International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1223-1229
Journal homepage: http://iieta.org/journals/ijsse

Pixels Substitution-Permutation Employing ISING Model and Gyrator Transformation for Securing Image

Ali Shakir Mahmood

Computer Science Department, College of Education, Mustansiriyah University, Baghdad 10052, Iraq

Corresponding Author Email: asmjhm2006@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.140419

Received: 8 May 2024
Revised: 2 August 2024
Accepted: 16 August 2024
Available online: 30 August 2024

Keywords:
ISING model, gyrator transformation, image encryption, confusion, diffusion

ABSTRACT

In recent duration, exponential internet growth usage has necessitated robust methods for securing data during transmission. Image encryption has emerged as a crucial technique to prevent unauthorized access and manipulation of digital content. This study introduces a novel encryption method that enhances image security through a two-stage process. The first stage involves substituting and shuffling plain image pixels using a set of random numbers generated by the ISING model, where these numbers are described as a sequence of movements. In the second stage, pixel values are permuted using the Gyrator transformation, resulting in a ciphered image. Extensive numerical simulations have been conducted to calculate the effectiveness of the suggested method. The results confirm the method's efficacy, demonstrating significant improvements in security and robustness compared to existing encryption techniques. Statistical analyses further prove the advantages of using the confusion and diffusion properties for improving the proposed method. The proposed method represents a substantial improvement in the field of image encryption, presenting a secure and reliable solution for protecting digital images.

1. INTRODUCTION

People around the world in the current time are affected by the huge revolution in communication and using wired and wireless networks to exchange their digital data, which is increasing the transfer of multimedia data through the Internet, especially images. At the same time, some people have developed their programming capabilities to hack the transferred data and therefore need to develop new methods to secure the transferred data over the Internet [1].

If we want to overcome these limitations, several methods were suggested to keep the data secure from outsiders by using encryption. Furthermore, the main objective of encoding is to give a service to those organizations for maintaining the secrecy of important data [2].

The four main objectives of using cryptography are ensuring confidentiality, maintaining data integrity, verifying identity, and preventing ingratitude [3]. Numerous of the latest methods try to demonstrate the security of images by applying a generator to random numbers to produce an encryption key. As the generated key was random, the computational complexity of the designed method can be performed better and more efficiently [4].

The main challenge in any encryption algorithm is an encryption key. In contrast, the key was a random reflection of unbreakable encryption text. In the case of an image environment, we need a method to deal with pixel value and position when changing both to overcome an encrypted image. Many methods were introduced to produce a random encryption key; one of them is the ISING model, which is employed in this study as a random number generator to create an encryption key.

The present work tries to use an ISING model as a random key generator for use as encryption keys. Essentially, generates a set of movements used to change pixel positions for substitution. Permutation is also present in the current work for changing pixel values where the gyrator transformation is used. Also, several test methods were used to measure the designed encryption methods, and scientific discussion was presented for each test.

The structure of the present paper is represented as follows: In the next section, we introduce the literature review of the previous work. The detailed description of the ISING model and gyrator transformation are described in sections three and four, respectively. The detailed description of the design encryption method is reviewed in the fifth Section. In the sixth Section, the discussion and performance analysis of the proposed method, as well as comparing the obtained results comparisons with previous works, are performed.

2. LITERATURE REVIEW

Several encryption systems, in their design, need to generate a series of numbers called encryption keys, used in both encryption and decryption. These encryption keys must obey specific rules to be used as encryption keys; these rules can be summarized in terms of randomness, renderability, and effect with minor changes in the initial state.

Many random generators introduced in research papers use

a chaotic system in their design. They used Chebyshev's polynomial for image encryption, used in pixel permutation in an image encryption algorithm for two stages. This method is thought to provide greater security compared to a single-stage image encryption algorithm; it is resistant to plain-chosen assaults and can be statistically measured [1].

A color image encryption method that uses two random phase encodings in the gyrator transform domain is introduced. In this method, the color image is first decomposed into its three primary colors (RGB). Each color is then encrypted separately with a random phase mask. The encrypted colors are subsequently transmitted through a structured phase mask before undergoing gyrator transformation to produce the final cipher image [5].

As well as the need to permute the pixel value mathematically. The gyrator operation is a linear canonical integral transformation that produces distorted versions of the rotation, spatial frequency planes, and phase space [6, 7].

Another researcher used a tensor map to encrypt an image; wherever it is suggested, the improvement grouping confusion and diffusion. Furthermore, the modification yields an excellent encryption result. against differential attacks and the Logistic Map was used in image encryption with the substitution approach [8].

Table 1. Summary of previous work

Ref.	Methodology Key	Features	Measurements and Results
[1]	The random phase encoding mask for the gyrator transforms is converted into a structured phase mask using the devil's vortex Fresnel lens in the frequency plane.	The double phase is intermediately connected with the frequency domain and phase mask by the gyrator transform; this process is repeated two times to give the corresponding cipher images. A masked structure addresses the issue of axis alignment in an optical setup.	•Mean squared error •Sensitivity to encryption keys
[2]	Tent Map is used to permute the pixels for producing an encrypted image.	A tent map is a one-dimensional random array used as a discrete dynamical system to optimize key space confusion. improvement in encryption results	•Key space analysis •Key sensitivity •Histogram analysis •Correlation analysis •Information entropy Differential attack
[3]	The double random and structure phases are used for encoding images.	Gyrators modify the amplitude and encode Fresnel zone plate masks. Each of these component images is then independently encrypted using a random phase mask applied to the image plane and transmitted through the initial structured phase mask.	•Key space
[4]	This work introduces the use of double image encryption, where these images are transformed by a gyrator into an imaginary part of a complex number, and then converted to a binary number for a complex function.	Double images are encoded using the gyrator transform, where the secret images are treated as a complex signal's real and imaginary components. The security is further enhanced by modifying the chaotic map parameters of the imaginary part.	•Normalized mean square error •Histogram analysis •Correlation analysis •Information entropy
[5]	Chebyshev's chaotic map as a random number generator.	They used Chebyshev's polynomial for image encryption, used in pixel permutation in a two-stage image encryption algorithm.	•Histogram analysis •Correlation analysis •NPCR and UACI •Differential attack
[6]	Ising model as a random number generator with fife dimension array with heat balance for scaling relation.	Exploring the ISING model for complementary estimation of exponential heat reduction in finite-dimensional random field numerical simulations by modified hyper-scale relations	•Random test •Heat detection •Linear regression
[7]	Employ the ISING model to estimate the patient's prostate MR images, combined with the Wolff algorithm.	The combination of the ISING model and the Wolff algorithm to estimate the number of patients with prostate cancer in a certain population. The early detection of prostate cancer increases the probability of life	•Exams set •Sensitivity •Specificity •Accuracy
[8]	Pixel exchange of phase encoding of the gyrator transform of a double image for pixel phase exchanging.	Double-image phase encryption by pixel exchanging and gyrator domains. The amplitude of pixels in two images controlling storage of key	•Uniform distribution •Random pattern
[9]	Proposed the use of gyrator transform domains with a chaotic map. An iterative structure was used to increase randomness and produce a cipher image.	The gyrator transform's phase encoding is utilized to alter image pixel values for diffusion, while a two-dimensional chaotic map generates random numbers to shift pixel positions for confusion. This combination enhances the security of the encryption algorithm.	•Key space analysis •Histogram analysis •correlation analysis •Information entropy •Differential attack

Additionally, one of the signal generators, called the ISING model [9], uses a set of signals to produce the random numbers used as an encryption key. These signals, or random numbers, can be composed as a set of movements to substitute the position of the pixels [10].

Double image encryption is achieved in two stages: (I) image encryption using random pixel switching as a confusing scheme, and (ii) arbitrary phase of gyrator domains. During the initial step of the encryption process, double plain images are identified as the absolute and fictional components of the complicated function. The complex function is then encrypted in the second stage by the two logical operations [11].

In image encryption, encryption keys are crucial and must adhere to specific rules such as randomness and the ability to regenerate for secure encryption and decryption processes. Research explores various methods using chaotic systems like Chebyshev's polynomial and Tent Map for pixel permutation, enhancing security against chosen attacks, and statistical measures. The ISING model generates random numbers crucial for encryption, utilizing them to substitute pixel positions. Gyrator transformers play a significant role in distorting pixel values mathematically, enhancing encryption robustness. Techniques like duplicating arbitrary phases of the gyrator transform domain to improve security by encrypting images independently. As stated in Table 1, the reviewed research compares these methodologies in terms of effectiveness, advantages, and limitations, aiming to advance image encryption systems.

3. ISING MODEL KEY GENERATOR

The ISING model can be categorized as the simplest statistical mechanics system, has highly non-trivial behavior, and looks random. The applied values to replace and obtain a prominent level of complexity, as well as the ability to return to the original image, lead to the use of the ISING model as a random number generator to be used in image security. The two-dimensional ISING can be represented as Eq. (1):

$$H = -J \sum_{i,j}^{N} \sigma_i^z \sigma_j^z \tag{1}$$

where, J is the interaction strength and σ is a twist at the site $i, j\ \sigma = \pm 1$, the sum runs over all nearest-neighbor spin sites.

The 2D ISING model consists of an array with a size of (N×N) two variables that are horizontally and vertically connected with equal capabilities. There can be an external field applied to the variables that bias them towards a certain argument. Figure 1 shows the results of the 2D ISING.

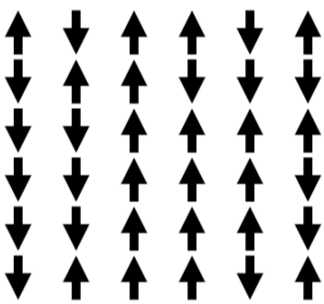

Figure 1. 2D ISING representation

When applying the 2D ISING array to a plain image, that will change the pixel position and move it to another location during the image.

4. GYRATOR TRANSFORMATION

Lately, several transformation methods have been used for image ciphering using a random phase mask. filtering in the spatial field has been proposed [3, 10]. The main benefits of these transformations are correct image decryption.

The application of gyrator transformation has recently expanded to encode 2D image-based rotation in the twisting (position and spatial frequency) phase planes, which is achieved by rotating twice at the input and output levels. Interference is used during the transformation phase to record digital stereoscopic images of the input image, as well as to produce keys for decoding. In other words, encoding parameters have a role in fractional domains. On the gyrator domains, expansion is achievable due to a resemblance between fractional gyrator transformation approaches.

The encoding procedure for the image pixels can be represented as described in Eq. (2):

$$F = exp(i\emptyset_{1..N}) R^{\propto 1..N}[f] \tag{2}$$

where, N is an operation number, $\propto 1..N$ transformation angle, $exp(i\emptyset_{1..N})$ random phase mask.

The decryption procedure corresponds to that written as illustrated in Eq. (3):

$$f = \exp(-i\emptyset_{1..N}) R^{-\propto 1..N}[F] \tag{3}$$

The decoding process is the reverse of the encoding process, as illustrated in Figure 2. It contains an image before encoding, an encoded image, and finally an image after decoding (the original image).

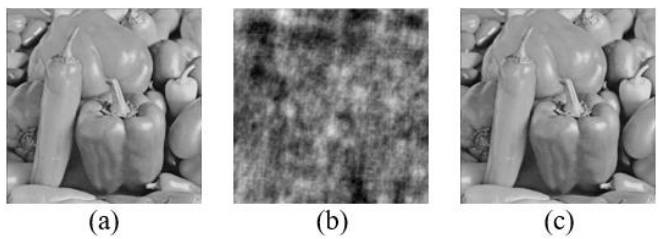

Figure 2. Implement gyrator transformation on an image, (a) Plain image, (b) Encoded image, (c) Restored image

5. PROPOSED ENCRYPTION METHOD

The design of an image encryption system needs to satisfy two basic primary concepts, known as substitution and permutation [11]. The plain image segments into arrays of fixed size depending on the size of the gyrator transform filter to apply the ISING model and gyrator transform. Firstly, the substitution denotes the alternation of plain image pixels according to movements generated by the ISING model. After that, permutation denotes influencing the order of pixels according to a gyrator transform. Consequently, the development of an encryption system includes both previous principles.

5.1 First phase: Substitution

Based on the previous discussion on the ISING model and its capability to generate a series of movements, this concept aids in diffusing the pixel locations in the plain image, altering their locations, which consequently decreases the robust correlation between neighboring pixels and reduces the correlation coefficient value between pixels. A key advantage of the ISING model is its ability to generate movement in two directions: up and down. This breaks the continuous sequence of plain image pixels. To better understand the proposed diffusion procedure, a practical example is required. By initializing the ISING model with N=4 and $\sigma = 100^{\circ}$, the output of the ISING model is illustrated in Figure 3(a). The plain image will be divided into blocks that are equal in size to the ISING model. As demonstrated in Figure 3(b), each block can be swapped over with its corresponding block in the next row to produce a new image with diffused blocks. The first row of blocks is related to the last row of blocks in a chain-like manner, as depicted in Figure 3(c).

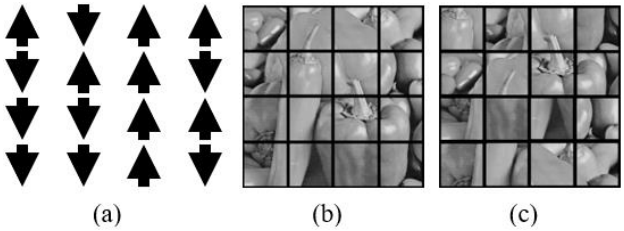

Figure 3. Describe how ISING movements work, (a) Basic ISING movements, (b) Plain Image blocks, (c) Produced image after applying ISING movements on plain image blocks

5.2 Second phase: Permutation

The previous explanation on permutation indicates the necessity to build a technique for modifying the value of pixels. The designed method changed the pixel value in the spatial domain by using gyrator transformation, where the diffused image will be confused in this phase. That will generate a completely altered image since the pixel values resolve to be disobediently changed. After applying the gyrator transformation to get the cipher image, and now this image is ready to be sent to the recipient with the seed value of the ISING model and gyrator transformation. The recipient in his role will use these parameters to initiate the system for preparing to decrypt the encrypted image as well as recover the plain image.

Figure 4 depicts the flowchart of the developed image encryption system. To create a cipher image, two suggested phases that correspond to the principles of replacement and permutation are employed. And Figure 4 describes the encryption procedure in detail, while the decryption method is a reverse operation of the encryption method. Where the initial values are sent from sender to recipient to generate the same sequence of movements by using the ISING model and, at the same time, initiate the gyrator transformation. Firstly, the cipher image is exposed to the inverse of the Gyrator transformation to produce a substitution image. Secondly, subjecting the substitution image to the reverse shuffling movements generated by the ISING model will lead to reconstructing the plain image.

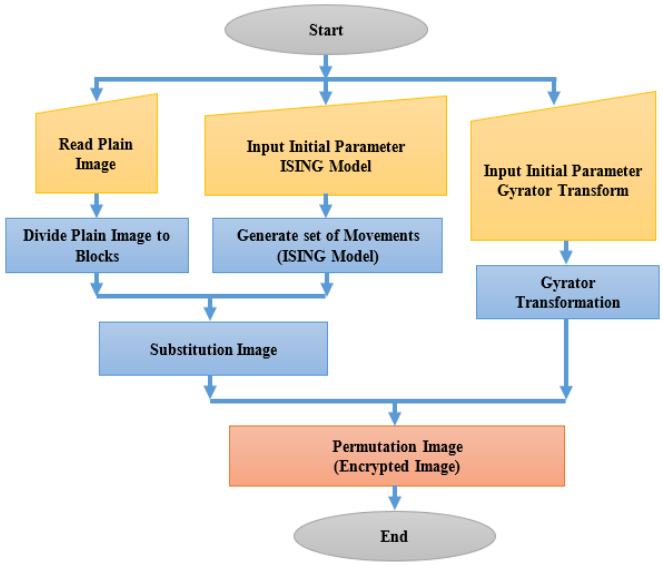

Figure 4. Proposed method

6. RESULTS AND DISCUSSION

The evaluation of the suggested encryption algorithm was presented in the current section to determine its efficiency. The evaluation employed standard images taken from the USC-SIPI image dataset as well as the standard initial parameter.

6.1 Security analysis

The effectiveness of the security component is fundamental to the success of any encryption algorithm. The encryption algorithm must be highly robust against any form of brute, differential, or statistical attack with a strong key length. These elements affect the security and reliability of encryption algorithms in modern computing environments.

6.1.1 Differential attack analysis

According to the encryption principles, the superior encryption system should be sufficient against the suspected plain image. Therefore, NPCR and UACI tests were accomplished on the encrypted images to calculate the changed pixels, with average density between the normal and the encrypted image [12]. Each initial value will produce a diverse set of encryption movements. As the image changes, the original values of the map change. Different values are used each time to encrypt different images. The mathematical representation for NPCR and UACI is shown in the below Eqs. (4)-(6):

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \quad (4)$$

$$\text{NPCR} = \frac{\sum_{i=1}^{w} \sum_{j=1}^{h} D(i,j)}{w \times h} \times 100\% \quad (5)$$

$$UACI = \frac{\sum_{i=1}^{w} \sum_{j=1}^{h} |C_1(i,j) - C_2(i,j)|}{255 \times w \times h} \times 100\% \quad (6)$$

where, C_1 and C_2 represent the encrypted images with the identical height and width as cipher images, then compute the values of NPCR and UACI are stated in Table 2.

Table 2. Computed NPCR and UACI and their comparisons

Image	Proposed Method		Other Works		Ref.
	NPCR %	UACI %	NPCR%	UACI%	
Lena	99.810	33.163	99.600	33.390	[13]
Baboon	99.824	33.197	99.604	33.180	[14]
Elaine	99.684	33.598	99.620	33.440	[14]

As well as indicating that the algorithm provides good diffusion and a complex relationship between the input image and encryption key. The previous table concludes that the proposed method has achieved impressive results that exceed those of other algorithms.

6.1.2 Key space analysis

Encryption uses a distinct key set, with the size of the key space directly correlated with security. To be effective, an algorithm must have a key space that exceeds a particular threshold probably 2^{100} to withstand attacks [15, 16]. Where the ISING model and gyrator transformation can generate an encryption key with a huge space of approximately 10^{157}, that means the proposed method is robust against several types of differential attacks.

6.1.3 Key sensitivity analysis

A minor alteration in constraints leads to the generation of a completely different encryption key, as presented in Figure 5.

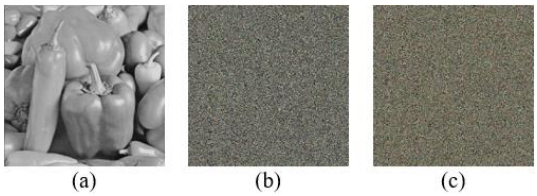

Figure 5. Key sensitivity, (a) Plain image, (b) Cipher image by key-1, (c) Cipher image by key-2

The images in the figure above were encrypted using the original encryption key with some alterations. Along with the values of the correlation coefficient between the plain and cipher images, the suggested method is extremely sensitive to even tiny changes in encryption key values, maintaining the original image's privacy and confidentiality. As a result, the suggested encryption scheme is highly sensitive to variations in encryption keys [17].

6.2 Statistical analysis

This type of analysis is performed on both conventional and encrypted images to acquire further information about the security of the proposed encryption technology as well as to demonstrate its integrity.

6.2.1 Histogram analysis

The histogram acts as a fundamental character in indicating the occurrence distribution of pixel intensity values, as shown in Eq. (7).

$$X^2 = \sum_{i=1}^{256} \frac{\left(N_i - \frac{(w \times h)}{256}\right)^2}{\frac{(w \times h)}{256}} \quad (7)$$

where, N_i is the frequency number of pixels; width and height represent w and h frequently of an image, respectively; and the histogram is produced and displayed for both plain and cipher images [18]. As illustrated in Figure 6, the pixel value pattern in the cipher image must be sufficiently comparable and distinct from the plain image.

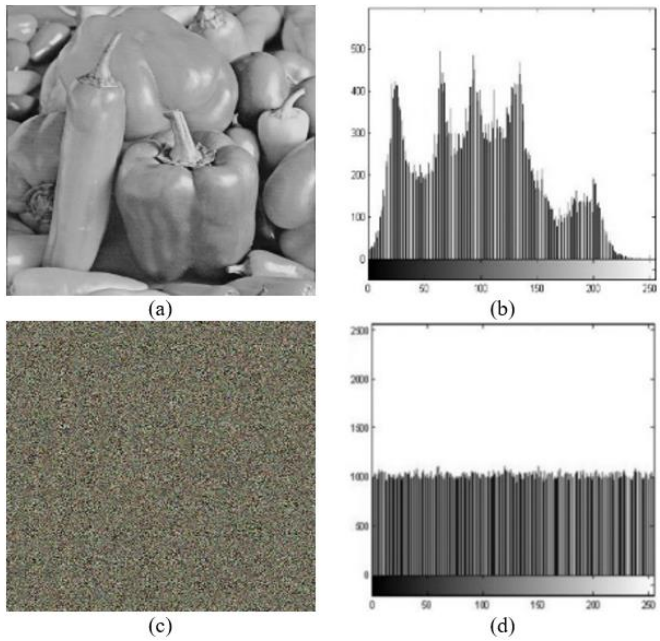

Figure 6. Histogram distribution, (a) Plain image, (b) Histogram for plain image, (c) Cipher image, (d) Histogram for cipher image

Also, the histogram of the ciphered images is scattered homogeneously as pixel values are changed by applying gyrator transformation to the scrambled image, which indicates effective diffusion and robust encryption against statistical attacks.

6.2.2 Adjacent pixels correlation analysis

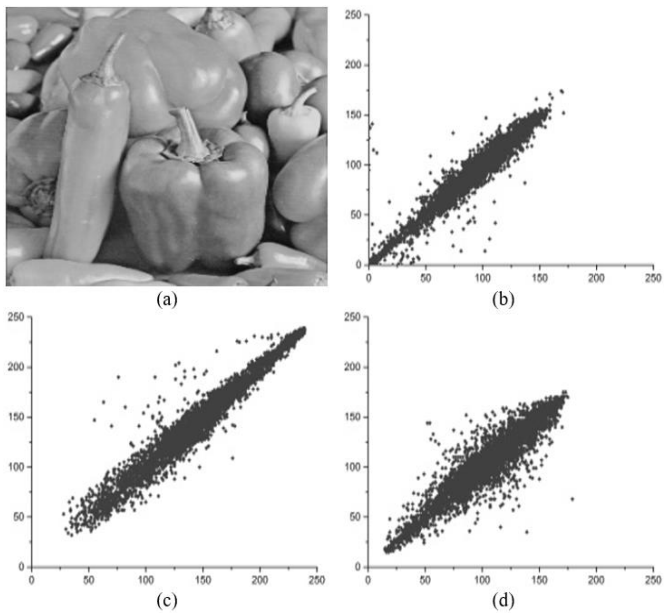

Figure 7. Correlation distribution of plain image, (a) Plain image, (b) Horizontal distribution, (c) Vertical distribution (d) Diagonal distribution

The neighboring pixels have a strong correlation because the color or intensity values of adjacent pixels are often similar which influences the proposed encryption system's performance. Each pixel in the image has a strong relation with adjacent pixels in vertical, horizontal, and diagonal directions, as shown in Figure 7 [19].

The encryption method reduces the strong relationships among neighboring pixels. The graphical results in Figure 8 demonstrate that there is no correlation between neighboring pixels in the encrypted image, with very weak correlations in the horizontal, vertical, and diagonal directions.

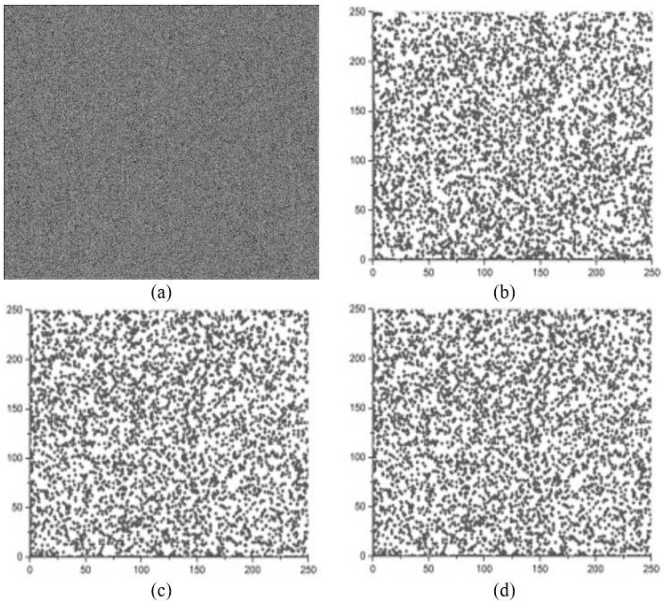

Figure 8. Correlation distribution of cipher image, (a) Cipher image, (b) Horizontal distribution, (c) Vertical distribution, (d) Diagonal distribution

The three directions of correlation coefficients are lower than those in other approaches. Thus, this approach succeeded in deleting relationships between neighboring pixels in the plain image, resulting in no association between surrounding pixels in the cipher image.

6.2.3 Information entropy

This analysis is used to measure the strength of the encryption system. Encryption key sequences are being verified as being important in image encryption issues, as presented in Eq. (8). In summary, if neighboring pixels are identical, entropy should be low, not high. A high entropy value indicates a rich variety of pixel values, whereas identical neighboring pixels point to low entropy.

$$H(s) = \sum_{i=0}^{2^{m-1}} \left(P(s_i) log_2 \frac{1}{P(s_i)} \right) \quad (8)$$

The entropy should be close to 8 [20, 21]. This means that the pixel values in the encrypted image are uniformly distributed across the 256 possible intensity levels, maximizing randomness and minimizing predictability. This is a crucial aspect of image encryption, as it ensures that the encrypted image does not reveal any patterns that could be exploited to reverse-engineer the original image, as shown in Table 3.

Table 3. Entropy value and comparisons

Image	Proposed Method	Other Works	
	Entropy	Entropy	Ref.
Lena	7.9993	7.9991	[22]
Pepper	7.5997	7.5936	[23]
Elaine	7.9837	7.9984	[14]

This implies that the image entropy value of all established images is ideal due to the change in cipher image gray levels.

6.2.4 Peak signal-to-noise ratio analysis

A tool is used as a standard quantitative measure to estimate the image quality compared to the original image, as shown in Eq. (9).

$$PSNR = 10 \log_{10} \left(\frac{I_{max}^2}{\sqrt{\frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(A(i,j) - B(i,j) \right)^2}} \right) \quad (9)$$

As illustrated in Table 4, a set of images shows that the degree of convergence between the two images is extremely low. This suggests that there are significant numerical variations between the plain and encryption images.

Table 4. Computed PSNR and comparisons

Image	Proposed Method	Other Works	
	PSNR	PSNR	Ref.
Lena	7.555	5.803	[24]
Pepper	8.961	5.833	[24]
Elaine	9.294	8.058	[25]

7. CONCLUSION

This paper demonstrates the novel method of using an ISING model and a gyrator transformation to ensure the security of a plain image by applying substitution and permutation, respectively. The initial parameters are set to the ISING model to generate a scrambling set of movements that scrambles the pixel values of the plain image. The image is then subjected to a gyrator transformation to produce a cipher image. Mathematical investigations (statistical and security analyses) were carried out, and the high results obtained from the applied tests led to high security and immunity against different types of attacks. The comparison with other works proves that the proposed method is better than other methods. show that the proposed system achieves high encryption reliability, has an extensive key space, is robust to the private key, and avoids various kinds of attacks.

ACKNOWLEDGMENT

The author would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

REFERENCES

[1] Singh, H., Yadav, A.K., Vashisth, S., Singh, K. (2015).

Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. Optics and Lasers in Engineering, 67: 145-156. https://doi.org/10.1016/j.optlaseng.2014.10.011

[2] Wu, T.Y., Fan, X., Wang, K.H., Pan, J.S., Chen, C.M., Wu, J.M.T. (2018). Security analysis and improvement of an image encryption scheme based on chaotic tent map. Journal of Information Hiding and Multimedia Signal Processing, 9(4): 1050-1057.

[3] Yadav, R., Sachin, Singh, P. (2024). Multiuser medical image encryption algorithm using phase-only CGH in the gyrator domain. Journal of the Optical Society of America A, 41(3): A63-A72. http://doi.org/10.1364/JOSAA.507308

[4] Abdelfattah, M.G., Hegazy, S.F., Obayya, S.S. (2024). Optical essential secret image sharing using unequal modulus decomposition and gyrator transform. Optical and Quantum Electronics, 56(1): 107. http://doi.org/10.1007/s11082-023-05639-2

[5] Wu, T.Y., Fan, X., Wang, K.H., Pan, J.S., Chen, C. M. (2019). Security analysis and improvement on an image encryption algorithm using Chebyshev generator. Journal of Internet Technology, 20(1): 13-23. http://doi.org/10.3966/160792642019012001002

[6] Fytas, N.G., Martín-Mayor, V., Parisi, G., Picco, M., Sourlas, N. (2019). On the critical exponent α of the 5D random-field Ising model. Journal of Statistical Mechanics: Theory and Experiment, 2019(9): 093203. http://doi.org/10.1088/1742-5468/ab3987

[7] Reis, A.B.S., Silva, A.C., de Paiva, A.C., Gattass, M. (2019). Automatic prostate lesions detection on MR images based on the Ising model. Journal of Computational and Theoretical Nanoscience, 16(2): 341-350. http://doi.org/10.1166/jctn.2019.8019

[8] Liu, Z., Zhang, Y., Li, S., Liu, W., Liu, W., Wang, Y., Liu, S. (2013). Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains. Optics & Laser Technology, 47: 152-158. http://doi.org/10.1016/j.optlastec.2012.09.007

[9] Liu, Z., Xu, L., Lin, C., Dai, J., Liu, S. (2011). Image encryption scheme by using iterative random phase encoding in gyrator transform domains. Optics and Lasers in Engineering, 49(4): 542-546. https://doi.org/10.1016/j.optlaseng.2010.12.005

[10] Perez, R.A., Vilardy, J.M., Pérez-Cabré, E., Millán, M.S., Torres, C.O. (2023). Nonlinear encryption for multiple images based on a joint transform correlator and the gyrator transform. Sensors, 23(3): 1679. http://doi.org/10.3390/s23031679

[11] Zhang, Y., Zhao, R., Zhang, Y., Yi, S., Lan, R. (2024). Visually semantics-aware color image encryption based on cross-plane substitution and permutation. IEEE Transactions on Industrial Informatics, 20(8): 10576-10586. http://doi.org/10.1109/TII.2024.3395646

[12] Sutar, S.A. (2018). Differential power attack analysis of ultra-lightweight block cipher BORON. In 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 365-370. http://doi.org/10.1109/ICECA.2018.8474902

[13] Tang, Z., Yang, Y., Xu, S., Yu, C., Zhang, X. (2019). Image encryption with double spiral scans and chaotic maps. Security and Communication Networks, 2019(1): 8694678. http://doi.org/10.1155/2019/8694678

[14] Karawia, A.A. (2018). Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. Entropy, 20(10): 801. http://doi.org/10.3390/e20100801

[15] Pradhan, B., Sengupta, S. (2018). Chaotic-cipher based memory efficient symmetric key cryptosystem. In 2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT), Kolkata, India, pp. 1-3. http://doi.org/10.1109/EDCT.2018.8405066

[16] Shao, Z., Shang, Y., Fu, X., Yuan, H., Shu, H. (2018). Double-image cryptosystem using chaotic map and mixture amplitude-phase retrieval in gyrator domain. Multimedia Tools and Applications, 77: 1285-1298. http://doi.org/10.1007/s11042-016-4279-0

[17] Chen, J.X., Zhu, Z.L., Fu, C., Yu, H., Zhang, L.B. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation, 20(3): 846-860. http://doi.org/10.1016/j.cnsns.2014.06.032

[18] Wu, J., Liao, X., Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. Signal Processing, 153: 11-23. http://doi.org/10.1016/j.sigpro.2018.06.008

[19] Agung, K., Suprajitno, H. (2018). Image encryption based on pixel bit modification. Journal of Physics: Conference Series, 1008(1): 012016. http://doi.org/10.1088/1742-6596/1008/1/012016

[20] Ye, G., Pan, C., Huang, X., Zhao, Z., He, J. (2018). A chaotic image encryption algorithm based on information entropy. International Journal of Bifurcation and Chaos, 28(1): 1850010. http://doi.org/10.1142/S0218127418500104

[21] Patil, M., Gawande, A., Dilendra. (2020). Biometric image encryption based on chaotic sine map and information entropy. In Intelligent Data Communication Technologies and Internet of Things: ICICI 2019, Coimbatore, India, pp. 724-732. http://doi.org/10.1007/978-3-030-34080-3_81

[22] Li, C., Zhao, F., Liu, C., Lei, L., Zhang, J. (2019). A hyperchaotic color image encryption algorithm and security analysis. Security and Communication Networks, 2019(1): 8132547. http://doi.org/10.1155/2019/8132547

[23] Zhang, Y. (2019). A fast image encryption algorithm based on convolution operation. IETE Journal of Research, 65(1): 4-18. http://doi.org/10.1080/03772063.2017.1400406

[24] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., Blažauskas, T. (2019). An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. Entropy, 21(7): 656. http://doi.org/10.3390/e21070656

[25] Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S.M., Mosavi, M.R. (2014). A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimedia Tools and Applications, 71: 1469-1497. http://doi.org/10.1007/s11042-012-1292-9