An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator

Vandana Roy

Gyan Ganga Institute of Technology and Sciences, Jabalpur, India

Email: vandana.roy20@gmail.com

Abstract

The field of cryptography oversees the development of methods for transforming information between coherent and incoherent formats. Encryption and decryption techniques controlled by keys maintain the privacy of the substance and who can access it. Private key cryptography refers to methods of encryption and decryption that employ the same secret key. The alternative is public key cryptography, wherever the encryption and decryption keys are different. It is essential for the sanctuary of any crypto scheme that the confusion and diffusion properties be met. While the diffusion property rearranges the pixels in an image, the confusion property simply replaces the pixel values. In-depth discussion of a genetic-algorithm-based hybrid approach to secure and complex three-dimensional chaos-based image encryption (SCIE) has been presented. Here, we use mathematics edge, multipoint edges operator, and coupled transmutation operatives to accomplish permutation. In this method, a key stream is created using a 3D CSI (Compound Sine and ICMIC) map. Using a private key, hybrid operators are used to encrypt data. Several metrics were considered while evaluating the suggested algorithm's efficacy, including the UACI (Unified Average Change Intensity), correlation constant, NPCR (Net Pixel Change Rate). Experiments with the same have shown promising results in protecting real-time photos.

Keywords: SCIE; Image Encryption; NPCR; ICMIC; Information Security

1. Introduction:

Digital photos, which are increasingly being employed as data carriers, are unquestionably one of the resources that are most prone to vulnerability. Because of the rapid development of the internet, picture security has become a matter of great concern, which has necessitated the use of complex methods for image encryption. Medical diagnostic information is one example of highly sensitive data, the unauthorised disclosure of which might have extremely negative consequences [1]. When it comes to image encryption, dealing with large data sizes is the fundamental challenge that must be solved. Textual data techniques may not scale well to multimedia due to storage and processing time limits. In order to increase the entropy and significantly minimise the considerable correlation that exists between neighbouring pixels in the majority of natural photographs, we require an image encryption technique that is both complex and effective [2].

Data hiding can be managed at '2' degrees of security, low level and high level, despite the fact that it is nearly an absolute necessity in the modern day. In low-level security encryption, the visual quality of the encrypted image is poorer, but the content may still be read and understood in a significant way. When the security level is raised to its highest possible setting, the image transforms into incomprehensible random noise [3]. It is essential to have both the quality of secrecy and the methods to prevent information from slipping into the hands of unauthorised individuals. The use of cryptography ensures that only those with the appropriate authorization may decrypt the information that has been encrypted. A secure cryptographic calculation and method of procedure should be designed in such a way, and carried out in such a way, that an unauthorised

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

group is unable to identify the meaning of the encrypted data without the necessary decryption keys [4]. This will ensure the highest level of protection possible.
The integrity of the information ensures that the data have not been tampered with after they have been generated, transmitted, or stored. This indicates that the data have not been finished by having any additions, deletions, or replacements made to them yet. Cryptographic tools such as sophisticated marks or message validation codes can be used to differentiate between accidental modifications brought about by equipment failure or gearbox problems and malicious modifications done by an adversary [5]. Some inadvertent modifications can be attributed to gearbox problems or equipment failure. Even if non-cryptographic properties can be utilised to differentiate between inadvertent and deliberate updates, there is no guarantee that this will always be the case.
By doing an evaluation of the source's credibility, you can ensure that no new information has come to light. Through the use of source verification, the identities of data creators such as clients and systems can be validated. Message verification codes or digital stamps are the two most common methods that confirmation services utilise. This service could also be delivered by utilising strategies that use key assertion [6].
The authorization to carry out a specific function or operation pertaining to security. It is well knowledge that using encryption in administrative work can improve one's sense of personal safety. In most cases, approval is given after the successful implementation of a source verification service. In the world of key administration, the term "non-renouncement" refers to the authoritative management of an authentication topic achieved through the use of modern mark keys and digital testaments to an open key [7]. In the same way that a handwritten signature on a report would signify a dedication by the use of the testimony subject, a computerised mark might be able to do the same thing. The benefits of the digital revolution have not been realised without the accompanying drawbacks, such as limitations placed on the copying and sharing of digital multimedia system papers. Academics have been putting in a lot of hard work to come up with innovative and cost-effective document protection solutions that can be used in multimedia system documentation in order to meet the challenge that has been presented to them. New techniques, such as coded writing and digital watermarking, are introduced into this environment [8-10].

2. Related Work

The authors presented a strategy for embedding a code that protects confidential information within digital photographs. The chaos philosophy and the approach known as "the minimum important bit" are two methods that can be used to conceal a message within an image. In this particular instance, Bernoulli's chaotic maps are put to use to mimic the succeeding procedures, which are as follows: (i) Encode the data being transmitted across the communication channel before adding it to the shared image. (ii) The depiction's layouts, as well as the rows and columns into which the hidden message is inserted, are selected at random [11]. First, the message's statistical behaviour is altered with the help of a chaotic map, and then the message itself is concealed [12]. The proposed method of steganography encrypts sensitive data by means of a chaotic map, and then makes use of two additional chaotic maps in order to pseudo-randomize the pixel determination, so concealing the encoded data somewhere within the image. A variety of evaluation criteria are used on the outcomes of some of the experiments that have been previously published [13]. According to the findings of an experiment [14], the recommended method achieves much better results in terms of PSNR and image quality estimation when compared to the results obtained from competing methods.

The primary focus of the research team was on the development and application of a method for encrypting images by utilising the Arnold 3D cat map. For purposes of security, chaotic maps can be beneficial since it is very easy to build them, they are deterministic, and it is very difficult to forecast what will happen on them. The mechanisms of diffusion and substitution are broken down into their component parts in this manner [15]. During the phase of substitution, a chaotic map is used in order to rearrange the position of the image's pixels. In order to decipher the original picture, Arnold's 2D and 3D cat maps were utilised. A histogram study was able to validate the confidentiality of this encryption [16]. In a manner analogous to this, differential attacks utilising NPCR and UACI values have been utilised in order to assess the level of security provided by this strategy. The findings demonstrate that the suggested approach offers improved safety and is resistant to attacks based on standard differentials [17].

The authors proposed a chaos-based picture algorithm that is both effective and efficient. We employ a scheme of two free disordered purposes with a deep knowledge to the preliminary conditions in order to appropriately implement misperception and dispersal criteria for images of arbitrary entropy. This allows us to correctly implement both sets of criteria. One approach allows for the movement of pixels, while the other modifies the values of the pixels [18]. The subsequent new pixel association will pit neighbouring pixels with normally close values against the values that are radically different from one another, which will make deciphering the image even more difficult. Some logical procedures, including ex-or and rounded revolution, are utilised to

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

increase the framework's resistance to differential attacks [19]. These methods blowout the influence of a little variation in the lone pixel supremacy of the basic picture across multiple pixels in the cypher image. The examination into the problem indicated that the proposed strategy required less operations than the comparable method did in order to achieve the same level of key space, security, and encryption speed. A battery of tests and analyses, including an arithmetic examination, an analysis of key comprehension and key space, a research of the sensitivity of simple images, and a speed test [20-22], have proved the validity and safety of the suggested calculation. These results can be attributed to the fact that the calculation has been shown to be accurate. Even when used to low-entropy photographs, the suggested method has been shown to be both more secure and quicker than the algorithms that came before it [23, 24].

These algorithms are a subset of evolutionary algorithms, which are designed to solve optimisation problems by modelling natural evolutionary processes and searching for optimal solutions. An EA is a powerful instrument that can tackle some of the most difficult challenges that individuals are confronted with in today's world [25]. After providing a comprehensive explanation of the CEC-14 benchmark suite, the authors emphasised the influence that arithmetic edge has on set DE systems [26]. There are a number of genetic factors that contribute to the trait that was researched. The process through which this influence is accounted for in genetic traits is referred to as epistasis. In this example, the epistasis is represented graphically as the product of two separate charts that are controlled by vectors that are combined into a single, hybrid process. Out of all the other components that may have been used for the diagram, the Cartesian chart was chosen. Charts that use the Cartesian approach, on the other hand, are not the same thing as straight diagrams [27].

For the purpose of optimising the monarch butterfly's life, a strategy called the greedy approach coupled with a self-adaptive edge operator (GCMBO) has been suggested. Within the GCMBO, the Movement Administrator and the Butterfly Changing Administrator have been integrated into a single eager system. If more benchmark issues, especially applications that are used in the real world, are used in the future, it will be possible to achieve better performance [28]. Researchers have developed a system for the watermarking of grayscale images that is both secure and effective. The scheme is based on the Lagrangian twin support vector relapse (LTSVR) and the genetic algorithm (GA) in discrete Cosine transform (DCT) space. The use of fuzzy entropy is what is going to be used to figure out the essential components that the watermark will be inserted into. The inability to defend against attacks including rotation and translation is a significant flaw in the design. Researchers suggest for a paradigm of autonomous multi-goal development, which may simultaneously prioritise safety and quality of service for any particular computing resource [29]. Using the information that is already known about the target problem, a new edge method is being created with the intention of making the optimisation process even more effective.

3. The proposed Work:

The encrypted images are produced through an advanced chaos-based encryption method that makes use of a hybrid Genetic operator. This method is three-dimensional and chaotic. In the initial step of the process, two offspring are produced through the use of an arithmetic edge operator.

The newly created people are eventually destroyed into bit planes. The following process involves the multi point edge of these bit planes. To create a secret picture, image compounders use a combination of edge photos. Then we employ a hybrid mutations operator. Elements of an array are swapped out in a top-to-bottom direction using first boundary mutation. When its pixels are added in any direction other the horizontal or vertical, the result is a mutation that is not uniform. The pixels are then replaced using a circular shift and uniform mutation. The three-dimensional CSI maps are responsible for the creation of the most essential stream. Combining the results of the hybrid mutations results in the creation of the final encrypted image. Figure 1 depicts the proposed encryption arrangement.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

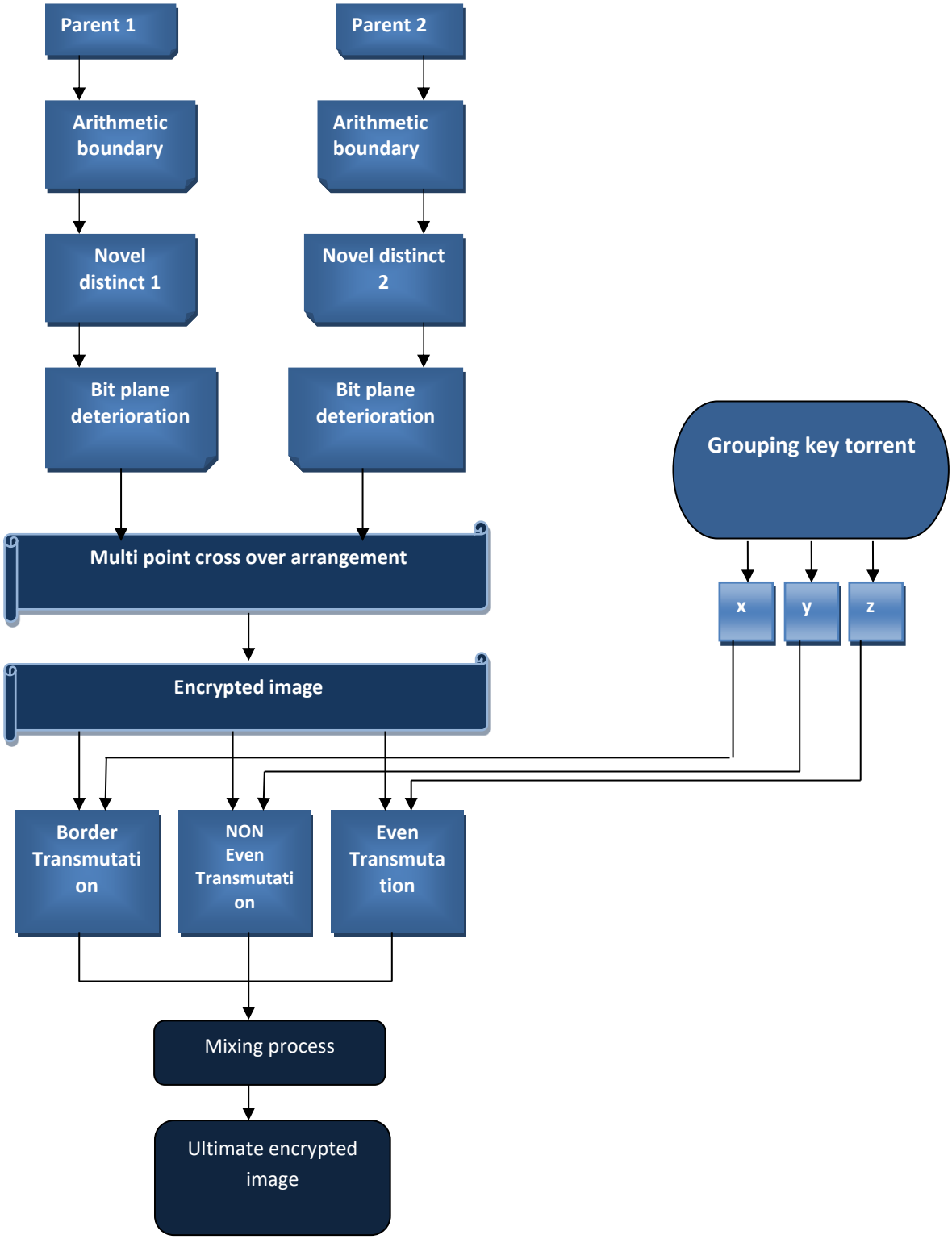

Figure 1: The Projected Encryption Algorithm system Design.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

SCIE Encryption Process:

1. Start with unmitigated input images.
2. Mathematical crossing-over between parent 1 and parent 2 is used.
3. Two brand-new pictures that we'll call N1 and N2.
4. Degenerate the bit planes of the 'N1' and 'N2' input pictures.
5. Use multipoint crossover to shift the bit set positions and reveal the hidden picture.
6. A secret key is made with the help of the 3-D CSI map.
7. Use a mixed-key-stream hybrid mutation.
8. The final encrypted output is mixed via the mutation process.
9. Determine the Entropy, Correlation Coefficient, NPCR, and UACI.

3.1. The representation ‘N1’ and ‘N2’ correspondingly signifies the novel entities that consequence from execution a mathematics edge process on ‘Parent 1’ and ‘Parent 2’. After that, fresh individuals take on the roles of parents 'Parent 1' and 'Parent 2' in order to produce the subsequent series.

3.2. The encryption computation is done using two different binary bit plane degeneration procedures. This is done using the Bit Plane Deterioration method. It is possible to represent a grayscale image using an 8-bit paired representation since individually pixel in the appearance has a worth that falls between 0 and 255. A grayscale spitting image can be converted into an 8-bit binary format by using bit plane degeneration. The higher bit plane contains the MSB, while the lower bit plane contains the LSB of the initial image. The initial step is a degradation of the simple image into eight bit planes.

3.3. The multipoint edge is a generalisation of the single point edge; it introduces a greater numeral of cut-points than the single point edge does. The scenario entails the selection of numerous positions based on arbitrary criteria. This process is used to obtain the first original image when bit plane decomposition is complete, and it then changes the bit position of the image to produce the second bit even disintegrated image. It is possible to modify the bit location of pictures N1 and N2 by using a technique called multipoint edge. Choose the greatest possible number of bits, and then put them to use to switch their positions in the two images. Alter the locations of the first image so that they correspond to those of the second image.

3.4. After performing a multipoint edge operation on 'N1' and 'N2', proceed to step 3.4 and compound the bit planes. In order to move the images from the MSB position to the LSB position. Get a picture that has been jumbled up. The newly encrypted image has been given the name child.

3.5. The population undergoes mutation after a hybrid task that guarantees to prevent all arrangements in the population from falling into a local ideal of the addressed problem. A child is arbitrarily changed from what its parents delivered in a hybrid form when they undergo transformation. It is an inherited administrator that may change the state of at least one bit in a chromosome.

3.6. 3D CSI Map:

When the value of 'b' is between (0,∞), the Combined of Sine and ICMIC (CSI) map displays chaotic behaviour with the control parameter 'A' in the interval [0,45]. This is the CSI map, delivered by given equations with having further higher orders of m(x).

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

$$p(x+1) = modulus\left(\left(q * m(x)\right) * \left(1 - m(x)\right)\right) \quad (1)$$

$$q(x+1) = modulus\left(\left(q * n(x)\right) * \left(1 - n(x)\right)\right) \quad (2)$$

$$r(x+1) = modulus\left(\left(q * s(x)\right) * \left(1 - s(x)\right)\right) \quad (3)$$

Sine and ICMIC map were used to build the key matrix. The mutation process was thrown into the new key stream that was generated. A logical 'x'-operated mutation of a border key. Then, using logical AND, we merged the 'y' key's non-uniform mutation with the 'z' key's uniform mutation.

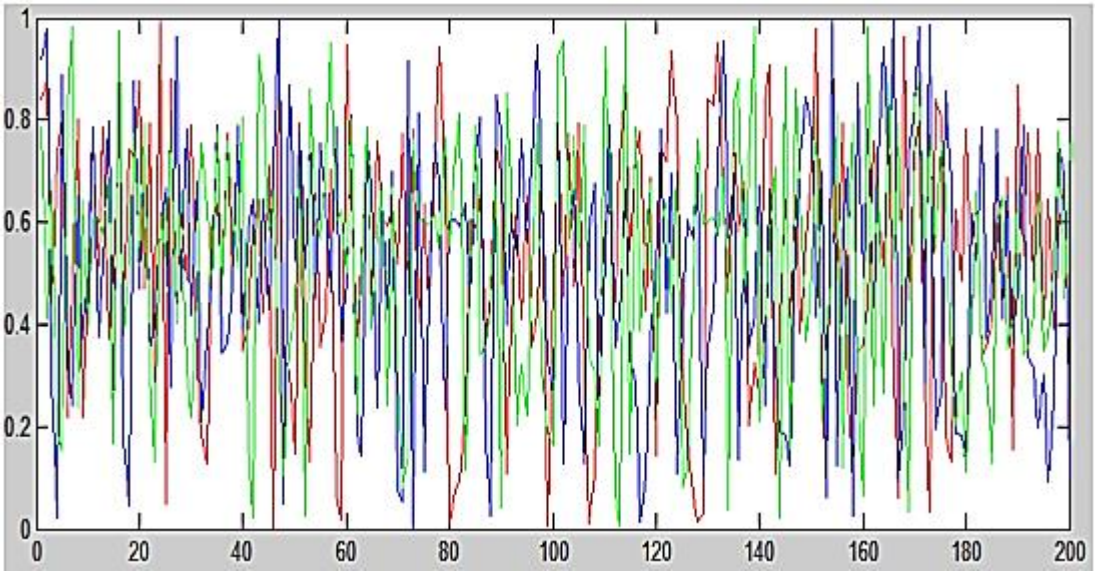

Figure 2: 3-D CSI map with 550 iterations.

A brand-new, triple-encrypted image was then created. Add complexity to the process by combining the three encrypted images into one. The 3D CSI map in Figure 2 exhibits chaotic behaviour. It seems to generate a more multifaceted set of arbitrary keys, which is useful for increasing confusion and dispersal.

4. Result and Discussion:

In this section, we are going to examine the correlation coefficients, entropy, and differential research that were used in order to put the technique that was proposed into action. About 200 different configurations of 256x256 8-bit grayscale test images have been tried in the trials.

4.1. The first image's neighbouring pixels are very closely connected to one another in all three orthogonal directions. A flawless encryption calculation needs to ensure that the construction constants of the pixels in the encoded image have a sufficiently low association to withstand assessable attacks. Only then will the computation be considered perfect.

$$Corr\left(\frac{A}{B}\right) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{i,j}-\hat{A})(B_{i,j}-\hat{B})}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{i,j}-\hat{A})^2}\ \sum_{i=1}^{m}\sum_{j=1}^{n}(B_{i,j}-\hat{B})^2} \quad (4)$$

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

Table 1: Correlation analysis of various Test Images.

	Pareek & Patidar [16]		**Ravichandran & Padhmapriya [18]**		**Proposed Work**	
	plain imageries	**cipher-imageries**	**plain imageries**	**cipher-imageries**	**plain imageries**	**cipher-imageries**
Horizontal Correlation	0.973	-0.0016	0.968	-0.0014	0.986	-0.0002
Vertical Correlation	0.964	0.0072	0.957	-0.0018	0.978	0.0001
Diagonal correlation	0.962	-0.0054	0.958	-0.0015	0.969	-0.0015

4.2. The numeral of bits per second (BPS) and the numeral of pixels changed per second (NPCR) are the two most important characteristics that need to be measured in order to evaluate the robustness of a calculation with regard to differential attacks. It is a common measurement that is used to examine the effect that a change in just one pixel has on the entire image. This will display the rate at which different pixels between the two photographs change. Let the pixel measurements of the original and encoded photos, Io and C, at the ith pixel push and the jth pixel section, respectively, be denoted by the notation Io (i, j) and C(i, j), respectively. The following equation is suggested for use in determining the NPCR:

$$NPCR = \frac{1}{MxN} * \sum_{i,j} D(i,j) * 100\% \quad (5)$$

This can be analysed by comparing two encrypted images, one derived from the average picture and another from the same plain image with a single pixel changed. The NPCR indexes the proportion of evenly-spaced pixels.

4.3. Any modification to the plaintext picture must result in a substantial modification to the encrypted content image. When comparing two images, UACI is helpful for determining the average contrast in pixels.

$$UACI = \frac{1}{MxN} * \sum_{i,j}[\frac{C1(i,j)-C2(i,j)}{225}] * 100\% \quad (6)$$

4.4. Data Entropy Investigation:

Entropy is a degree of the arbitrariness and instability of an image, and it is commonly engaged to calculate the consistency of the brightness distribution across individual pixels. Since an entropy of 8 is the maximum, the most secure image is the one in which the storage area is given a positive incentive of 8.

4.5. Peak to Signal Ratio:

The PSNR (peak signal-to-noise ratio) is defined as the comparison amongst the extreme likely assessment (power) of a standard and the force of ambiguous noise that detracts from its otherwise excellent display. There is a benefit in comparing and ranking the various picture enhancement calculations available. It verifies if the

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

cover photo and its steganogram are compatible. The peak-to-average signal-to-noise ratio (PSNR) is a widely used objective metric for gauging the quality of altered images. It is expressed as a decibel (dB) value.

$$PSNR = 10.log_{10}\frac{Max_i}{\sqrt{MSE}} \quad (7)$$

Table 2: Parameter Comparison with the Existing Methods.

S. No.	Algorithm	Information entropy	NPCR %	UACI %	PSNR dB	Speed Sec
1	Proposed	7.98	99.98	33.54	49.24	0.493
2	Pareek & Patidar [16]	7.83	99.67	33.47	38.27	2.43
3	Ravichandran & Padhmapriya [18]	7.76	99.51	33.24	40.16	2.41

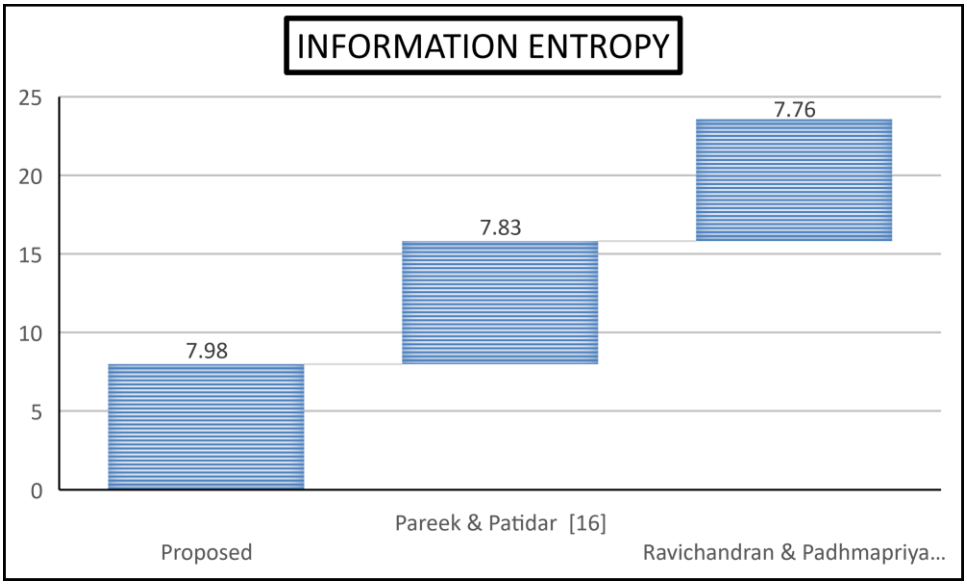

Figure 3: Information Entropy Comparison with the Existing Methods.

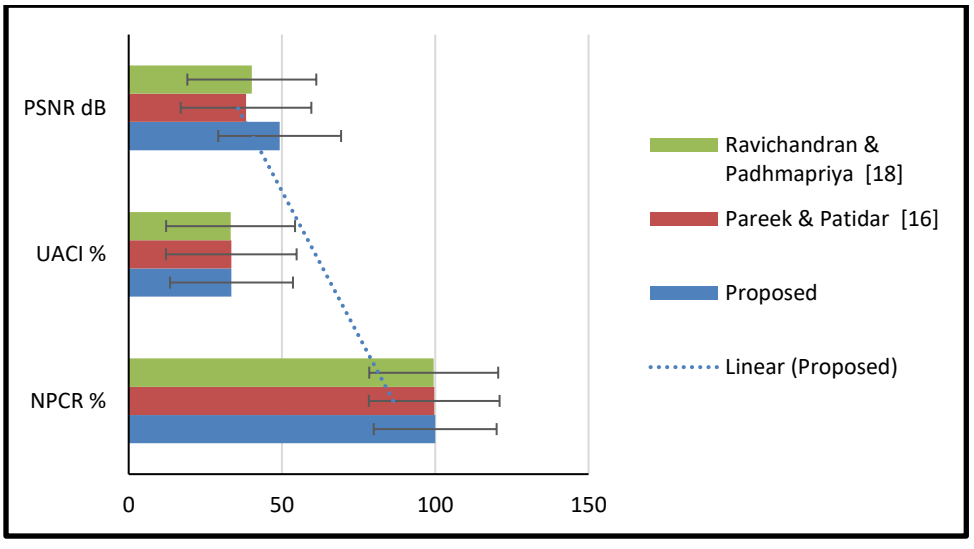

Figure 4: Evaluation parameters comparison with the existing approach.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

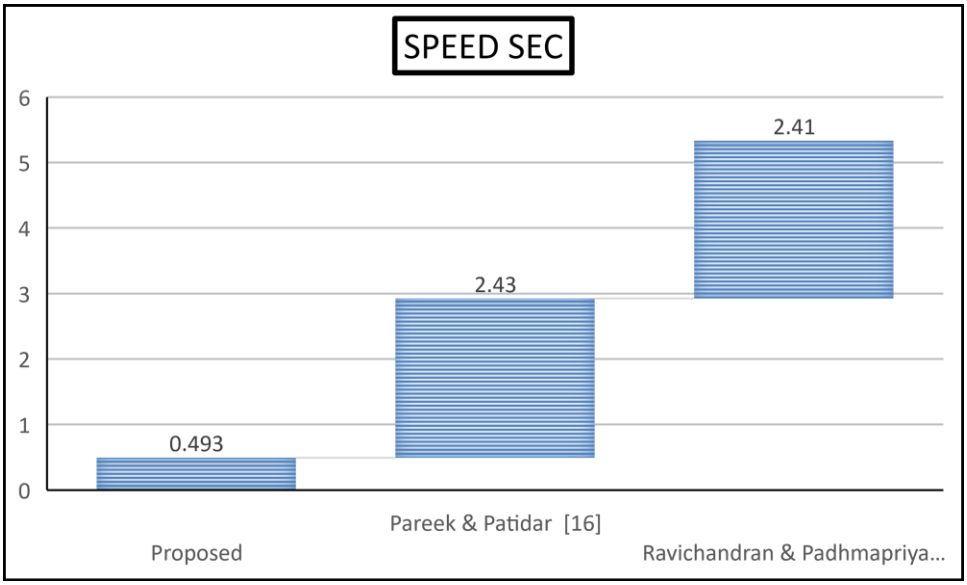

Figure 5: Speed Comparison of the proposed work with the Existing approach.

The table 2 provides a comparison of the proposed cryptosystem with previously developed picture encryption methods that make use of certain execution pointers. This configuration may not have the most available room, but it is large enough to resist an entire assault, making it an excellent choice for important space exploration. The association constants of this cryptosystem are closer to 0 in comparison to the association constants of other encryption strategies, which demonstrates that it is more resistant to accurate occurrences. The data entropy shown here exhibits larger contrast as compared to the works that are referenced in the references (Pareek and Patidar and Ravichandran and Padhmapriya, respectively). As can be shown in Tables 2 and 3, the NPCR and UACI estimates for the proposed cryptosystem are pretty close to the theoretical maximums. This fact demonstrates that the system is resistant to attacks based on either the known plaintext or the chosen plaintext. Because of this, the picture cryptosystem that was proposed is both reasonable and applicable.

An algorithm for encrypting images has been developed, and it makes use of both a genetic operator and a hybrid technique. After degenerating the input images into bit planes, we encrypt them with the arithmetic edge, and then we utilise the multipoint edge operator to swap the bit planes. To begin, we encrypt the input images with the arithmetic edge. A hybrid mutation is performed, after which the key stream of a three-dimensional Sine and ICMIC hybrid map is utilised. The application of the compound mutation process results in the production of an encrypted image. The calculation that was suggested guarantees complete encryption execution, and it just takes one round. The feasibility of the proposed picture cryptosystem, which offers high levels of both safety and convenience when it comes to its deployment has been proven by both the theoretical investigation and the imitation of its results. All of this indicates to the fact that the strategy that has been offered is not only successful but also meets the requirements that have been set out by the researchers.

5. Conclusion and Future Scope

The process of using encryption to create a new, secret image is known as image encryption. This picture makes little sense because its details are difficult to obtain. The majority of today's multimedia files are distributed online. Data assurance is essential for solicitations alike satellite image communication, medical image distribution, and statement picture preservation. This research study elaborates on the next generation of image encryption, which is based on a hybrid approach and makes use of a Genetic operator. A large number of edge and mutation strategies were proposed in the aforementioned Genetic operator based Image encryption algorithm literature. Because maximal pixel correlation (shuffling ratio) could not be attained with those methods, security was poorly managed, computation time was excessive, and execution speed was slow. In the recommended genetic operator-based hybrid approach to image encryption, the idea images are primary encoded using mathematics edge, then deteriorated into bit air plane, and then exchanged by means of a multipoint edge operative. The key stream of a three-dimensional Sine and ICMIC hybrid map is then used in a hybrid mutation. The suggested calculation guarantees high-quality encryption in a single pass. The replication and theoretic analysis demonstrate that the projected depiction cryptosystem is both easy to implement and highly secure, making it resistant to attacks of any kind.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

Despite this, there is still a great deal of room for improvement in this domain. The mechanism of diffusion might become muddled. Various analytical equations model a wide variety of diffusion phenomena. In this context, we want to investigate whether or not these models can be used to predict how cryptographic techniques will spread. In addition, it can use fractional calculus to develop fractional diffusion equations and explore how well they model the diffusion process when applied to cryptography.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1]. Chen, C, Liu, J, Wen, Y & Dong, Z 2015, 'A hybrid genetic algorithm for privacy and cost aware scheduling of data intensive work flow in cloud', Springer, International Conference on Algorithms and Architectures for Parallel Processing, vol. 25, no. 1, pp. 578-591.

[2]. Chen, TY, Hwang, MS & Jan, JK 2013, 'A secure image authentication scheme for tamper detection and recovery', Imaging Science Journal, vol. 60, no. 4, pp. 219-233.

[3]. Congyang Chen, Jianxun Liu, Yiping Wen & Dong Zhou 2015, 'A Hybrid Genetic Algorithm for Privacy and Cost Aware Scheduling of Data Intensive Work flow in Cloud', Springer, vol. 9528, no. 1, pp. 578-591.

[4]. Das, S, Mandal, SN & Ghoshal, N 2014, 'Diffusion and encryption of digital image using genetic algorithm', Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing Theory and Applications (FICTA), vol. 12, no. 2, pp. 729-736.

[5]. Devaraj, P & Kavitha, C 2016, 'An image encryption scheme using dynamic S-boxes', Springer Science+Business Media Dordrecht, vol. 86, no. 2, pp. 927 - 940.

[6]. Dhivya Ravichandran & Padmapriya Praveenkumar 2016, 'Chaos Based Edge and Mutation for Securing DICOM Image', Computers in Biology and Medicine, vol. 72, no. 1, pp. 170 - 184.

[7]. Gaurav Bhatnagar, QM & Jonathan Wu 2012, 'Selective image encryption based on pixels of interest and singular value decomposition', Digital Signal Processing, vol. 22, no. 4, pp. 648-663.

[8]. Guesmi, R, Farah, MAB, Kachouri, A & Samet, M 2016, 'Hash keybased image encryption using edge operator and chaos', Multimedia Tools and Applications, vol. 75, no. 2, pp. 4753 - 4769.

[9]. Guodong Ye 2010, 'Image scrambling encryption algorithm of pixel bit based on chaos map', Pattern Recognition Letter, vol. 31, no. 5, pp. 347-354.

[10]. Huang, X & Ye, G 2014, 'An image encryption algorithm based on hyper-chaos and DNA sequence', Multimedia Tools and Applications, vol. 72, no. 1, pp. 57–70.

[11]. Huijuan Li, Yurong Wang , Haitao Yan, Liben Li, Quize Li & Xiaoyan Zhao 2013, 'Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform', Optics and Lasers in Engineering, vol. 51, no. 12, pp. 1327-1331.

[12]. Majid Khan & Tariq Shah 2014, 'A novel image encryption technique based on Henon chaotic map and S8 symmetric group', Neural Computing & Applications, vol.70, no. 8, pp. 1717-1722.

[13]. Manish Kumar & Sunil Kumar 2016, 'Intertwining Logistic Map and Cellular Automata Based Color Image Encryption Model', International Conference on Computational Techniques in Information and Communication Technologies, vol. 10, pp. 58-67.

[14]. Mohammad Ali Bani Younes & Aman Jantan 2008, 'Image Encryption Using Block-Based Transformation Algorithm', IAENG International Journal of Computer Science, vol. 35, no.1, pp. 35 - 46.

[15]. Muhammad Rafiq Abuturab 2017, 'Multiple color-image fusion and watermarking based on optical interference and wavelet transform', Optics and Lasers in Engineering, vol. 89, no. 1, pp. 47-58.

[16]. Pareek, NK & Patidar, V 2016, 'Medical image protection using genetic algorithm', Soft Computing, vol. 20, no. 2, pp. 763–772.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021

[17]. Ramzi Guesmi, Mohamed Amine Ben Farah & Abdennaceur Kachouri 2015, 'Hash key-based image encryption using edge operator and chaos', Springer, vol. 75, no. 8, pp. 4753-4769.

[18]. Roy V., Shukla S. (2013) Image Denoising by Data Adaptive and Non-Data Adaptive Transform Domain Denoising Method Using EEG Signal. In: Kumar V., Bhatele M. (eds) Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE 2012). Lecture Notes in Bioengineering. Springer, India. https://doi.org/10.1007/978-81-322-0970-6_2.

[19]. Subhajit Das, Satyendra Nath Mandal & Nabin Ghoshal 2014, 'Diffusion and Encryption of Digital Image Using Genetic Algorithm', Advances in intelligent computing-Springer, vol. 327, no. 1, pp. 729-736.

[20]. Tang, Z 2016, 'Multiple- image encryption with bit-plane decomposition and chaotic maps', Optics and Lasers in Engineering, vol. 80, no. 2, pp. 1-11.

[21]. Tao Xiang, Jia Hu & Jianglin Sun 2015, 'Outsourcing chaotic selective image encryption to the cloud with steganography', Digital Signal Processing, vol. 43, no. 4, pp. 28-37.

[22]. Xiang, T, Qu, J, Yu, C & Fu, X 2012, 'Degradative encryption: An efficient way to protect SPIHT compressed images', Optics Communication, Elsevier, vol. 285, no. 24, pp. 4891-4900.

[23]. Xingyuan Wang & Hui-li Zhang 2015, 'A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems', Springer, vol. 83, no. 2, pp. 333-346.

[24]. Xu, L & Li, Z 2016, 'A novel bit level image encryption algorithm based on chaotic maps', Optics and Lasers in Engineering, vol. 78, no.1, pp. 17-25.

[25]. Xuancai Zhao, Qiuzhen Lin , Jianyong Chen, Jianping Yu & Zhong Ming 2016, 'Optimizing security and quality of service in a Real-time database system using Multi-objective genetic algorithm', Elsevier , vol. 64, no. 1, pp. 11-23.

[26]. V. Roy and S. Shukla, "Mth Order FIR Filtering for EEG Denoising Using Adaptive Recursive Least Squares Algorithm," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), 2015, pp. 401-404, doi: 10.1109/CICN.2015.85.

[27]. Yadav, AK, Mehta, R, Kumar, R & Vishwakarma, VP 2016, 'Lagrangian twin support vector regression and genetic algorithm based robust grayscale image watermarking', Multimedia Tools and Applications, vol. 75, no. 15, pp. 9371-9394.

[28]. Yanbin Li, Feng Zhang & Yuan 2015, 'Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform' Optics and Lasers in Engineering, vol. 72, no. 1, pp. 18-25.

[29]. Ahmad, M.; Haleem, H.; Khan, P.M. A new chaotic substitution box design for block ciphers. In Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 20–21 February 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 255–258.

DOI: https://doi.org/10.54216/JCIM.080105
Received: May 19, 2021 Accepted: September 25, 2021