1,2)] School of Mathematics and Statistics, Yancheng Teachers University, China
[1)] 2050103508@qq.com, [2)] ycxcm@126.com
*Corresponding author

ABSTRACT

This study introduces an innovative image encryption algorithm that leverages multiple rounds of matrix scrambling and matrix product transformation. Each round of encryption integrates cross-scrambling operations within the image matrix and invertible matrix product transformations, thereby effectively disrupting pixel positions and values. By iteratively adjusting pixel positions and transforming pixel values, the algorithm significantly enhances the security and robustness of the encryption process. The experimental results demonstrate that the proposed algorithm exhibits excellent resistance to statistical analysis, differential attacks, and other potential threats, thereby ensuring high security and practical applicability.

Keywords: Image encryption, matrix scrambling, matrix product transformation, chaotic systems, network security

INTRODUCTION

In the wake of the rapid advancement of information technology, digital images have proliferated across military, commercial, medical, and personal domains. However, their susceptibility to replication and widespread dissemination exposes them to a range of security vulnerabilities, such as unauthorized access, tampering, and data leakage. To safeguard the privacy and security of digital images, image encryption technology has emerged as a crucial solution (Liang et al., 2022; Malik et al., 2020; Wang et al., 2021). This technology employs specific algorithms to process image data, rendering it unintelligible without proper authorization and thereby effectively protecting the security of image information. Its significance extends beyond military, commercial, and medical applications to everyday information security (Wang et al., 2023; Xiong et al., 2023).

At present, the predominant image encryption methods encompass symmetric encryption algorithms (e.g., DES, AES) (Muhajer, 2020), chaotic encryption algorithms (Tao et al., 2022), the Arnold transform (Qu et al., 2022), and matrix transformation-based encryption methods (Aqel et al., 2018), among others. Symmetric encryption algorithms are widely adopted for their rapid encryption speed and robust security. However, their relatively short key lengths render them susceptible to brute-force attacks. Chaotic encryption algorithms capitalize on the inherent randomness of chaotic systems and their sensitivity to initial conditions to generate pseudo-random sequences as encryption keys, thereby offering enhanced security and a broader key space. The Arnold transform, a classical image scrambling technique, disrupts pixel positions to eliminate correlations between adjacent pixels and achieve encryption. Matrix-based encryption methods, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) (Liu et al., 2020), apply specific matrix operations to the image

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

for encryption. While these methods provide a certain degree of security, their effectiveness is increasingly challenged by advancements in decryption technologies. Thus, the development of more secure and efficient image encryption algorithms is of utmost importance.

This study proposes an innovative image encryption algorithm that integrates multiple rounds of scrambling and matrix transformations to enhance the security and efficiency of image encryption. The algorithm executes multiple rounds of encryption, combining internal cross-scrambling of the image matrix with invertible matrix product transformations to disrupt both pixel positions and values. By innovatively integrating these techniques, the proposed method significantly strengthens encryption and increases the complexity and attack resistance of the encrypted image data.

METHOD

Chaotic Systems

Chaotic systems, known for their extreme sensitivity to initial conditions, exhibit inherently random and unpredictable behaviors, making them highly suitable for generating encryption keys in image encryption applications. This study leverages chaotic sequences to introduce significant randomness and unpredictability into the encryption process, thereby enhancing security. Specifically, the Lorenz chaotic system, a classic example has been employed to generate these sequences (Singh et al., 2024). The system's sensitivity ensures that minor alterations in initial conditions lead to substantial variations in the generated keys. The governing equations of the Lorenz system are as follows:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = x(b - z) - y \\ \frac{dz}{dt} = xy - cz \end{cases} \quad (1)$$

Here, x, y, and z denote the state variables, whereas a, b, and c represent the control parameters. Through numerical integration, chaotic sequences are derived for integration into the encryption algorithm.

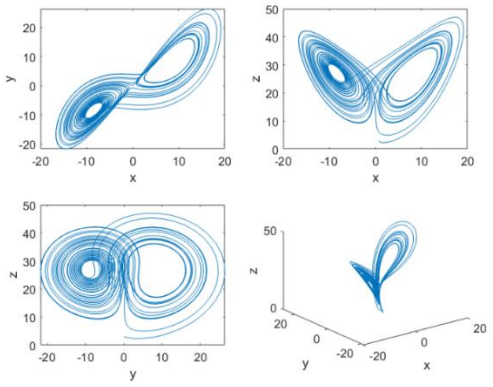


Figure 1: Phase Diagram of the Lorenz Chaotic System

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

As shown in Figure 1, the phase diagram of the Lorenz system illustrates its complex trajectory evolution and irregular motion paths, which are hallmarks of chaotic behavior. These characteristics render the Lorenz system an optimal choice for generating chaotic sequences in encryption algorithms, thereby fortifying the security of the encryption process.

Reversible Transformation Matrices

In the realm of image encryption, reversible transformation matrices are indispensable. They enable the effective alteration of pixel values via matrix multiplication, thereby achieving encryption. The reversibility of the encryption process is ensured by these matrices, allowing the encrypted image to be precisely restored to its original state through a corresponding decryption process. This study employs the modular M reversible transformation matrix, initially proposed by Dong (2007), to modify pixel values through matrix transformation. Constructed on the foundation of combinatorial theory, the modular M reversible integer matrix can be defined. Given a non-negative integer $x \geq 0$, an n-order reversible matrix $A(x)$ and its inverse $B(x)$ are formulated as:

$$a_{ij}(x) = C_{i-1}^{x+j-1} \qquad (2)$$

$$b_{ij}(x) = (-1)^{i+j} C_{x+l-1}^{l} C_{j+l-1}^{i-1} \qquad (3)$$

where C_x^l denotes the binomial coefficient. It can be shown that:

$$A(x)B(x) = I(mod\ M) \qquad (4)$$

Leveraging modular M reversible integer matrices enables effective pixel value encryption during the image encryption process. By altering pixel values through matrix multiplication, this method complicates the recovery of the original image using simple statistical features. During decryption, the inverse matrix $B(x)$ can accurately restore the original pixel values of the image. This approach not only enhances encryption security but also guarantees the reversibility of the encryption process, ensuring reliable image transmission and restoration in secure communications.

Design of Image Encryption Algorithm

The proposed image encryption algorithm integrates multiple rounds of scrambling and matrix transformations to enhance security through iterative processes. It combines pixel position scrambling with pixel value transformation, leveraging the efficiency of matrix operations and the inherent randomness of chaotic systems. The algorithm's steps are outlined as follows:

(1) Initialization

Load the target color image, extract its dimensions M (height) and N (width), and compute the total number of pixels $L = M \times N$.

(2) Component Stretching

Flatten the R,G and B components of the image into row vectors of length L, and then concatenate these vectors into a $3 \times L$ matrix I. This matrix structure facilitates subsequent matrix transformations by mapping each pixel value to a matrix element.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

(3) Multiple rounds of scrambling and matrix transformation

Utilize the ode45 function to solve the Lorenz chaotic system with initial conditions:

$$\begin{cases} x_0 = \dfrac{x_0 \sum_{ij} PR_{ij}}{255M*N} - 0.01 \\ y_0 = \dfrac{x_0 \sum_{ij} PG_{ij}}{255M*N} + 0.03 \\ z_0 = \dfrac{x_0 \sum_{ij} PB_{ij}}{255M*N} - 0.05 \end{cases} \quad (5)$$

After discarding the first 2000 values, generate three sequences S_1,S_2, and S_3 of length L with values ranging from 1 to 256:

$$\begin{cases} S_1 = |x_s| * 10^{15} \ mod \ 256 \\ S_2 = |y_s| * 10^{15} \ mod \ 256 \\ S_3 = |z_s| * 10^{15} \ mod \ 256 \end{cases} \quad (6)$$

Additionally, derive the scrambling sequence T and the encryption round number K as follows:

$$T = |x_s| * 10^{13} \ mod \ L \ + 1 \quad (7)$$

$$K = mean(x) * 10^{13} \ mod \ 50 \ + 100 \quad (8)$$

(4) Multiple rounds of scrambling and matrix transformation

$For\ i = 1{:}K$, perform the following operations:

(4.1) Random Swap Operation: Randomly swap the segments of matrix I based on sequence T:

$$I = \left[I(:, T(i) + 1{:}L), I\left(:, 1{:}T(i)\right)\right] \quad (9)$$

(4.2) Invertible matrix product transformation: Construct an invertible transformation matrix $A(x)$ (with $x = 1$ in this study) and multiply it with matrix I to alter pixel values:

$$I = A(x) * I \quad (10)$$

The use of an invertible matrix ensures the reversibility of the encryption process while enhancing the randomness of the encrypted image.

(5) XOR operation

Apply XOR operations on each row of matrix I using sequencesS_1,S_2, and S_3:

$$\begin{cases} I(1,:) = I(1,:) \oplus S_1 \\ I(2,:) = I(2,:) \oplus S_2 \\ I(3,:) = I(3,:) \oplus S_3 \end{cases} \quad (11)$$

(6) Image Reconstruction

Reassemble matrix I into a color image of dimensions $M \times \mathrm{N} \times 3$. The encrypted image retains the original format but with scrambled content.

Given that the decryption process is essentially the inverse of the encryption algorithm, with steps mirroring the encryption process in a highly symmetric manner, it is omitted here to avoid redundancy.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

RESULTS

Image Encryption Results

We employed a "pepper" image as the test subject to evaluate the encryption and decryption processes. As depicted in Figure 2, a comparative analysis was conducted among the original, encrypted, and decrypted images. The encrypted image exhibited a complete loss of the original image's features, characterized by high randomness and noise levels. This outcome confirms that the encryption algorithm effectively altered the pixel arrangement and values, thereby enhancing security. The decrypted image's perfect alignment with the original further validates the decryption algorithm's accuracy and the method's reliability.

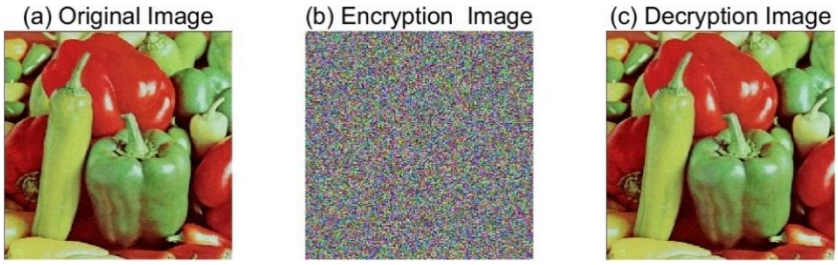


Figure 2: Original Image, Encrypted Image, and Decrypted Image

Key Space Analysis

The key space of the proposed algorithm is determined by several critical factors, including the parameters of the chaotic system, the initial values of the chaotic sequence, the parameters of the reversible transformation matrix, and the number of iterations K. Consequently, the key space is significantly larger than2^6, providing robust resistance against brute-force attacks.

Histogram Analysis

Histogram analysis serves as a pivotal metric for assessing the performance of image encryption algorithms. Ideally, an encrypted image should exhibit a histogram that approximates a uniform distribution, indicating random pixel value distribution and thwarting attackers' attempts to extract useful information through statistical analysis.

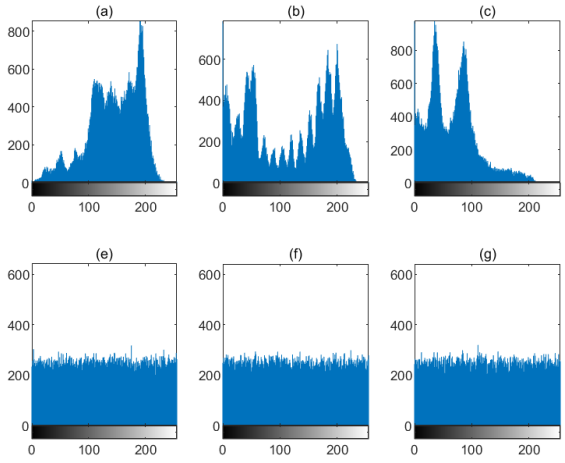


Figure 3: Histogram Analysis

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

As shown in Figure 3, the histograms of the R, G, and B components of both the original and encrypted images reveal a significant deviation between them. The encrypted image's histogram demonstrates effective erasure of statistical characteristics, making it impossible for attackers to infer any useful information about the original image. This uniform distribution not only enhances image security but also visually distinguishes the encrypted image from the original, thereby strengthening the encryption effect.

Adjacent Pixel Correlation Analysis

Correlation analysis is a fundamental method for evaluating encryption algorithm security in image encryption technology (Wang et al., 2021). By examining the correlation between original and encrypted images, one can assess the degree of confusion introduced by the encryption algorithm. In this study, we analyzed the correlation in horizontal, vertical, and diagonal directions, with results presented in Figures 4 and 5 and Table 1.

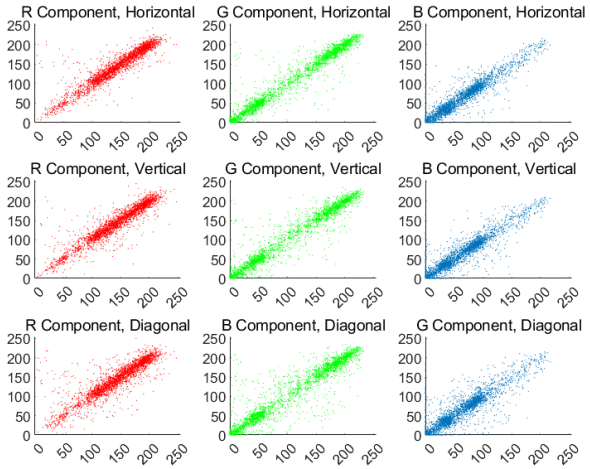


Figure 4: The Correlation Between Pixels in the Original Image

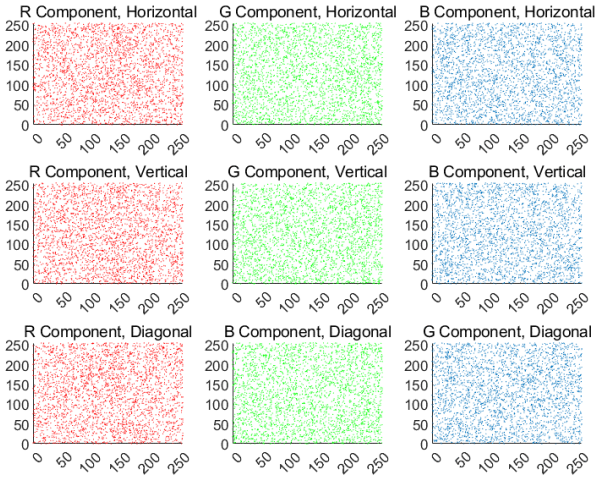


Figure 5: The Correlation Between Pixels in the Encrypted Image

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

Table 1: Correlation Coefficients Before and After Image Encryption

Direction	Horizontal	Vertical	Diagonal
Original Image	0.9262	0.962	0.9209
Encrypted Image	-0.03	-0.0352	0.0214

The original image exhibited high correlation coefficients, such as 0.9262 in the horizontal direction, 0.9286 in the vertical direction, and 0.9297 along the diagonal. These values indicate strong regularity and predictability in the original image's pixel arrangement, making it susceptible to attacks. In contrast, the encrypted image's correlation coefficients significantly decreased to -0.0300 horizontally, -0.0352 vertically, and 0.0214 diagonally. These near-zero coefficients demonstrate that the encryption algorithm effectively disrupted the correlation between adjacent pixels, rendering the image information random and unpredictable. This reduction in correlation enhances the image's security by making it difficult for attackers to interpret the encrypted content.

In summary, the correlation analysis clearly illustrates that the encryption algorithm significantly reduces image correlation, thereby enhancing security.

Information Entropy Analysis

Information entropy is a crucial indicator of encryption randomness and effectiveness in image encryption (Hosny et al., 2022). Higher entropy values signify greater image randomness, lower information leakage risk, and superior encryption quality. For an 8-bit image, the ideal entropy value is close to 8.

Table 2: Information Entropy Analysis

Information Entropy	Red	Green	Blue
Original Image	7.3920	7.6150	7.1738
Encrypted Image	7.9971	7.9971	7.9967

As shown in Table 2, the entropy values of the original image's R, G, and B components were 7.3920, 7.6150, and 7.1738, respectively. In contrast, the encrypted image's entropy values were 7.9971, 7.9971, and 7.9967, nearly reaching the ideal value of 8. These results demonstrate that the encryption algorithm effectively randomized the pixel values, increasing statistical uncertainty and resistance to attacks.

Sensitivity Analysis

Sensitivity analysis is a vital method for evaluating an image encryption algorithm's response to minor changes in the original image (Malik et al., 2020). An ideal encryption algorithm should produce significant changes in the encrypted image when the original image undergoes minor modifications, indicating high security and attack resistance. In this study, we performed sensitivity analysis by modifying a single pixel in the original image and encrypting the altered version. The results were

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

evaluated using NPCR (Number of Pixels Change Rate) and NUCI (Unified Average Changing Intensity), as shown in Table 3.

Table 3: Sensitivity Analysis

Evaluation Method	Red	Green	Blue
NPCR	0.9956	0.9964	0.9962
NUCI	0.3352	0.3349	0.3348

As indicated in Table 3, the NPCR values for the R, G, and B components were 0.9956, 0.9964, and 0.9962, respectively. These values suggest that over 99.5% of the encrypted image's pixels changed when a single pixel in the original image was modified. This high sensitivity to minimal changes effectively prevents attackers from gaining useful information by comparing modified and unmodified encrypted images. Additionally, the NUCI values of 0.3352, 0.3349, and 0.3348 indicate that the average intensity of pixel changes was approximately 0.33 across all components. This uniform distribution of changes further enhances the encrypted image's randomness and unpredictability.

In conclusion, the encryption algorithm's high NPCR and NUCI values in sensitivity analysis highlight its excellent performance in enhancing image randomness and unpredictability, thereby strengthening its resistance to attacks.

Discussions

The image encryption algorithm proposed in this study has made remarkable progress in terms of security. By combining multiple rounds of permutation with matrix transformation, it can not only randomize pixel positions effectively but also adjust pixel values through reversible matrix multiplication, thereby increasing the complexity and security of the encryption process. Compared with traditional methods, this approach not only speeds up the encryption but also significantly enhances resistance to various attacks. The use of chaotic sequences adds dynamism and randomness to key generation, further improving security. Moreover, the introduction of matrix transformations increases the randomness of the encryption process, enabling the algorithm to better resist common threats such as statistical analysis and differential attacks. These advantages make the algorithm highly practical and reliable for real - world applications.

Conclusions

This research has successfully developed an innovative image encryption algorithm that significantly boosts the security and efficiency of image encryption through multiple rounds of permutation and matrix transformation. Experimental results show that the algorithm performs excellently in image encryption, with fast speed and strong attack resistance. Dynamic key generation and additional randomness further strengthen its security. Future research will focus on optimizing the algorithm and exploring its potential applications in more fields to meet the growing demand for image information security.

ACKNOWLEDGEMENTS

This work is supported by the Jiangsu Provincial Undergraduate Innovation and Entrepreneurship Training Program (Project No.: 202310324094Y).

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 7, Number 2, April 2025
https://doi.org/10.47709/cnahpc.v7i2.5643

Submitted : Mar 02, 2025
Accepted : Apr 02, 2025
Published : Apr 04, 2025

REFERENCES

Liang, Z., Qin, Q., & Zhou, C. (2022). An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. Neural Computing and Applications, 34, 19313-19341.

Malik, M. G. A., Bashir, Z., Iqbal, N., & Imtiaz, M. A. (2020). Color image encryption algorithm based on hyper-chaos and DNA computing. IEEE Access, 8, 88093-88107.

Wang, X., & Su, Y. (2021). Image encryption based on compressed sensing and DNA encoding. Signal Processing Image Communication, 12, 116246.

Wang, X. Y., Wang, X. L., Teng, L., Jiang, D. H., & Xian, Y. (2023). Lossless embedding: A visually meaningful image encryption algorithm based on hyperchaos and compressive sensing. Chinese Physics B, 32(2), 020503.

Xiong, G. Q., Cai, Z. C., & Zhao, S. F. (2023). A bit-plane encryption algorithm for RGB image based on modulo negabinary code and chaotic system. Digital Signal Processing, 141(9), 104153.

Muhajer, S. (2020). A review of DES and AES algorithms for image encryption. Al-Qadisiyah Journal of Pure Science, 27(1), 48-56.

Tao, Y., Cui, W. H., Ming, Z. J., Zhao, Z., & Shi, T. W. (2022). An image encryption algorithm based on Hopfield neural network and Lorenz hyperchaotic system. IAENG International Journal of Computer Science, 49(1), 3131-3136.

Qu, G., Meng, X., & Yin, Y. (2021). Optical color image encryption based on Hadamard single-pixel imaging and Arnold transform. Optics and Lasers in Engineering, 137(20), 106392.

Aqel, M. J., ALQadi, Z., & Abdullah, A. A. (2018). RGB color image encryption-decryption using image segmentation and matrix multiplication. International Journal of Engineering and Technology, 7(3), 104-107.

Liu, Z., Yang, M. L., & Yan, W. Q. (2020). A framework for image encryption on frequency domain. In Research Anthology on Artificial Intelligence Applications in Security (pp. 151-168). IGI Global.

Singh, P. K., Jha, B., & Kumar, S. (2024). An efficient and lightweight image encryption technique using Lorenz chaotic system. Mathematical Modeling and Computing, 11(3), 702–709.

Dong, Y. S. (2007). Proof of a method for finding the inverse of integer matrices. Journal of Changchun Normal University, 4(2), 4-5.

Wang, J., Zhi, X., Chai, X., & Lu, Y. (2021). Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion. Multimedia Tools and Applications, 80(01), 16087-122.

Hosny, K. M., Kamal, S. T., & Darwish, M. M. (2022). Novel encryption for color images using fractional-order hyperchaotic system. Journal of Ambient Intelligence and Humanized Computing, 13(2), 973-988.

Malik, M. G. A., Bashir, Z., Iqbal, N., & Imtiaz, M. A. (2020). Color image encryption algorithm based on hyper-chaos and DNA computing. IEEE Access, 8, 88093-88107.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.