Technium Vol. 4, Issue 2 pp.24-35 (2022)
ISSN: 2668-778X
www.techniumscience.com

Digital Image Encryption Techniques: Article Review

Enas Ali Jameel [1,2], Sameera Abbas Fadhel[2]
[1]Department Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq
[2]Department Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq

Corresponding name: **Sameera Abbas Fadhel** and e-mail: sameeraabbasfadhel@uomosul.edu.iq

Abstract. In this age of the multi-media, images have an important impact on communication. When users upload images over an insecure communication network, total security is a difficult problem to address in order to maintain image confidentiality. Also, encryption is a technique for keeping images secret. This study gives a basic introduction to cryptography, as well as a concise overview regarding the many image encryption algorithms' elemental security criteria. This paper includes an overview of several image encryption approaches as well as a comparison of discrete image encoding techniques, before coming to a conclusion and recommending future research

Keywords. Image processing, Image encryption, Comparison techniques, Image encoding, Scrambling

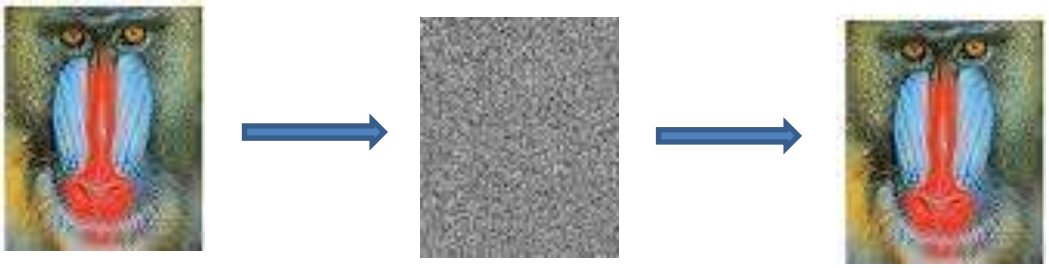
1. INTRODUCTION

The information and internet technologies are exploding rapidly. Therefore, interactive media is frequently used in the communication, for example, audio, images, and videos. The images make up a sizable portion of multimedia. National-security agencies, military, and diplomatic issues, for instance, all rely heavily on images for communication. Because such images might contain extremely confidential information, users must entail extreme protection when storing them in an untrustworthy repository. When users want to send images via an insecure network, it's critical to guarantee complete security. In a nutshell, an image must be protected against a variety of security threats.

The fundamental goal of protecting images is to ensure their integrity, confidentiality and authenticity [1]. Encryption is one of the approaches that may be used to make images more secure. Encryption can be defined as one of the processes which uses a key for transforming images into cryptic images. In addition, by using an approach of decryption on cipher image [2] that is typically a reverse execution regarding encryption, users might get the original image. Figure 1 depicts the process of encryption in which (a) the primary image is displayed; a user utilizes an encryption approach to create a secret image; (b) encrypted image is displayed as a result of encoding procedure. In a case where the receiver gets that hidden image, he/she uses the method of the decryption for recovering original data, as shown in Figure (c).

There are two major categories of cryptography, asymmetric and symmetric key cryptography. In secret key or symmetric cryptography, recipients and senders use the same key in decryption and encryption [2], as depicted in Figure 2, whereas public key or asymmetric cryptography utilizes separate

keys in decrypting and encrypting message [2]. For encoding and decoding images, this approach uses a private key and a public key, respectively. The two keys are distinctive, although they have a mathematical connection, as shown in Figure 3.



a b c

Figure 1: Encryption process

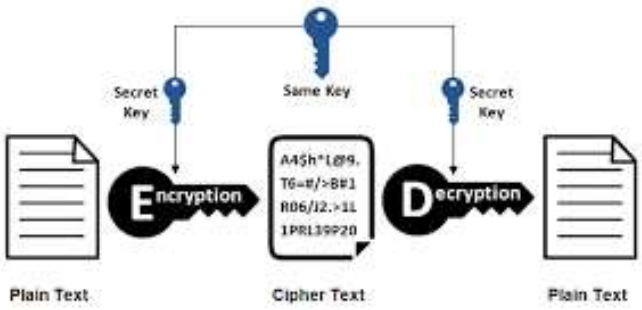


Figure 2: Symmetric Key Encryption

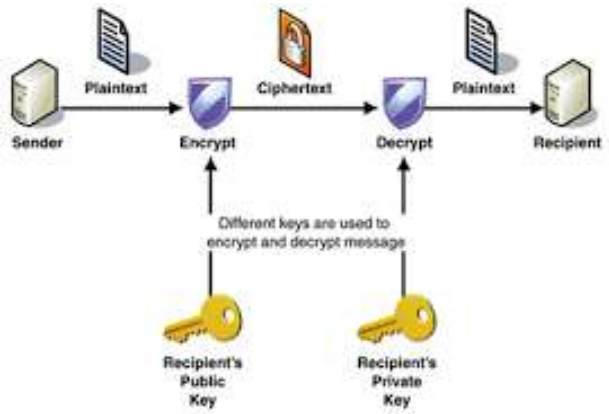


Figure 3: Asymmetric Key Encryption

Primarily, cryptography has two main categories; symmetric key cryptography and asymmetric key cryptography, in symmetric or secret key cryptography, senders and recipients use a same key in encryption and decryption [2] as illustrated in Figure 2, while in asymmetric or public key cryptography uses different keys in encrypting and decrypting messages [2]. This technique applies a public key and

a private key to encode and decode an image respectively. However, both keys are unique, but mathematically have a connection as illustrated in Figure 3.
For encrypting the data, a variety of methods are available, including RSA, DES, and AES. Yet, while such algorithms are essential for enciphering the text data, they are ineffective for image encryption [3]. Because images have inherent characteristics, like high redundancy and a significant correlation between adjacent pixels, it's simple to obtain the value of a pixel's neighbors. As a result, images require an effective way for achieving invulnerability [4]. Image encryption methods majorly use three approaches: (1) pixel permutation: the pixels are scrambled by the algorithm [5, 6], (2) pixel substitution: the pixel value is modified by the encryption technique, and (3) visual transformation. Because of its non-linear and one-way features, artificial neural network (ANN) represents unique method for the implementation of image protection [8,9]. Calculating the end result in ANN is simple; however, getting raw data from the conclusion is a difficult issue. Therefore, determining initial data from results back without weight and bias values will be impossible [9, 10]. Figure 4 shows feed forward NN, with equation (1) assisting in determining network's output.

$$y = f\left(\sum_{i=1}^{n} w_i x_{i+b}\right) \qquad (1)$$

In which *y* represent the output, *x* represent the input; *b* represents the bias, *w* represent weight, and n represent number of the neurons in different layers.

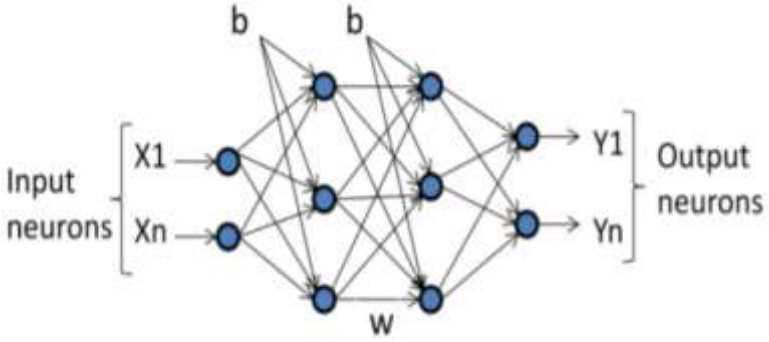


Fig 4: Artificial neural network structure

Compression is a method of encoding images by abbreviating the images. As a result, understanding the compressed form of an image is challenging. Furthermore, the fundamental benefit of encryption via compression is that it minimizes the image size without losing information if lossless compression is used. When a small amount of distortion is acceptable, lossy compression might be applied.

2. IMAGE SECURITY PARAMETERS

In general, a good encryption method meets a number of security requirements, including the following:

1.1. A subsection

Large key space: For thwarting brute force attacks, a huge key space is required [11]. The key space of a 512-bit key, for instance, is 2,512 (approximately 10,154 possibilities of the combinations). Therefore, if a computer does 1010 calculations per second, finding the correct key will take around 10136 years.
A subsubsection.

2.2. Key sensitivity

It ensures that, in spite of a minor change in key, the system will produce totally opposite results [12]. As a result, an encryption method must be key-sensitive.

2.3 Uniform Histogram of the Image

The histogram gives data on distribution of frequency regarding density estimation and continuous pixels [13,14]. To be safe against a known plaintext attack, a cipher image must have a uniform histogram, as shown in Figure 5, which compares the histograms of encrypted as well as original images.

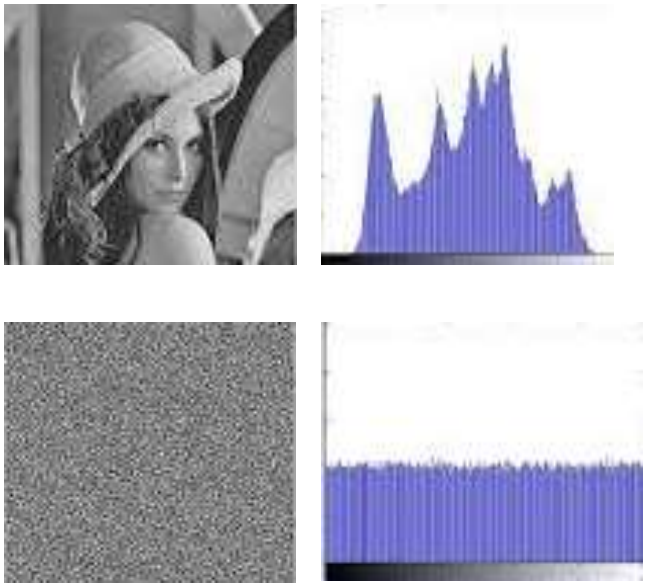


Figure 5. Exhibit differences of histogram of the encrypted and original images

2.4 Information entropy

It determines the system's uniform distribution and level of uncertainty [14]. As a result, in the encryption process, an encryption approach must demonstrate randomness and uniform distribution. The next formula (2) is used to compute information entropy.

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i) log_2[P(P(m_i)] \qquad (2)$$

In which p (mi) represents likelihood of a pixel and N represents number of the bits in every one of the pixels. For graylevel images, every one of the pixels has 8 bits, which is why, the pixel probability is 1⁄ 2 ^{8}. As a result, a graylevel image's information entropy is H (m) = 8. Yet, because obtaining optimal entropy is difficult in practice, a small difference is acceptable.

Correlation analysis: which evaluates the relation between 2 adjacent plain-image pixels and cipher image 15]. The association between two neighboring pixels in an encrypted image has to be low. If yi and xi are two-pixel pairs, then equation (6) may be used to compute the correlation coefficient [16,17].

$$E(x) = \frac{1}{N}\sum_{i=0}^{N} x_i\,, \qquad (3)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (4)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} \big(x_i - E(x)\big)\big(y_i - E(y)\big) \quad (5)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} \quad (6)$$

In which yi and xi are graylevel value of a pair neighboring pixels, N represent number of the pairs (xi, yi) and E(x) represent average value of of xi and E(y) represent average value of yi.

2.6 Differential analysis

The algorithm's invulnerability against differential image attacks is measured by NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [17]. As a result, a high NPCR value is effective. NPCR analyzes the rate of the pixels change in a coded image after the modifications in one pixel of prime image [18]. UACI also calculates the variation of the intensity of the relevant pixel in the encrypted and plain images [19,20]. UACI and NPCR might be determined using formulas (8) and (7), respectively, if C2 and C1 represent two-cipher image before and after a 1-bit modification in original image [17].

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(I.J) \times 100\% \quad (7)$$

Where if C1 (i, j) ≠C2 (i, j), then D (i, j) = 1, otherwise, D (i, j) = 0

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C1(i,j) - C2(i,j)|}{225}\right] \times \frac{100\%}{M \times N} \quad (8)$$

Where, M & N represent dimensions and (i, j) represents image coordinates.

3. METHODS OF IMAGE ENCRYPTION

3.1 Encryption of the Image with the Use of the XOR Operation and Affine Transformation

Various researchers have shared an approach in this work that utilizes a 64-bit key in the process of encryption. Initially, the proposed approach uses an affine transformation for dispersing the pixels by using four 8-bit sub keys. The algorithm then decomposes a image into 2*2-pixel blocks and performs an XOR operation on one of blocks utilizing 4 sub keys of 8-bits to change the value of the pixels. For producing an imparted image, this imparted system performs a transform process on the original image. Following that, the suggested approach uses XOR operation to this altered image for producing a full cipher image, as shown in Figure, which shows the cipher and original image after the XOR operation, as well as the histogram differences. The results show that the proposed approach is less successful at minimizing pixel correlation and also has a small key space. In the key technique employed via the encryption process, such algorithm lacks sufficient complexity. As a result of the easy XOR operation and short key, the imparted approach does not offer an acceptable level of security for images.

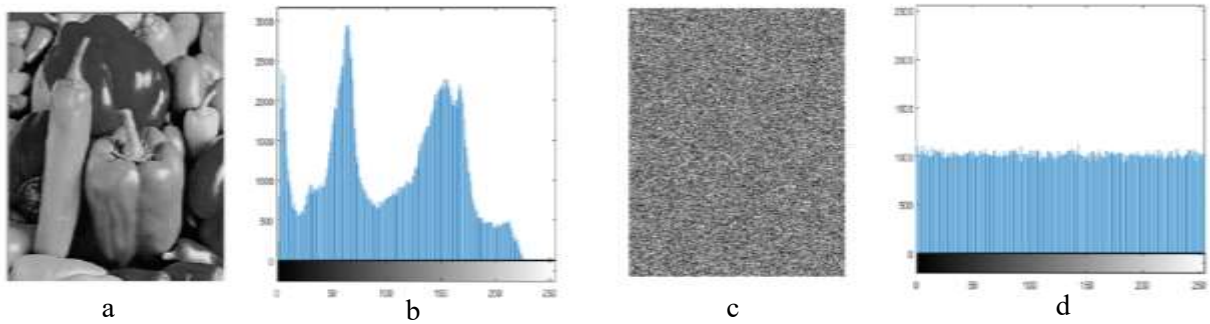


Figure 6: (a) plain-image; (b) histograms of the plain-image; (c) Cipher image after XOR operation; (d) histograms of the cipher-image

3.2 Chaotic System for Image Encryptions

Y. Zhou and L. Bao [11] proposed a new chaotic system that consists of 3 unique 1D chaotic maps in this script. The proposed method uses a Logistic map as controller in order to determine whether to produce random sequences using a Sine map and a Tent map [2]. The algorithm then employs the substitution-permutation network (SPN) topology to acquire the diffusion and confusion properties [11, 25]. For a large key space, this approach utilizes a 240-bit key. This key primarily comprises all of the new chaotic system's initial values and parameter settings, as well as excessive sensitivity in key changes for decryption and encryption. As a result, the suggested method offers great security towards the brute force attacks, in addition to excessive chaotic behavior and key sensitivity.

3.3 Digital Image Encryption Approach Based upon 1-D Random Scrambling

Ping Guan, Qiudong Sun, Yunfeng Xue, and Yongping [26] proposed a 1D random scrambling-based approach in this work. The algorithms start by converting a 2D image to a 1D vector, after that using 1D random shuffling [26]. The approach next applies an anti-transformation to dispersed vector in order to produce encrypted image. As a result, the presented approach doesn't necessitate iterative computing because 1 or 2 executions suffice for optimal result. Because of the scrambling process, the histogram of cipher image and original image are equal after the experimentation. The scrambling technique, on the other hand, reduces the correlations between pixels while having no effect upon histogram. Due to the fact that cipher image's histogram will give a lot of information regarding the original image. As a result, the proposed approach is less appropriate for high-confidentiality images.

3.4 An Approach for Image Encryption Based upon the Explosive nxn Block Displacement Succeeded by the Inter-Pixel Displacements of the RGB Attribute of the Pixel

Nidhi Chandra and Amnesh Goel [27] have proposed an effective approach for decomposing the original image into n*n blocks in their study. After that, an algorithm of transformation is used to reduce relation between pixels [27]. This approach is mostly divided into two stages. At the initial stage, this algorithm conducts horizontal displacement of the block before moving on to vertical block displacement. The approach executes inter pixel displacement of the values of RGB in the second stage. Each one of the stages has a stage mask or key that is used during the procedure [27]. Figure. 7 (a) is an original image of 300*300 pixels, and figure 7 (b) is the result of applying horizontal block displacement to it. In addition, after applying vertical displacement of the block to a horizontally displaced image, the image that has been shown in figure 7(c) is created. After that, a cipher image is created by applying

inter pixel displacement in RGB values, as shown in figure 7. (d). The results of the experiments show that the proposed method generates a robust cipher image using explosive displacement in the values of the RGB.

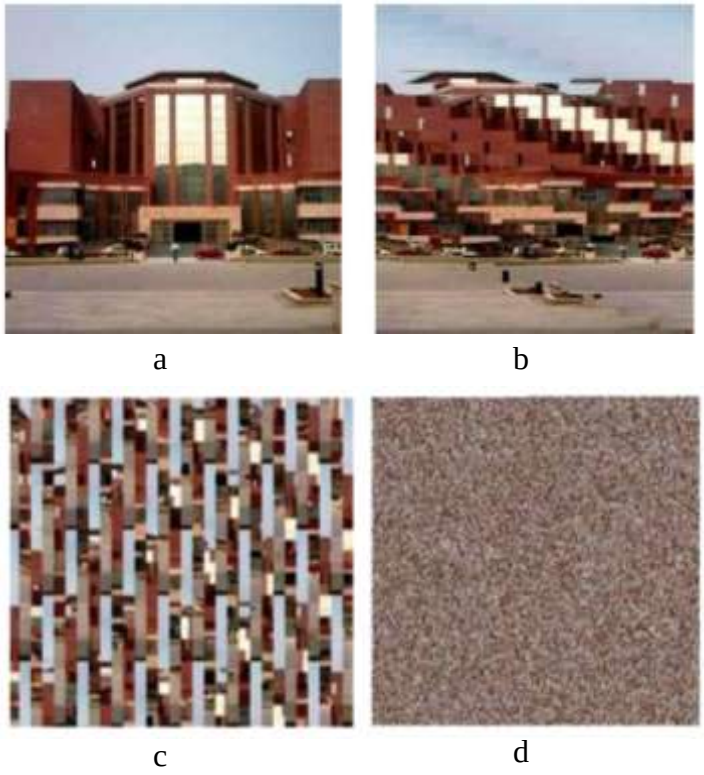


Figure: (a) Original-image; (b) Horizontal displacements at (10*10) block size; (c) Vertical Cipher Image displacements at 10*10 blocks size; (d) Cipher Image

3.5 NN Method for the Encryption/Decryption of the Digital Data

A study by [28] have proposed a method for scanning an image pixel by pixel. After that, it applies permutation and substitution to such pixels to transform them. The encoding technique garbles the transformed image by inserting the impurity. To ensure effective security, this method employs two levels of enciphering. For decrypting the cipher image, the presented approach leverages an ANN. There are three steps to decryption. The system removes the additional impurity in first stage. The network then rejects excess conjoined columns in matrix in the second stage. The received image data and weight values that have been saved after training have been used for the purpose of stimulating the network in the third step.

The significance of this approach is owing to the availability of random encryption on the side of the sender, which eliminates the need for an exchange of keys. As a result, the suggested approach delivers a high level of safety. The drawbacks is that decryption takes longer. A study conducted by [29,30] shows how to create encryption algorithms using genetic algorithms in cryptography, as well as the randomness characteristics of Linear Congruential and Fibonacci generators, as well as CNN and dynamic adaptive diffusion. This entire method of conveying secret information is extremely secure and dependable. As a result, no one will be able to deduce the message without knowing the pseudorandom sequence. These studies were completed and evaluated. C# was used for implementation purposes.

Following the analyses of the suggested approach, it is obvious that it meets the aims which any encryption technique must meet. Lastly, experimental analysis and numerical analysis are used to confirm the algorithms' effectiveness and practicality.

3.6. Encryption method for Image Security

A study conducted by [31, 32] devised a method based on bit level permutation. To meet the diffusion and confusion features, this system uses 2 Boolean operations on pixel bits: Rotation and XOR. In addition, the technique encrypts an image by performing a sequential XOR operations on all pixel bits in the image, which were succeeded by a circular right rotation regarding such bits. Following that, the approach repeats these 2 steps several times in order to achieve greater security. Furthermore, this approach encrypts and decrypts using the same secret key.
A study conducted by [33] developed a system referred to as (FCIES-Fr-HP) which showed and compared the cipher image with its related histogram, as shown in Figure 8. The input image histogram depicted in Figure 8 (d) appears to have a certain pattern which highlights the notion connected to image structure. The randomization properties of the output value may be observed in the histogram of the encryption image with even and randomly distributed pixel values. Yet, the histogram of cipher image depicted in Figure 8 (e) exemplifies consistently distributed pixel values, making information gathering complicated for the hacker. Furthermore, the estimated deviation between absolute matrices of decrypted and plain images that have been given in Figure 8 (f) demonstrates the suggested FCIES-Fr-HP Scheme's superiority in terms of effective decryption and encryption.

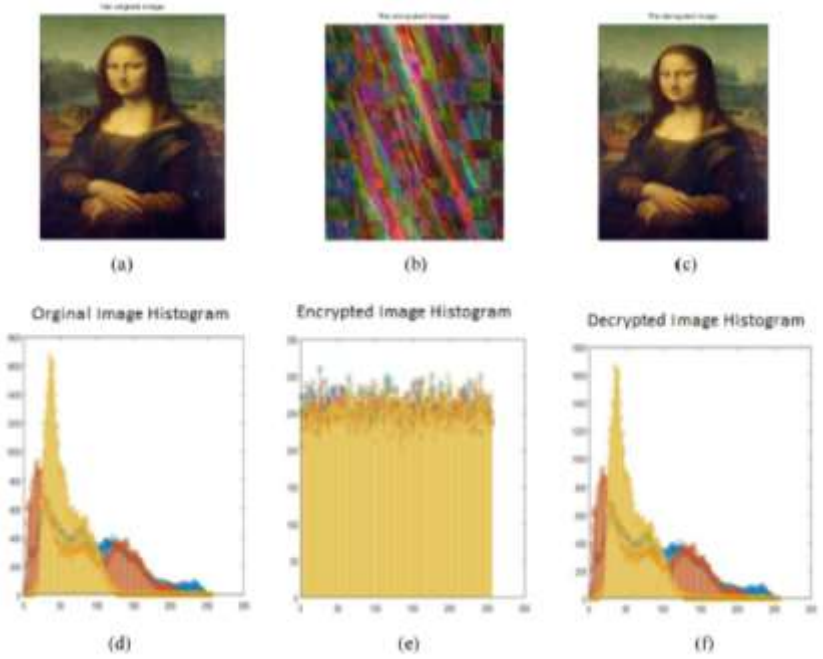


Figure 8. The original plain image, the encrypted image, the decrypted images derived based on the enforcement of the proposed FCIES-Fr-HP scheme.

3.7. A 2-Layer Chaotic Network Based Image Encryption Method

Navin Rajpal and Anchal Jain [34] have demonstrated a substitution and diffusion method. For encryption and decryption, the suggested system uses two-layer chaotic NN. This method employs a

logistic chaotic map for designing the NN's biases and weights, as well as external key to give initial condition. In general, the proposed approach uses an 80-bit key. Yet, in both decoding and encoding, the chaotic sequence is generated in the same way. The approach uses the network's first layer for diffusion and the 2nd layer for substitution, with layers being arranged in reverse order for decipherment. As a result, the given approach offers strong security against brute force attacks as well as attacks based on chosen plaintext or known plaintext.
Using Recursive Cellular Automata (RCA) and Deoxyribonucleic Acid (DNA), Homayun, Abdorreza, and Rasul [35] suggested a new approach for image encryption. The encryption of images is done in two stages. A logistic map has been used for the cellular shift in image columns and rows during permutation. The RCA and DNA are after that utilized to modify the graylevel of pixels to new values during diffusion. This approach yielded an ideal entropy value of 7.9994 and a coefficient of correlation that equals 0.0001, indicating good results. Furthermore, newly suggested approach has been shown to improve the level of the resistance to a range of the attacks by encrypting images in a desirable way.

3.8. Cryptographic Approach for Image Encryption

Due to the faster communication medium and effective internet technology, information transformation has lately been a hot topic [36]. Huge amounts of data are transferred across a variety of transferring mediums nowadays, with images being one of them. Singh, Parida, and Pradhan must use any cryptographic technology, such as encryption, to guarantee confidentiality and present ownership of the data. To present a new image encryption cryptography approach that combines two different image encryption methods in order to improve data security. Arnold's cat map and Zaslavskii map are two different approaches. The two approaches are used for decryption and encryption. In this study, we first encrypt the image with the use of Zaslavskii approach, and after that re-encrypt the encrypted image with the use of Arnold's cat map to achieve the desired image utilizing two encryptions. The final encrypted image is after that decrypted with the use of Arnold's cat map, and the decrypted image is after that decrypted utilizing Zaslavskii decryption in order to provide the final derived image that must be identical to original image. Which suggested approach, which has a high correlation value and high entropy value, provides users with more key values for improved unpredictability and security. The UACI and NPCR, which are utilized for every little change in pixels, as well as entropy and correlation coefficient values, are used to verify the efficiency of image encryption systems.

3.9. SD-AEI: Advanced Encryption Method for images

Somdip Dey [37] has introduced a combined method. The proposed approach is based on three cryptographic techniques: Extended Hill Cipher, Bit rotation and reversal, and Modified MSA Randomization [37]. In addition, the suggested technique encrypts an image in four phases. The algorithm produces distinctive number from symmetric key in the first step. Depending on symmetric key's length, the 2nd stage performs bit rotation and reversal. The system then uses the Extended Hill Cipher algorithm for encryptions in third phase. The technique then utilizes the modified MSA randomization method for substitution in the fourth phase. Because of the added randomization, empirical results have confirmed that the SD-AEI encoding approach is dominating on the SD-EI.

3.10. Digital Encryption Based upon Multidimensional Chaotic System and Pixel Locations

Hazern M. Al-Najar [38] had provided a proposal to image encryption approach depending on multi-dimensional chaotic function in the present work. Also, this system adjusts the value of the pixels by dispelling them. The imparted approaches utilize two substitution approaches to modify the pixel value and the 2 scrambling operations for pixel scattering. In addition, the proposed course encrypts the image in the following way: the algorithm uses the 1st scheme of substitution based upon index value of the column, then uses first scrambling approach based on X, Y, and Z planes of the Rossler formula. The system then performs a second replacement method based on the value of row index, succeeded by a

2nd plan of shuffling that is based on the X, Y, and Z planes [38]. Observations have corroborated that the proposed approach has sensitivity to initial condition as well as being invulnerable to brute force attacks and other attack types as a result of the large key space, which is 10^45.

4. CONCLUSIONS

The present paper examined a variety of image encryption methods and concluded that the chaotic technique has the most uncertainty and delivers the most security. Furthermore, the work reveals that NPCR is independent of key sensitivity; thus, in block-based encryption systems, the encrypted block values must be reliant upon values of the other cipher blocks in order to obtain sufficient NPCR. The results demonstrate that scrambling alone is insufficient to provide exceptional security; a substitute must be used in addition to shuffling. As a result, this work concludes that a superior image encoding approach must possess the next properties in order to offer exceptional security: (i) present a large key space, (ii) have high key sensitivity, (iii) create an even histogram, (iv) meet Shannon's diffusion and confusion properties, (v) efficiently decrease correlation between 2 neighboring pixels, (vi) present uncertainty in this system, and (vi) have a high NPCR value (about 100%) and a proper rate of the UACI (about 33%).

5. FUTURE WORK

Since machines' calculating powers are continually expanding, almost all image encryption approaches suffer from a number of flaws with regard to security and speed. As a result, image enciphering algorithms necessitate efficient, continual enrichment. Images take up more space on the network than text data and demand more bandwidth to send. Generally, there's a scarcity of excellent image encryption approaches which may as well minimize size (i.e. compress image) of encoded image. Furthermore, the recipient expects the decrypted image to reproduce original data without any distortion. As a result, operating in speed, space, and security is now a must.

References

[1] Stinson, D. R. (2005). Cryptography: theory and practice. Chapman and Hall/CRC.
[2] Choo, K. K. R., Domingo-Ferrer, J., & Zhang, L. (2016). Cloud Cryptography: Theory, Practice and Future Research Directions. *Future Gener. Comput. Syst*., **62** (C), 51-53.
[3] Marwaha, M., & Bedi, R. (2013). Applying encryption algorithm for data security and privacy in cloud computing. *International Journal of Computer Science Issues (IJCSI), 10* (1), 367.
[4] Hou, J., Jiang, M., Guo, Y., & Song, W. (2019). Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model. *Journal of Information Security and Applications*, 47, 329-334.
[5] Srivastava, A. (2012). A survey report on Different Techniques of Image Encryption. *International Journal of Emerging Technology and Advanced Engineering*, **2** (6), 163-167.
[6] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, **20** (18), 5162
[7] Patel, S., Bharath, K. P., & Kumar, R. (2020). Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique. *Multimedia Tools and Applications*, **79** (43), 31739-31757.
[8] Kengnou Telem, A. N., Meli Segning, C., Kenne, G., & Fotsin, H. B. (2014). A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. *Advances in Multimedia*, 2014.
[9] Lakshmi, C., Thenmozhi, K., Rayappan, J. B. B., Rajagopalan, S., Amirtharajan, R., & Chidambaram, N. (2021). Neural-assisted image-dependent encryption scheme for medical image cloud storage. *Neural Computing and Applications*, **33** (12), 6671-6684.

[10] Chalam, S. V., & Singh, M. K. (2012). Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP. *International Journal of Image Processing (IJIP),* **6** (1), 13.
[11] Bao, L., Zhou, Y., Chen, C. P., & Liu, H. (2012, June). A new chaotic system for image encryption. *In 2012 International Conference on System Science and Engineering (ICSSE)* (pp. 69-73). IEEE.
[12] Sethi, N., Sharma, D. (2012, December). A new cryptology approach for image encryption. *In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing* (pp. 905-908). IEEE.
[13] Xu, S., Wang, Y., Guo, Y., & Wang, C. (2009, December). A novel chaos-based image encryption scheme. *In 2009 International Conference on Information Engineering and Computer Science* (pp. 1-4). IEEE.
[14] Fu, C., Lin, B. B., Miao, Y. S., Liu, X., & Chen, J. J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics communications*, **284** (23), 5415-5423.
[15] Yang, H., Wong, K. W., Liao, X., Zhang, W., & Wei, P. (2010). A fast image encryption and authentication scheme based on chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, **15** (11), 3507-3517.
[16] Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering*, 2012.
[17] Diaconu, A. V., & Loukhaoukha, K. (2013). An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. *Mathematical Problems in Engineering*, 2013.
[18] Zhang, L., Liao, X., & Wang, X. (2005). An image encryption approach based on chaotic maps. *Chaos, Solitons & Fractals*, **24** (3), 759-765.
[19] Gong, Q., Wang, H., Qin, Y., & Wang, Z. (2019). Modified diffractive-imaging-based image encryption. *Optics and Lasers in Engineering*, 121, 66-73.
[20] Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, **3** (3), 118-126.
[21] Li, X., Meng, X., Yang, X., Wang, Y., Yin, Y., Peng, X., & Chen, H. (2018). Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme. *Optics and lasers in engineering*, 102, 106-111.
[22] Singh, A., & Dhanda, N. (2015). DIP using image encryption and XOR operation affine transform. IOSR J. *Comput. Eng.*, **17** (2), 7-15.
[23] [23] Liu, Z., Yang, M., Liu, W., Li, S., Gong, M., Liu, W., & Liu, S. (2012). Image encryption algorithm based on the random local phase encoding in gyrator transform domains. *Optics Communications*, **285** (19), 3921-3925.
[24] Liu, H., Zhao, B., & Huang, L. (2019). A novel quantum image encryption algorithm based on crossover operation and mutation operation. *Multimedia Tools and Applications*, **78** (14), 20465-20483.
[25] Stinson, D. R. (2005*). Cryptography*: theory and practice. Chapman and Hall/CRC.
[26] Sun, Q., Guan, P., Qiu, Y., & Xue, Y. (2012, May). A novel digital image encryption method based on one-dimensional random scrambling. *In 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery* (pp. 1669-1672). IEEE.
[27] Goel, A., & Chandra, N. (2012, May). A technique for image encryption based on explosive n* n block displacement followed by inter-pixel displacement of RGB attribute of a pixel. *In 2012 International Conference on Communication Systems and Network Technologies* (pp. 884-888). IEEE.
[28] Joshi, S. D., Udupi, V. R., & Joshi, D. R. (2012, January). A novel neural network approach for digital image data encryption/decryption. *In 2012 International Conference on Power, Signals, Controls and Computation* (pp. 1-4). IEEE.
[29] Bharadwaj, G. V. S. E., Vijaya, K., Balaga, S. K., & Thanikaiselvan, V. (2018, March). Image Encryption Based on Neural Network Architecture and Chaotic Systems. In 2018 Second International

Conference on Electronics, *Communication and Aerospace Technology* (ICECA) (pp. 767-774). IEEE.
[30] Mert, A. C., Öztürk, E., & Savaş, E. (2019). Design and implementation of encryption/decryption architectures for bfv homomorphic encryption scheme. *IEEE Transactions on Very Large Scale Integration* (VLSI) Systems, **28** (2), 353-362.
[31] Singh, A., Singh, V. K., & Yadav, S. (2019, April). Image Encryption Technique Using Huffman Coding and Spatial Transformation. *In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 352-356). IEEE.
[32] Al-Husainy, M. A. F. (2012). A novel encryption method for image security. *International Journal of Security and Its Applications*, **6** (1), 1-8.
[33] Anandkumar, R., & Kalpana, R. (2019). Designing a fast image encryption scheme using fractal function and 3D Henon Map. *Journal of Information Security and Applications*, 49, 102390.
[34] Jain, A., & Rajpal, N. (2012, November). A two layer chaotic network based image encryption technique. *In 2012 National Conference on Computing and Communication Systems* (pp. 1-5). IEEE.
[35] Babaei, A., Motameni, H., & Enayatifar, R. (2020). A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. *Optik*, 203, 164000.
[36] Parida, R. R., Singh, B. K., & Pradhan, C. (2021). A Novel Approach for Image Encryption Using Zaslavskii Map and Arnold's Cat Map. *In Data Engineering and Intelligent Computing* (pp. 269-282). Springer, Singapore.
[37] Dey, S. (2012, July). SD-AEI: An advanced encryption technique for images. In 2012 Second *International Conference on Digital Information Processing and Communications (ICDIPC)* (pp. 68-73). IEEE.
[38] Al-Najjar, H. M. (2012). Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location. *International Journal of Computer Theory and Engineering*, **4** (3), 357.