IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Image Encryption Using Chaotic Maps

Siddharth Kumar[1], Sumeet Sah[1], Shivanshu Mall[1], Ritik Tyagi[1], Mr Prem Prakash[2*]

1. Under-graduate Students, Computer Science Engineering Department, GNIOT, Greater Noida, India
2. Assistant Professor, Computer Science Engineering Department, GNIOT, Greater Noida, India

Abstract:-

Image encryption is a crucial aspect of data security, which involves the transformation of an image into an unreadable form, making it inaccessible to unauthorized parties. Chaotic maps have been increasingly used as a means of encryption due to their inherent properties of unpredictability and sensitivity to initial conditions. This paper proposes a novel image encryption scheme based on chaotic maps, which employs a chaotic logistic map. The scheme utilizes a key matrix generated by the two chaotic maps to perform a substitution-permutation network on the input image, ensuring a high degree of security. The proposed scheme is evaluated using various statistical tests and is found to be robust against attacks such as brute force, differential, and statistical attacks. Furthermore, the scheme demonstrates good performance in terms of encryption speed and is suitable for real-time image encryption applications. The results of the study suggest that the proposed scheme can be an effective solution for image encryption in various practical applications.

1. Introduction

Image encryption is an essential technique for protecting sensitive data from unauthorized access, especially in the digital era where images are widely shared and stored in various media. Various encryption techniques have been proposed for securing images, including symmetric and asymmetric encryption, steganography, and watermarking. However, most of these methods suffer from security vulnerabilities and computational complexity, making them unsuitable for practical applications.

Chaotic maps have been recognized as a promising method for image encryption due to their inherent properties of unpredictability, sensitivity to initial conditions, and pseudo-randomness. Chaotic maps generate a sequence of seemingly random numbers that can be used as encryption keys. The encryption process based on chaotic maps typically involves two phases: a substitution phase and a permutation phase. In the substitution phase, the pixels of the image are replaced with pseudo-random numbers generated by the chaotic map. In the permutation phase, the positions of the pixels are shuffled to increase the randomness of the cipher image.

In this paper, we propose a novel image encryption scheme using chaotic maps that employs a combination of the chaotic logistic map. The proposed scheme utilizes a key matrix generated by the two chaotic maps to perform a substitution-permutation network on the input image. The substitution-permutation network involves a series of bitwise operations, such as XOR and modulo, to scramble the pixel values and their positions. The resulting cipher image is highly resistant to various attacks, such as brute force, statistical, and differential attacks.

2. Related Works

This section provides an overview of the latest published chaos-based image encryption techniques. Several image encryption algorithms have been proposed, varying in efficiency and robustness. The theoretical overview and analysis of the above algorithms are discussed and evaluated based on various performance metrics such as Number of Pixel Changes (NPCR), Uniform Average Change Intensity (UACI), Key Analysis (KA), Histogram Analysis (HA), Correlation Coefficients (CC), information entropy (IE), noise attack (NA). A literature review of the latest articles is presented as follows: A review of ten conventional and five chaos-based image encryption techniques was recently presented. The comparison made was based on various evaluation metrics such as statistical, differential and quantitative attack analysis. In order to evaluate their effectiveness, experiments were performed on MATLAB-2015. The results showed the resilience of chaotic schemes against statistical attacks. The encrypted images were highly encoded with a consistent histogram distribution and lower correlation coefficient values in all three directions

(horizontal, vertical and diagonal). Similarly, chaotic schemes were resistant to differential attacks due to their high sensitivity to pixel and key change values. All techniques exhibited significantly large key space and high information entropy values, thereby providing resistance to brute force attacks. However, conventional schemes were shown to be less robust against difference attacks because they showed poor sensitivity to pixel change. Furthermore, they concluded that image encryption using chaotic scheme 15, RC4, and AES proved to be computationally efficient and had faster execution time compared to other considered encryption algorithms. In another study, digital image encryption and decryption schemes are discussed. These schemes use multiple chaotic map methods to improve existing algorithms providing a high level of image data security. Key size sensitivity, key space, computation time, and correlation coefficient are used to verify the protection of snapshots. However, the techniques and methods considered by the authors are somewhat outdated, and the results of the work are not based on the analysis of the latest methodologies. Monjul Saika et al. published a brief review of map-based chaotic image encryption in the spatial domain. The authors stated that chaos-based image encryption is most suitable for encryption processes due to its high sensitivity to initial conditions. Furthermore, a general overview of chaotic maps and the three different phases (choosing chaotic maps, swapping, and spreading images) that ensure system security by providing protection to digital data against unauthorized access were discussed and exemplified. . The disadvantage of this paper is that the authors did not discuss or review any research papers in the spatial domain and limited themselves to basic chaotic maps and phases. The authors attempt to explore image encryption and steganography. The research papers studied in this paper include various image encryption and steganography techniques used to ensure data integrity and security. Encryption techniques have been used to convert the input image into an encrypted image, while shorthand techniques have been used to improve the security of the system. In this way, the encryption key is kept hidden in the cipher image without changing or modifying the information in it. This reduces the key transfer time between the sender, receiver and third party distributor. In addition, the cost of key distribution is also minimized. An extensive analysis of several image encryption methods has been published. This paper describes four image encryption techniques, namely spatial, compressive sensing, optical, and transform domain. The paper also made a broad comparison of these techniques based on various performance metrics such as UACI, histogram analysis, key analysis, NPCR, noise, correlation coefficients, information entropy, and encryption speed. The paper mainly focused on the challenges associated with digital image encryption techniques, such as computational time, security risks, and debugging parameters. In addition, the author discussed considerable achievements using metaheurism-based image encryption schemes to overcome the above problems. According to research, these meta-heuristic techniques suffer from premature convergence, getting stuck in a local optimum, and slow convergence speed. The paper concludes that there is significantly more work to be done on image encryption based on metaheuristic methods and various imaging systems such as underwater, remote sensing, multispectral imaging, and 3D imaging systems. The authors analyzed some traditional and modern hybrid encryption techniques with post-quantum methods, such as DES–RSA, 3D Chaotic Map techniques, Singular Cubic Curve RSA, ECC-based RSA with AVK, Joint Compression and Encryption (JCE). These encryption techniques and algorithms were compared based on various performance metrics such as execution time, bit sizes, key length, possible keys, and security level. The comparison made in this paper showed that the combination of RSA-based singular cubic curve with AVK reduced the time consumption to a minimum level and provided the system with high functionality in terms of security. However, with double encryption, this technique appeared to be suitable only for small content. Similarly, a mixture of AES-ECC hybrid techniques showed a reduction in both space and time complexity compared to other algorithms. A hybrid approach has proven to be able to provide greater security. On the other hand, quantum encryption performed better in terms of key distribution, also requiring less resources. Experiments concluded that Blowfish outperformed other algorithms (DES, IDEA, and AES) in the analysis presented in this paper, and that compared to other current compression techniques, it performed much better in encryption execution time performance. Younes et al. presented a general introduction to image encryption and cryptography along with a brief overview of the latest image encryption techniques that provide security for confidential data. These image encryption techniques show considerable protection of sensitive information. Thus, these techniques can be further refined and new techniques developed to reduce the risk of data security and integrity.

In another survey, the authors drew attention to the problem of the co-evolution of security risks of digital images with the development of technology. The authors also discussed and analyzed ten papers dealing with image encryption techniques to promote further improvement of the performance of these encryption methods and make them highly resistant to security attacks. The methods discussed above use different combinational approaches to reduce security risks by embedding and encrypting the original image and sending it to the receiver. However, this approach still lags behind due to the slower transmission time from sender to receiver. Moreover, compression and segmentation techniques could not solve this problem because compression techniques were not erasable or reversible, while segmentation techniques take much longer to transfer large data. Based on the review of the techniques presented in the paper, the author concluded that chaos-based encryption techniques are more secure and simpler

due to the low consumption in the process of encrypting and decrypting a large image.

Various image encryption techniques have been reviewed and analyzed in the context of parameters used to demonstrate the effectiveness of security algorithms. Various aspects of image security in general and encryption in particular are discussed. Bhat et al. presented a general overview of image security in multimedia data and reviewed various image encryption techniques in the context of security parameters to verify the effectiveness of these algorithms to ensure image privacy and integrity. An analysis of encryption techniques showed that image encryption differs from other multimedia encryption due to the large data capacity and strong correlation between pixels, which makes conventional encryption schemes unsuitable. Therefore, before design, any image encryption algorithm must be analyzed with respect to security constraints to ensure the trustworthiness of the algorithms.

3. Proposed Method

3.1 Logistic Maps:

The logistic map equation is given by:

$$Xn+1 = r*Xn*(1 - Xn)$$

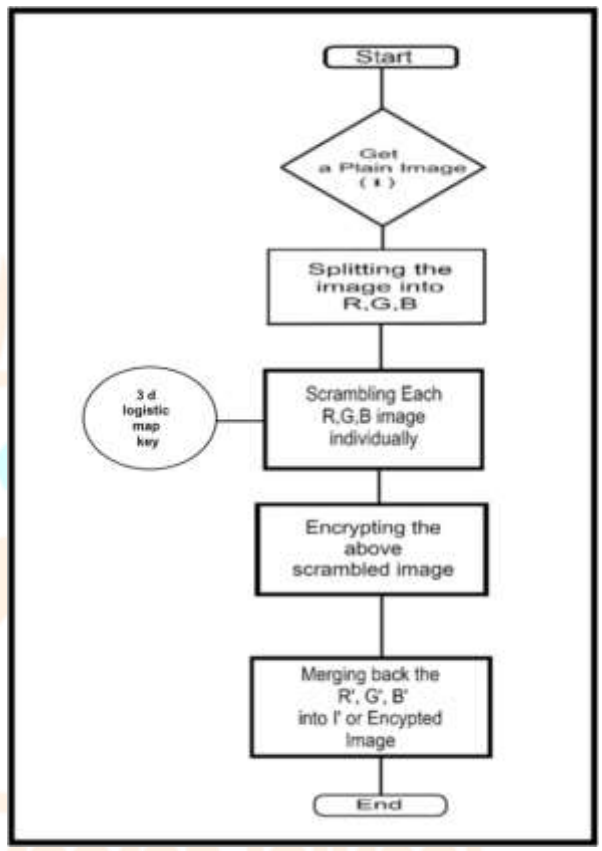
where Xn is the value of the system at time n, Xn+1 is the value at time n+1, and r is a constant parameter that controls the behavior of the system. The logistic map exhibits a range of complex and chaotic behavior for different values of r.

But, In this project we have used the 3d logistic map which instead of updating Xn alone we have two more Yn, and Zn represent the values of the system at time n, and a, b, c, and d are parameters that determine the behavior of the system. The 3D logistic map exhibits a range of chaotic behavior, including bifurcations, attractors, and strange attractors, depending on the parameter values.

3D logistic maps are often used in image encryption schemes based on chaotic maps, as they exhibit sensitivity to initial conditions and are pseudo-random. The chaotic behavior of these maps makes it difficult for an attacker to reconstruct the original image from the encrypted one.

3.2 Encryption:

1. Initialization:
The 3D logistic map parameters (a, b, c) and initial values (X, Y, Z) are set. which is needed to generate the 3d logistic key.
2. Pre-processing:
The input image is split into R, G, and B image.
3. Scrambling:
In this phase each and every pixels value is changed which add one more level of security into our encryption system.
4. Key generation:
In this phase we generate a secret three dimensional key than this key is used to encrypt the input images.
5. Output:
Output the encrypted image, which can be transmitted securely.

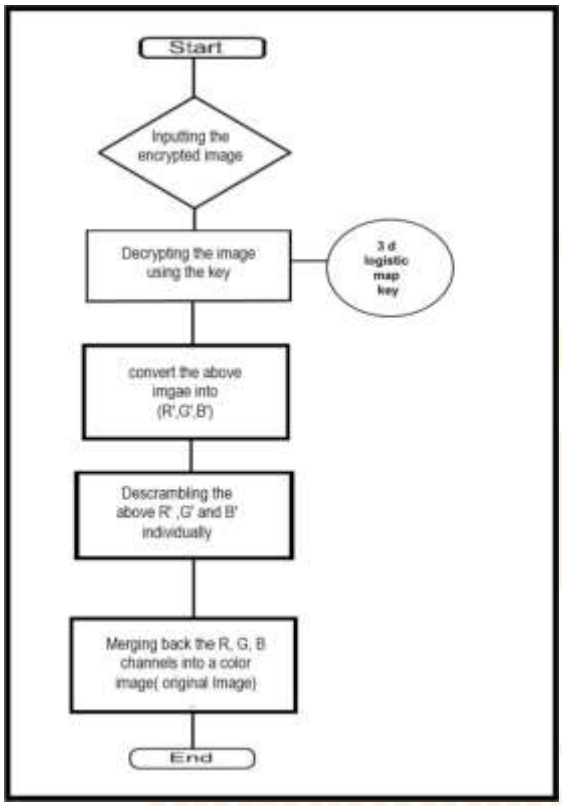


3.3 Decryption:

1. Initialization:
Choose initial values for the chaotic maps used in the decryption process.
2. Key generation:
In this phase the key is provided by the sender that is generated during the encryption process which will be used as the secret key for decryption.
3. Descrambling:
Apply the Inverse diffusion process to the encrypted image to recover the scrambled 3D images.
4. Decryption:
In this phase the sender's key is used to decrypt the image into plain image.

5. Output:
Output the decrypted image, which should be identical to the original 3D image.

This algorithm has been found to be robust against various attacks, including statistical, differential, and brute-force attacks. It also exhibits good performance in terms of encryption speed and security. However, the algorithm requires careful selection of the 3D logistic map parameters to ensure the security of the encrypted image.



Here are the some of the images that we have encrypted and decrypted by using above encryption and decryption algorithm.

I. Encryption and Decryption on Grayscale image

we have taken a grayscale image “lena.bmp” that has the size of 256*256 pixel shown in fig-1.

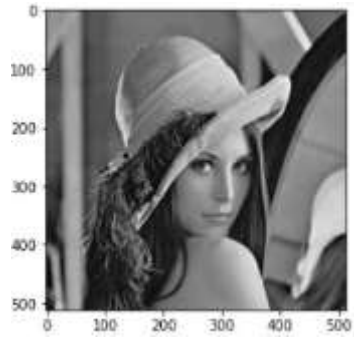


Fig-1 Original Image

Than it is used as input image and encrypted using the above algorithm and 3d Logistic key and a ciphered image is generated as shown in fig-2.

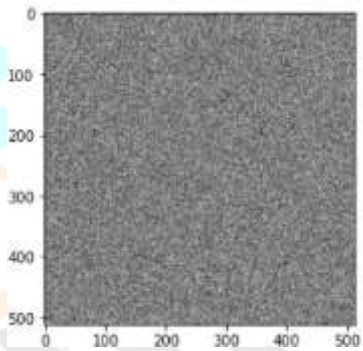


Fig-2 Encrypted Image

Now the above encrypted image is decrypt using the decryption algorithm the resultant image is generated that is shown in fig-3.

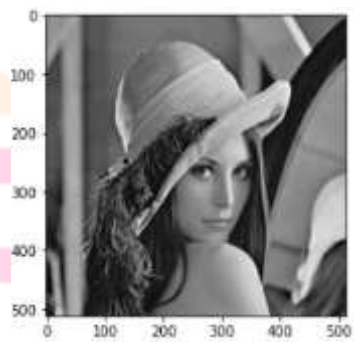


Fig-3 Decrypted Image

II. Encryption and Decryption on color image

We have tried the same algorithm to a color image "city.jpg" that has the size of 256*256 pixel shown in fig-4.

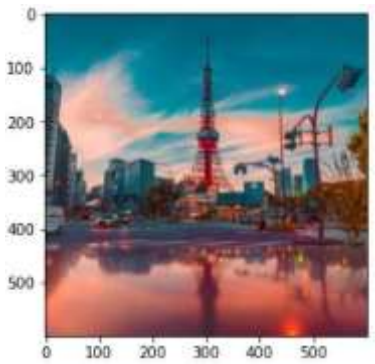


Fig-4 Original Image

Than it is used as input image and encrypted using the above algorithm and 3d Logistic key and a ciphered image is generated as shown in fig-2.

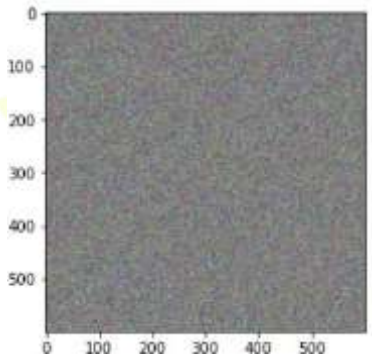


Fig-5 Encrypted Image

Now the above encrypted image is decrypt using the decryption algorithm the resultant image is generated that is shown in fig-3.

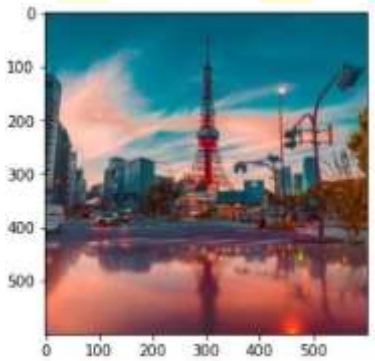


Fig-6 Decrypted Image

4. Security Analysis

In this section We have shown the robustness and encryption quality of our algorithm using the following analysis.

I. Histogram Analysis

The image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. Since a good image encryption method tends to encrypt a plaintext image to random-like, it is desired to see a uniformly-distributed histogram for an encrypted image.

The fig-7 shows the histogram of original image with R, G, and B as parameters which shows the random distribution of R, G, and B planes.

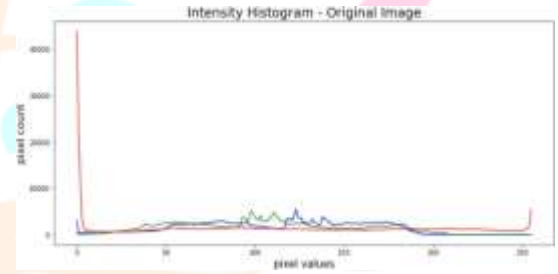


Fig-7 Histogram of Original Image

The fig-8 shows the uniformly-distributed histogram in the case of an encrypted image which shows that each R,G, and B pixel are distributed equally.

Fig-8 Histogram of Encrypted Image

II. Adjacent Pixel Auto-Correlation

Adjacent pixels correlation coefficient (APCC), another common measure used in the assessment of the security level for newly designed image encryption algorithms, is based on the well-known fact that, generally in plain-images, any arbitrarily chosen pixel is strongly correlated with its adjacent pixels

In the digital images the amount of redundant information is very high, a fact which translates in strong correlation of adjacent pixels within. In contrast, image encryption schemes should greatly reduce these correlations, as closely possible, to a zero value. If one plots the correlation distributions for the plain and encrypted images will notice that the set of adjacent pixels are concentrated along the main diagonal, in the case of plain image as shown in the fig-9 below.

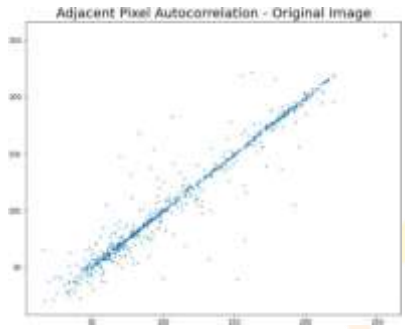


Fig-9 APCC of Original Image

In the case of the encrypted images, same sets of adjacent pixels are well scattered which is shown in the fig-10 below.

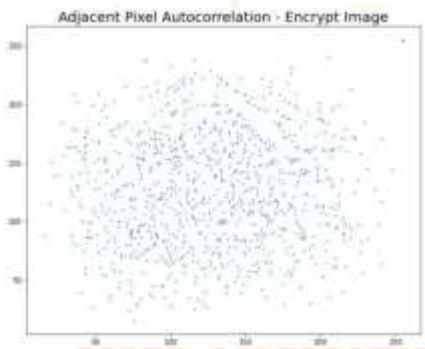


Fig-10 APCC of Encrypted Image

Conclusions

Image encryption using chaotic maps is a popular method for securing digital images. Chaotic maps provide a pseudo-random sequence of keys that can be used for encrypting the input image. The encryption process involves dividing the input image into blocks, generating keys using the chaotic map, and then applying XOR and permutation operations to the image blocks.

Several algorithms have been proposed for image encryption using chaotic maps, including the 3D logistic map image encryption algorithm. These algorithms have been found to be robust against various attacks, including statistical, differential, and brute-force attacks. However, it is important to carefully select the parameters of the chaotic map to ensure the security of the encrypted image.

In conclusion, image encryption using chaotic maps is an effective method for securing digital images. It provides robust encryption against different types of attacks and can be further strengthened by incorporating additional security measures. As the use of digital images continues to grow, the need for secure image encryption methods becomes increasingly important.

References

- Alpar O (2014) Analysis of a new simple one dimensional chaotic map. Nonlinear Dyn 78(2):771–778 Brindha M, Ammasai Gounden N (2016)
- A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem. Appl Soft Comput J 40:379–390 Cao C, Sun K, Liu W (2018)
- A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. Sig Process 143:122–133 Chai X (2017)
- An image encryption algorithm based on bit level Brownian motion and new chaotic systems. Multimed Tools Appl 76(1):1159–1175 Coppersmith D (1994)
- The data encryption standard (DES) and its strengths against attacks. IBM J Res Dev 38(3):243–250 Diaconu AV (2016)
- Circular inter–intra pixels bit-level permutation and chaos-based image encryption. Inf Sci 355:314–327 El-latif AAA, Li L, Zhang T, Wang N, Song X, Niu X (2012)
- Digital image encryption scheme based on multiple chaotic systems. Sens Imaging 13:67–88 Floating-point Working Group (1985) IEEE standard for binary floating-point arithmetic.

  ANSI. IEEE Std., pp 754–1985 Fu C, Lin B, Miao Y et al (2011)
- A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun 284:5415–5423 Gao T, Chen Z (2008)
- A new image encryption algorithm based on hyper-chaos. Phys Lett A 372(4):394–400 Gao H, Zhang Y, Liang S, Li D (2006a)
- A new chaotic algorithm for image encryption. Chaos Solitons Fractals 29(2):393–399 Gao T, Chen Z, Yuan Z, Chen G (2006b)

- A hyperchaos generated from chen's system. Int J Mod Phy C 17(4):471–478 Guesmi R, Farah MAB, Kachouri A, Samet M (2016)
- A novel chaosbased image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dyn 83(3):1123–1136 Gupta A, Thawait R, Patro KAK, Acharya B (2016)
- A novel image encryption based on bit-shuffled improved tent map. Int J Control Theory Appl 9(34):1–16 Huang CK, Nien HH (2009)
- Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 282(11):2123–2127 Kadir A, Hamdulla A, Guo WQ (2014)
- Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Opt Int J Light Elect Opt 125(5):1671–1675 Kulsoom A, Xiao D, Aqeel-ur-Rehman Abbas SA (2016)
- An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. Multimed Tools Appl 75(1):1–23 Lan R, He J, Wang S, Gu T, Luo X (2018)
- Integrated chaotic systems for image encryption. Sig Process 147:133–145 Li S, Chen G, Mou X (2005)
- On the dynamical degradation of digital piecewise linear chaotic maps. Int J Bifurc Chaos 15(10):3119–3151 Li Y, Wang C, Chen H (2017)
- A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Laser Eng 90:238–246 Liao X, Hahsmi MA, Haider R (2018)
- An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Opt Int J Light Electron Opt 153:117–134 Liu W, Sun K, Zhu C (2016)
- A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36 Mohanty S, Shende A, Patro KAK, Acharya B (2017)
- A DNA based chaotic image fusion encryption scheme using LEA-256 and SHA-256. Indian J Sci Res 14(2):190–201 Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR (2014)
- A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71(3):1469–1497 Patro KAK, Acharya B (2018)
- Novel data encryption scheme using DNA computing. Adv DNA Comput Cryptogr Patro KAK, Acharya B (2018b) Secure multi–level permutation operation based multiple colour image encryption. J Inf Secur Appl 40:111–133 Patro KAK, Acharya B, Nath V (2018)
- secure multi-stage oneround bit-plane permutation operation based chaotic image encryption. Microsyst Technol 1–8 Patro KAK, Banerjee A, Acharya B (2019)
- A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1-D chaotic maps. In: Proc Int Conf Next Gen Comput Technol. Springer, Singapore, pp 396–418 Pub NF. 197 (2001)
- Advanced encryption standard (AES). Fed Inf Process Standards Publ 197:441-0311 Samhita P, Prasad P, Patro KAK, Acharya B (2016)
- A secure chaosbased image encryption and decryption using crossover and mutation operator. Int J Control Theory Appl 9(34):17–28 Shadangi V, Choudhary SK, Patro KAK, Acharya B (2017)
- Novel arnold scrambling based CBC-AES image encryption. Int J Control Theory Appl 10(15):93–105 Sravanthi D, Patro KAK, Acharya B, Majumder S (2019)
- A secure chaotic image encryption based on bit-plane operation. In: Proc. Soft Comput. Data Analyt. Springer, Singapore, pp 717–726 Wang X, Guo K (2014)
- A new image alternate encryption algorithm based on chaotic map. Nonlinear Dyn 76(4):1943–1950 Wang X-Y, Yang L (2012)
- Design of pseudo-random bit generator based on chaotic maps. Int J Mod Phys B 26(32):1250208 Wang Y, Wong KW, Liao X, Chen G (2011)
- A new chaos-based fast image encryption algorithm. Appl Soft Comput 11(1):514–522 Wang X, Wang S, Zhang Y, Guo K (2017)
- A novel image encryption algorithm based on chaotic shuffling method. Inf Secur J A Glob Perspect 26(1):7–16 Wu X, Kurths J, Kan H (2017)
- A robust and lossless DNA encryption scheme for color images. Multimed Tools Appl Xu L, Li Z, Li J, Hua W (2016)
- A novel bit-level image encryption algorithm based on chaotic maps. Opt Laser Eng 78:17–25 Zhang Y-Q, Wang X-Y (2014)