

Secure Image Encryption using E-Fractal-Based Non-Commutative Group and Hash Function

Ola N. Kadhim¹, Fallah H. Najjar^{2,3*} and Ali J. Ramadhan⁴

¹Technical Institute of Al-Mussaib, Al-Furat Al-Awsat Technical University, Najaf, Iraq

²Department of Computer System Techniques, Technical Institute of Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq

³Department of Emerging Computing, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.

⁴Department of Computer Techniques Engineering, College of Technical Engineering, University of Alkafeel, Najaf, Iraq

Abstract. Due to the importance of data security at present, an encryption algorithm based on the principle of non-commutative group, hash function, and E-fractal has been proposed. Key generation depends on the array values generated by the braid group and using them as input to the SHA-3 (256) which increases the strength of the key because it generates values in one direction only. The results of the hash function are determined by the Lorenz hyper-chaotic system initial values, and four image-size arrays are generated as the final image-encryption keys using the RC4 algorithm. Then the use of the E-fractal diffusion method. To bolster the security of the encryption, it is employed to disperse the pixel values., adopting the control word that increases the randomness of the data. The security analysis of the proposed encryption algorithm demonstrates that it is difficult to decipher due to the presence of the hash function in addition to its easy implementation within seconds, and the efficiency scale was calculated that showed its strength in effectively resisting attacks by others.

1 Introduction

Given what we are witnessing today of a very wide development in the techniques of transmitting data over the Internet, which was adopted mainly for communication between people, it has boosted the increased interest in the security of that data and the information sent to preserve the privacy of people regardless of whether those data are of great importance or not. Deal with this data in numerical formats to be dealt with more smoothly and easily. One of the techniques used at present to protect that information is the encryption technology that deals with complex mathematical formulas to produce algorithms that are difficult to break and analyze. There are other fields I took to enter the field of coding other than mathematics, such as engineering, medicine, and others. In this paper, we will use the field of mathematics and engineering together to create an effective and attack-resistant algorithm [1]. Non-abelian group-based Cryptography has become the latest trend in research, one was

* Corresponding author: fallahnajjar@atu.edu.iq

used by Ko, Lee, and others, and another was used by Anshel, Anshel, and Goldfeld. These are set from non-commutative groups, Examples of groups include Braid groups, Polycyclic Groups, Thompson Groups, Grigorchuk Groups, and others [2], used to generate keys useful for encryption and decryption. A chaotic system possesses properties such as sensitivity to beginning values, pseudo-randomness, and unpredictable motion trajectories, all of which are cryptographic properties, and it is thus commonly utilized in image encryption [3]. The SHA-3 technique is used to determine the hash value of a plaintext image as the beginning value of the chaos systems, and the chaos-generated sequences are used to scramble the global pixel positions and pixel values of the images. Scrambling and diffusion are the two basic forms of image encryption algorithms. The pixels' locations are transformed to achieve scrambling. The correlation between neighboring pixels can be reduced by transforming the locations of the pixels, resulting in encryption. Diffusion is accomplished by altering the pixel values. Diffusion encryption can improve the unpredictability of cipher pictures while also breaking their statistical properties [4].

The rest of the paper is structured as follows. In Section 2, you can see prior studies on the subject topic by studying similar papers. Section 3 discusses the braid group and graph, E-fractals, and chaotic systems using basic theories. Section 4 introduces the suggested method's technique as well as the encryption process. Section 5 presents the simulation results and security analysis. Finally, Section 6 takes this paper to a conclusion.

2 Related Works

Ping et al. (2018) proposed a cellular automata and chaos-based picture encryption technique. There were two stages of confusion and dispersion in the encryption technique. To reduce processing complexity, the two-dimensional Logistic-adjusted-Sine map was employed to climb the image's pixel position during the confusion stage. A second-order cellular automata permuted the image pixels during the diffusion step. The encryption algorithm was reversed and undistorted after each repetition [5].

A. Kamal et al. (2021) planned a coding system for color images by using one of the modular Fractional Chaotic Sine Map (MFC-SM) ciphers, which generates good randomness with an Elliptic Curve. Where Elliptic Curve Diffie-Hellman (ECDH) was used to create secret parameters for key exchange and they worked on statistical analysis and sensitivity testing of the proposed system, which gave an effective algorithm in resisting hostile attacks [6].

Salvatore, C. et al. (2020) In this study, braid group was combined with encryption techniques like as RSA to calculate "public" and "private" encryption keys, which are the signatures in the DNA. The usage of "Chern Simons" is a key component of this method, as is the application of the system to biology [7].

N. Khalil (2021) He proposed an algorithm to encode gray and color images based on the hybrid 2D composite chaotic map combined with a sine–cosine cross-chaotic map to distort the image pixels and be very unclear after the generation of the key and XOR is made with the original image. As a final step, it creates a chaotic one-dimensional map of the XOR work with the image that was encoded in the previous step. One of its advantages is the combination of one-dimensional and two-dimensional chaotic systems [8].

3 Theoretical Framework

This part will outline the subjects addressed in this article.

3.1 Braid Group

The braid groups B_N is an infinite non-commutative group of N -strands, defined with generators $\{\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}\}$ Where $N \geq 2$. B_N is defined as:

$$B_N = \left\langle \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1} \mid \begin{array}{l} \alpha_i \alpha_{i+1} \alpha_i = \alpha_{i+1} \alpha_i \alpha_{i+1} \text{ for } 1 \leq i \leq n-2 \\ \alpha_i \alpha_j \alpha_i = \alpha_j \alpha_i \alpha_j \text{ for } |i-j| \geq 2 \end{array} \right\rangle \quad (1)$$

The braid group B_N is referred to as the braid group on N strands, and is usually pictured using so called braid diagrams. In the diagrams, the generators α_i are twists of adjacent strands, braiding the $(i + 1)$. In any two strands i and $i + 1$, a positive crossing is the strand $i + 1$ goes in front of strand i , and a negative crossing is the strand i goes in front of the strand $i + 1$ [9].

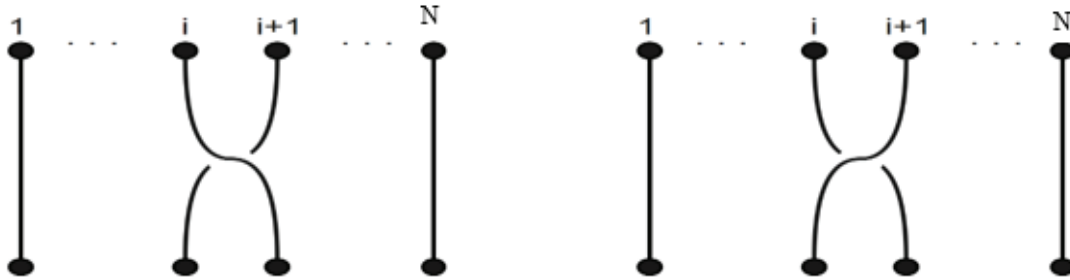


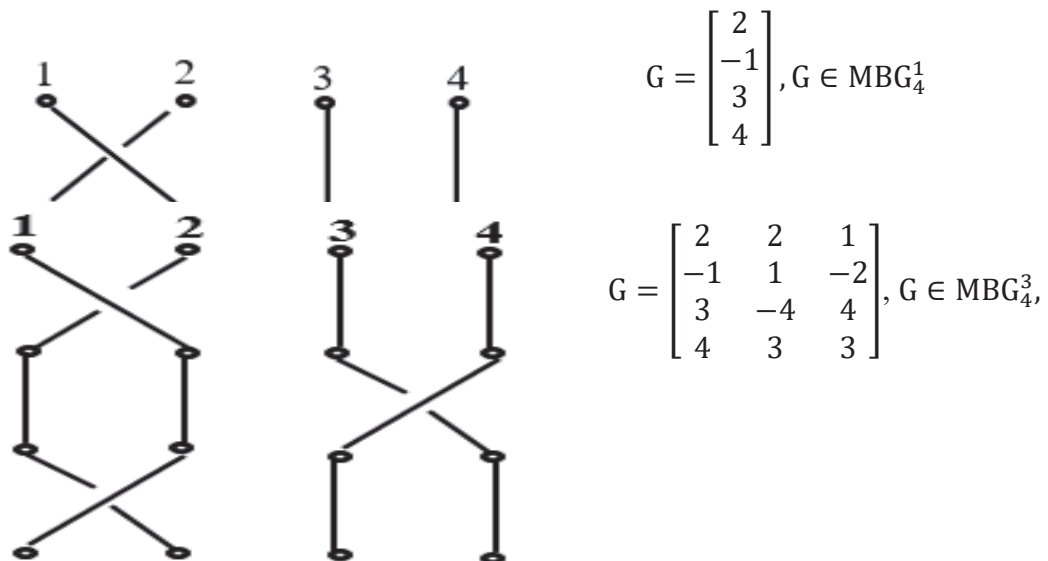
Fig 1. The elementary braid $\alpha_1^{-1} \alpha_1$

3.2 Braid Graph

Definition1: A braid graph with N strands and L level, denoted by BG_N^L , is a graph $BG_N^L = ((U_1, U_2, E_1), (U_2, U_3, E_2), \dots, (U_{L-1}, U_L, E_L))$, where (U_i, U_{i+1}, E_i) is a biregular graph of $G \forall 1 \leq i \leq L - 1$, such that the vertices in the set U_1 and U_L have degree one, there vertices in the set U_2, \dots, U_{L-1} have degree two, and the number of vertices in U_i is $N \forall 1 \leq i \leq L - 1$.

Definition2: Let $BG_N^L = ((U_1, U_2, E_1), (U_2, U_3, E_2), \dots, (U_{L-1}, U_L, E_L))$, and every vertices in the set $U_i, 1 \leq i \leq L - 1$ are labeled with numbers $1, 2, \dots, N$. A matrix of size $N \times L$ such that if $[u_i, u_k]$ is an edge in E_j and u_i goes in front u_k then u_i is k^{th} element with positive sign otherwise negative sign in j^{th} rows it's called braid matrix of BG_N^L , the set of all braid matrices denoted by MBG_N^L [10].

Example1:



3.3 Lorenz Hyper-chaotic System

Chaotic systems are instrumental in cryptography because of the randomness of their generated values and whose values are very sensitive to change. There are many types of chaotic systems. We used the hyper-chaotic Lorenz that generates four random strings. It can be formulated as follows:

$$\begin{aligned} x' &= a(y - x) + w, \\ y' &= cx - y - xz, \\ z' &= xy - bz, \\ w' &= -yz + rw \end{aligned}$$

The Lorenz hyperchaotic system has four parameters $a, b, c,$ and r . The Lorenz hyper-chaotic system is a hyper-chaotic state when $a = 10, b = 8/3, c = 28,$ and $1.52 \leq r \leq 0.06$. When $r = -1$, the hyper-chaotic system is iterated. Figure 2 shows the simulation results of the Lorenz hyper-chaotic system [11-13].

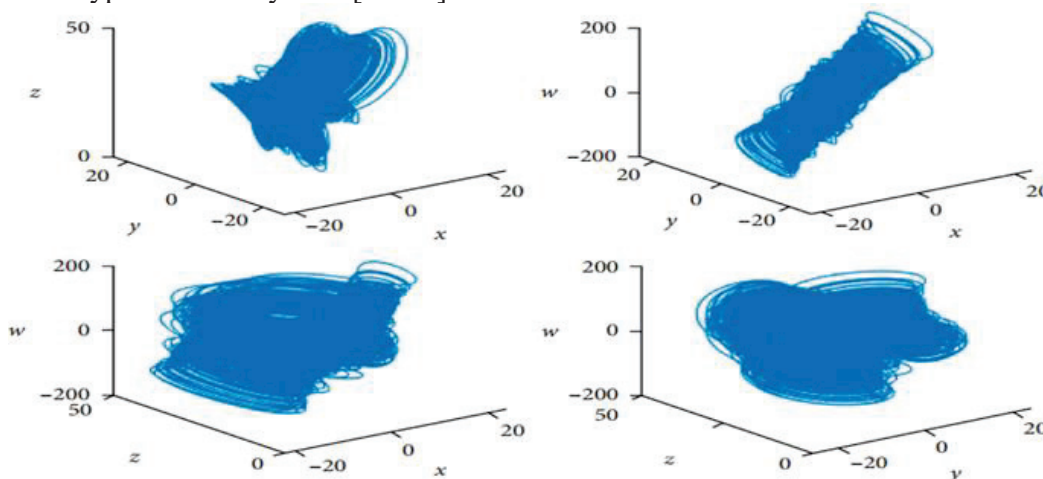


Fig 2. The Lorenz hyper-chaotic system's phase diagram.

3.4 E-fractal Diffusion

The fractal theory was first established by Mandelbrot in 1967. It is considered an important part of non-linear sciences and has been used in various fields. Specializing in the field of mathematics that studies the properties of a particular class of phenomena, so this theory can be exploited in the field of cryptographic research because the correlation of algorithms in the field of mathematics. Geometric shapes can be used in fractal theory as a new concept in cryptography to enhance the security of encrypted data. There are several geometric shapes, one of which is H-fractal, which appears in figure 3 [14].

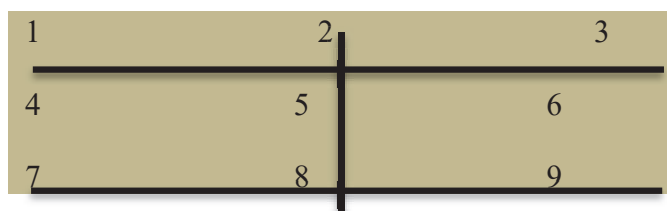


Fig. 3. The diagram of H-fractal diffusion.

The proposed method in this paper E-fractal cross-diffusion, which divides the image into $3 * 3$ blocks and is processed between every two opposite pixels, according to Figure 4.

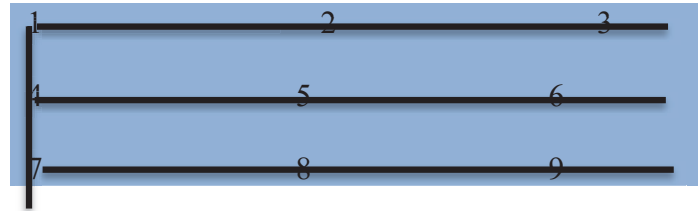


Fig. 4. The diagram of E-fractal diffusion.

To execute a crossover operation between pixel 1 and pixel 7 in Figure 4, employ the term "control pixel 4". Next, do a crossover operation between pixel 1 and pixel 3, utilising the term "control pixel 2". Next, do a crossover operation by utilising the term "control pixel 8" to combine pixel 7 and pixel 9. Conduct a crossover operation between pixel 4 and pixel 6, utilising the word control pixel 5.

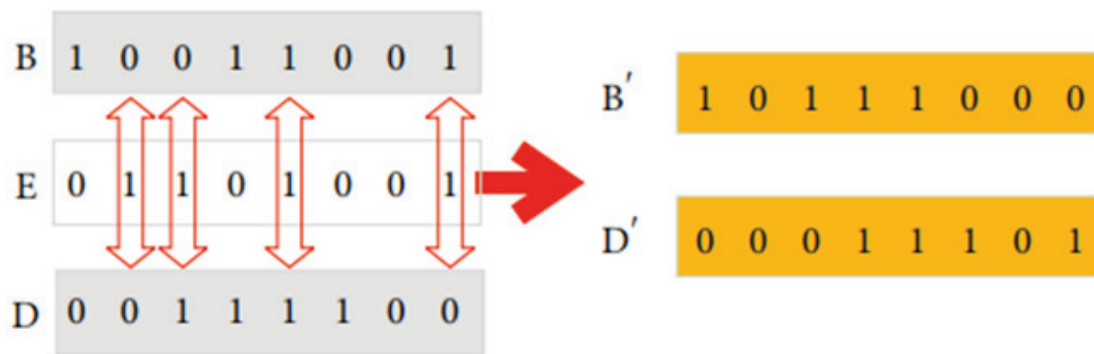


Fig. 5. Crossover operation.

Figure 5 illustrates the crossover operation method, assuming that pixel B and pixel D denote the upper and lower boundaries of the block, respectively, and that pixel E serves as the intermediary control word between them. Each pixel is translated into binary format and compared with the binary bit in the control word. If the binary bit is "1", the binary bits of pixels B and D are swapped. If the binary bit is "0", no operation is performed on the bits.

When exclusively applying E-fractal to the image, it results in the depiction shown in Figure 6. The image has dimensions of 256 * 256 and the process begins from the top left corner, progressing vertically and then horizontally.

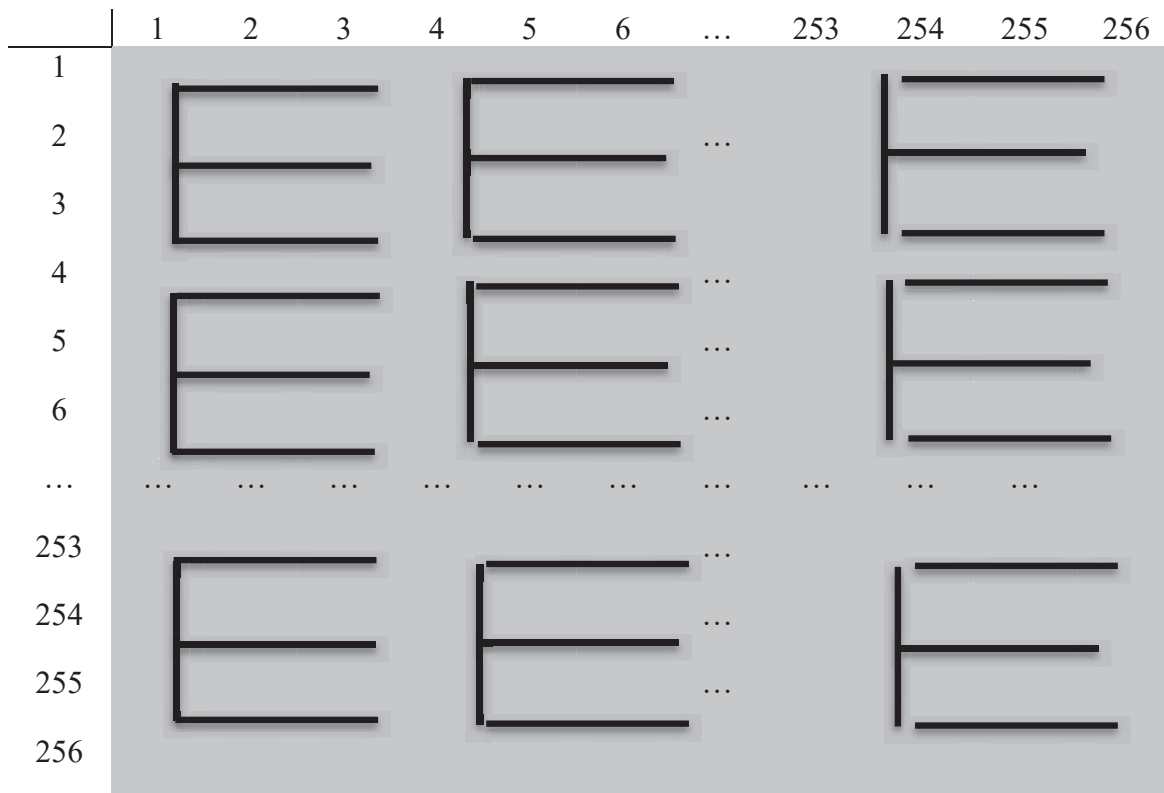


Fig. 6. The image covered by the E-fractal

4 Methodology

There are two aspects to the proposed technique, the first is key generation and the second is image data encryption.

4.1 Key generation

As it is known, the SHA-3 algorithm is highly secure because it generates one-way values that cannot be found in Inverse [15]. It effectively enhances the security and robustness of the algorithm as the resulting numeric braid group is fed to the hash function, producing a new 256-bit data string. Then that series is divided into four groups, each group consists of 64 bits as h_1, h_2, \dots, h_{64} , and the Lorenz hyper-chaotic system initial values are calculated as in the equations below:

$$\begin{aligned}
 x_0 &= (h_1 \oplus h_2 \oplus h_3 \oplus h_4 \dots \dots \dots \oplus h_{64}) \\
 y_0 &= (h_{65} \oplus h_{66} \oplus h_{67} \oplus h_{68} \dots \dots \dots \oplus h_{128}) \\
 z_0 &= (h_{129} \oplus h_{130} \oplus h_{131} \oplus h_{132} \dots \dots \dots \oplus h_{192}) \\
 w_0 &= (h_{193} \oplus h_{194} \oplus h_{195} \oplus h_{196} \dots \dots \dots \oplus h_{256})
 \end{aligned} \quad (2)$$

Through the laws of Lorenz hyper-chaotic, four matrixes of a size similar to the size of the original image will be generated. Where size of image N represent number of row and M represent number of columns.

$$X = \begin{bmatrix}
 u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & \dots & \dots & \dots & u_{1,M} \\
 u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & \dots & \dots & \dots & u_{2,M} \\
 u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} & \dots & \dots & \dots & u_{3,M} \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 u_{N,1} & u_{N,2} & u_{N,3} & u_{N,4} & \dots & \dots & \dots & u_{N,M}
 \end{bmatrix}$$

$$\begin{array}{l}
 y = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & \dots & \dots & \dots & u_{1,M} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & \dots & \dots & \dots & u_{2,M} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} & \dots & \dots & \dots & u_{3,M} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ u_{N,1} & u_{N,2} & u_{N,3} & u_{N,4} & \dots & \dots & \dots & u_{N,M} \end{bmatrix} \\
 z = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & \dots & \dots & \dots & u_{1,M} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & \dots & \dots & \dots & u_{2,M} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} & \dots & \dots & \dots & u_{3,M} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ u_{N,1} & u_{N,2} & u_{N,3} & u_{N,4} & \dots & \dots & \dots & u_{N,M} \end{bmatrix} \\
 w = \begin{bmatrix} u_{1,1} & u_{1,2} & u_{1,3} & u_{1,4} & \dots & \dots & \dots & u_{1,M} \\ u_{2,1} & u_{2,2} & u_{2,3} & u_{2,4} & \dots & \dots & \dots & u_{2,M} \\ u_{3,1} & u_{3,2} & u_{3,3} & u_{3,4} & \dots & \dots & \dots & u_{3,M} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ u_{N,1} & u_{N,2} & u_{N,3} & u_{N,4} & \dots & \dots & \dots & u_{N,M} \end{bmatrix}
 \end{array}$$

4.2 Encryption Image

After the key generation stage comes to the encryption stage. An algorithm must be used to encrypt the input. The algorithm used in this paper RC4 is one of the stream cipher algorithms. One of the reasons for using this algorithm is that it is easy to implement, fast and highly secure, in addition to the variable key length. The algorithm's private key generation is based on the hyper-chaotic Lorenz. Each layer is encrypted using this algorithm and with a different key. The first layer is encoded based on the X matrix generated by the Lorenz hyper-chaotic. The second layer is based on the Y matrix, and the third layer is based on the Z matrix.

$$\begin{aligned}
 R_{im_{enc}} &= RC4 (R_{ed} im_{org}, X) \\
 G_{im_{enc}} &= RC4 (G_{reen} im_{org}, Y) \\
 B_{im_{enc}} &= RC4 (B_{lue} im_{org}, Z)
 \end{aligned}$$

Subsequently, the three layers are merged to generate a color encryption image.

$$im_{encryption} = (R_{im_{enc}}, G_{im_{enc}}, B_{im_{enc}})$$

Then a fractal is applied to the encrypted image to increase the randomness of the image and increase security.

Encryption Algorithm:

Input: original image.

Output: encryption image.

Begin

Step1: Generating an array of numbers through a braid group the resulting values can be positive or negative.

- Step2: Utilize the SHA-3(256) method on the matrix obtained in step one to derive a hash sequence H.
- Step3: The Hash sequence H is used to obtain the initial variables x_0, y_0, z_0 , and of the Lorenz hyper-chaotic system.
- Step4: Using the Lorenz hyper-chaotic system to generated four sequences X, Y, Z, and W are as keys.
- Step5: The encryption of the image matrix (Red layer) is obtained using the RC4 technique between the original picture (Red layer) and sequence X.
- Step6: The image matrix encryption of the Green layer is obtained using the RC4 technique applied to the original image's Green layer and the sequence Y.
- Step7: The image matrix encryption (specifically the Blue layer) is obtained by applying the RC4 method on the original image (specifically the Blue layer) and a sequence called Z.
- Step8: The combination of the Red, Green, and Blue layers after encryption from steps 5, 6, and 7.
- Step9: Apply E-fractal on result from step 8.
- Step10: Combine the three layers and thereafter implement techniques for differential Attack Analysis.

End

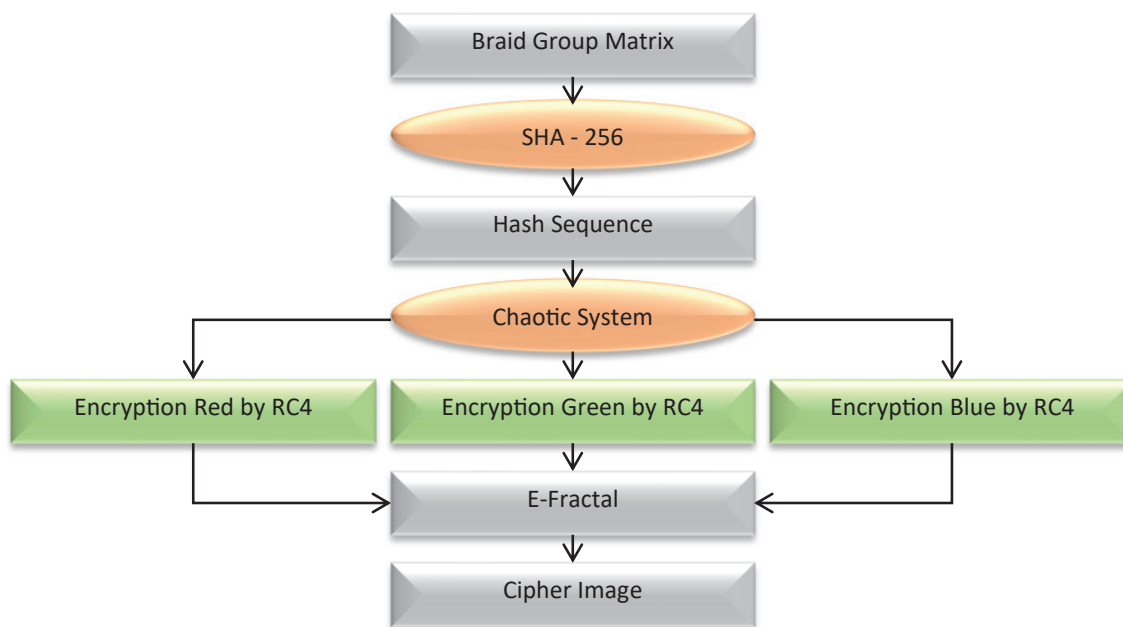


Fig. 7. The diagram illustrating the sequential steps of the encryption technique.

5. Security Analysis and Simulation Results

Simulated experiments were used to test the effectiveness and practicality of our approach. In this section, we will show the results obtained.

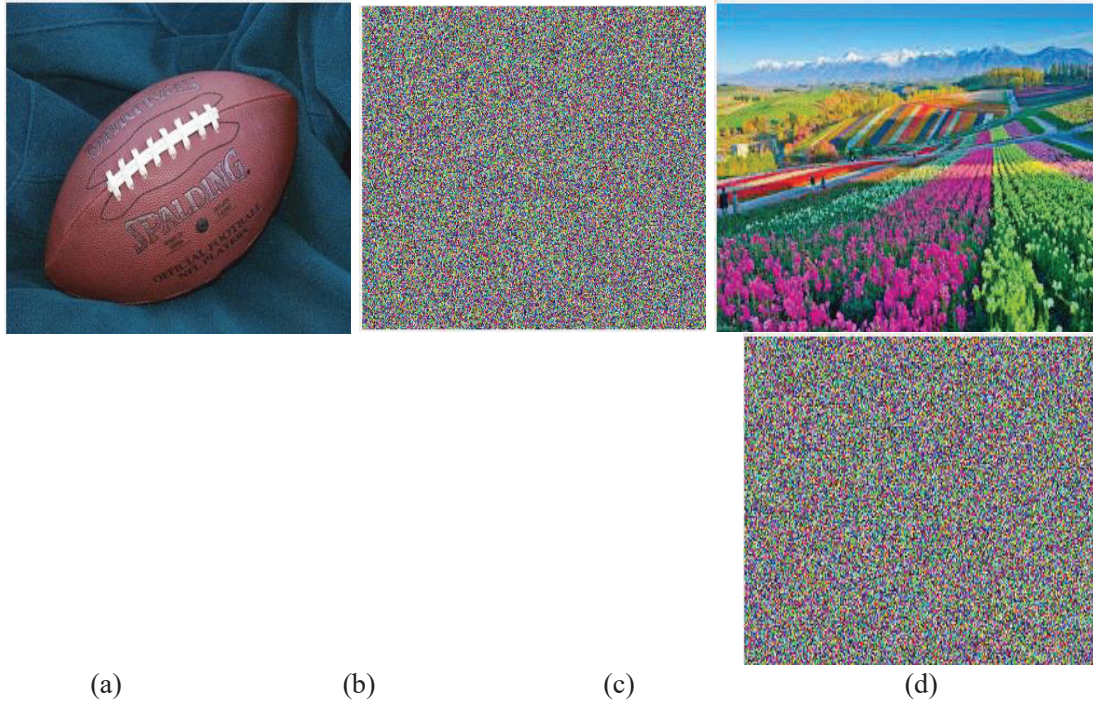


Fig. 8. (a) and (c) correspond to the original images, whereas images (b) and (d) correspond to the encrypted images.

5.1 Analysis of the sensitivity of key variables

The use of Non-commutative sums with the hash function gives a strong and efficient key flexibility. It is not easy to identify the output from the hash function. The primary area of the algorithm is too large enough to withstand attacks. In addition to Lorenz hyper-chaotic, which is an additional step to generate large randomness of the key so that these values are sensitive to any slight change in it. Simply changing the hash function and not giving the correct output will generate the key with incorrect values.

5.2 An analysis of differential attacks

The encryption system is highly susceptible to even little alterations, whether they occur in the key or in the encrypted image. Any minor alteration will result in a substantial modification in the appearance, regardless of whether it is the initial or encrypted image. The system's ability to endure attacks increases proportionally with increased sensitivity levels. For this section, we employed two metrics: Number of Pixel Changes Rate (NPCR) and Unified Average Changing Intensity (UACI). The following equations display both measures [16, 17]:

$$NPCR = \frac{\sum_i \sum_j |\text{sign}(P_1(i,j) - P_2(i,j))|}{M \times N} \times 100\% \quad (3)$$

$$UACI = \frac{\sum_i \sum_j |(P_1(i,j) - P_2(i,j))|}{255 \times M \times N} \times 100\% \quad (4)$$

The plain image is P_1 , and the cipher image is P_2 . The image size is represented by M and N , respectively. The symbol function is represented by $\text{sign}(x)$, and its computation technique is as follows:

$$\text{sign}(x) = \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}$$

The optimal value for NPCR is 100%, whereas for UACI it is 39.4635%. The NPCR scale increases and reaches its maximum value when there is a significant difference and change between pixels. The algorithm outcomes will be elucidated in Table 1 following the application of a series of photographs.

Table 1. A comparison of the NPCRs and UACIs of the four images.

Measures	NPCR	UACI
Img1	100	31.8218
Img2	100	31.7638
Img3	100	31.0423
Img4	100	35.0187

6. Conclusion

It is good not to generate the key directly or use an easy-to-crack algorithm, so it is preferable to combine two or more methods to produce a difficult-to-know key. In this paper, the key is generated indirectly through three steps represented by using a braid group to create an array that has the input of SHA-3(256) and the output of the hash function is the Lorenz hyperchaotic system's primitive values. After the image is encrypted by RC4 algorithm, an E-fractal structure is applied to increase the randomness of the pixels. The proposed method yielded good results by observing the scale ratios. This adds that the algorithm has a high resistance against hostile attacks, as it can also be used in the scope of the text, audio and video encryption.

References

1. N. Koduri, "Information security through image steganography using least significant bit algorithm," Master Thesis, Information Security and Computer Forensics University of East London, 2011
2. G. Lanel, T. Jinasena, and B. J. I. Welihinda, "A Survey of Public-Key Cryptography over Non-Abelian Groups," vol. **21**, no. 4, p. 289, 2021.
3. S. Dhall, S. K. Pal, and K. Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic system," *Signal Processing*, vol. **146**, pp. 22-32, May. 2018
4. C. Fu, J.-J. Chen, H. Zou, W.-H. Meng, Y.-F. Zhan, and Y.-W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express*, vol. **20**, no. 3, pp. 2363–2378, 2012.
5. P. Ping, J. Wu, Y. Mao, F. Xu, and J. Fan, "Design of image cipher using life-like cellular automata and chaotic map," *Signal Processing*, vol. **150**, pp. 233-247, Sep. 2018.
6. A. Kamal, E. A. Hagra, H. J. C. S. El-Kamchochi, and I. Systems, "Dynamic fractional chaotic biometric isomorphic elliptic curve for partial image encryption," pp. 18-18, 2021.
7. S. Capozziello, R. Pinčák, and E. J. S. Bartoš, "A Supersymmetry and Quantum Cryptosystem with Path Integral Approach in Biology," vol. **12**, no. 8, p. 1214, 2020.
8. N. Khalil, A. Sarhan, M. A. J. O. Alshewimy, and L. Technology, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps," vol. **143**, p. 107326, 2021.

9. Wilson, Jenny. "The geometry and topology of braid groups." RTG Geometry Topology Summer School. University of Chicago 2018.
10. H. S. Razaq;, S. A. Albermany; and H. H. Abbass, "Fuzzy Extractor Computation for Cryptography Based on Braid RADG Group," Master thesis, Faculty of Computer Science and Mathematics, University of Kufa, 2019.
11. Qu, Shao Cheng, Di Liu, and Li Wang. "Synchronization of hyper-chaotic Lorenz system and its application in secure communication." Key Engineering Materials. Vol. 467. Trans Tech Publications Ltd, 2011.
12. R. Jing-Ya, S. Ke-Hui, and M. J. A. P. S. Jun, "Memristor-based Lorenz hyper-chaotic system and its circuit implementation," vol. **65**, p. 190502, 2016.
13. K. Shahna and A. J. S. P. I. C. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," vol. **99**, p. 116495, 2021.
14. X. Zhang, L. Wang, Y. Niu, G. Cui, & S. Geng (2019). Image Encryption Algorithm Based on the H-Fractal and Dynamic Self-Invertible Matrix. Computational intelligence and neuroscience, 2019.
15. C. Dobraunig, M. Eichlseder, F. J. I. f. A. I. P. Mendel, and G. U. o. T. Communications, "Security Evaluation of SHA-224, SHA-512/224, and SHA-512/256," 2015.
16. Y. Wu, J. P. Noonan, S. J. C. j. m. j. i. s. Agaian, and J. o. S. A. i. T. technology, "NPCR and UACI randomness tests for image encryption," vol. **1**, no. 2, pp. 31-38, 2011.
17. X. Wang, X. Zhu, and Y. Zhang, "An image encryption al-gorithm based on josephus traversing and mixed chaoticmap," IEEE Access, vol. **6**, p. 23733–23746, 2018.