IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 12, December 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

Medical Image Encryption & Decryption using Chaos-based Technique

Swathi B S[1], Prasanthamurthy H G[2], Pavtra S R[3]

Senior Grade Lecturer, Department of Electronics and Communication, Govt. Polytechnic, Belur, DCTE, Karnataka, India[1]

Senior Grade Lecturer, Department of Electronics and Communication Engineering, Govt. Polytechnic, Holenarasipura, DCTE, Karnataka, India[2]

Senior Grade Lecturer, Department of Electronics and Communication Engineering, Govt. Polytechnic, Holenarasipura, DCTE, Karnataka, India[3]

ABSTRACT: Medical images possess significant importance in diagnostics when it comes to healthcare systems. These images contain confidential and sensitive information such as patients' X-rays, ultrasounds, computed tomography scans, brain images, and magnetic resonance imaging. However, the low security of communication channels and the loopholes in storage systems of hospitals or medical centres put these images at risk of being accessed by unauthorized users who illegally exploit them for non diagnostic purposes. In addition to improving the security of communication channels and storage systems, image encryption is a popular strategy adopted to ensure the safety of medical images against unauthorized access. In this work, we propose a cryptosystem based on Henon chaotic map to encrypt medical images with elevated security. The efficiency of the proposed system is proved in terms of histogram analysis, adjacent pixels correlation analysis and time complexity. The experimental results show that the proposed cryptosystem is a lightweight approach that can achieve the desired security level for encrypting confidential image-based patients' information.

KEY WORDS: IoHS, AES, DES

I. INTRODUCTION

In the era of exponential growth of communications technologies, security of data, in particular medical data, is of great interest. Cloud-based Internet-of-health systems (IoHS) are being increasingly used to store patient's data to make them remotely accessible at different facilities/locations. The stored and transferred data include sensitive identifiable information (e.g., names, address and the other health records) in addition to medical scans (i.e., medical images and physician reports). Non-authorized access to such data is catastrophic and thus, the security of patient data is of immense importance. Storage and transfer of medical images not only requires secrecy, but also legitimacy and integrity as prerequisites. Fortunately, cryptography algorithms can be exploited to ensure the required security prerequisites, by medical image scrambling to fulfil encryption.Validness and uprightness of a given cryptosystem are eventually assessed using various computerised marks.Early image encryption methods are primarily based on off-the-shelf data encryption technologies e.g., data encryption standard (DES), advanced encryption standard (AES), etc. However, those approaches are shown to be low in efficiency and anti-attack capabilities. To increase encryption efficacy, other advanced methods have been introduced in literature. Examples of the developed and utilized methods include the one-time keys methods, bit-level permutation techniques, and deoxyribonucleic acid (DNA) rule-based schemes. Recent advanced schemes utilized novel theories, such as chaotic maps, and quantum maps and harmonics. More specifically, encryption methods based on chaos theory have attracted researcher attentions due to their inherent advantages over conventional non-chaotic counterpart. Particularly, they are quicker, easierto enforce, and have greater key space, i.e., have wide variety of encryption values. Additional attractive characteristics include initial value-dependency, unpredictability, pseudo randomness, and ergodicity. Those characteristics make chaotic systems more desirable as they have great encryption potentials similar to ideal cryptosystems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

II. LITERATURE REVIEW

In the following section the literature related to proposed work is presented in the table 1.

Table 1: Literature review

SL.No	AUTHORS	TITLE AND YEAR OF PUBLICATION	OBSERVATION
1	Vinod Patidar & Gurpreet Kaur [1]	A Novel Conservative Chaos Driven Dynamic Image Encryption,2023	Key Generation : Pseudorandom sequenceusing chaotic map Encryption method: Dynamic DNA coding algorithm Entropy : 7.9956 Correlation-H : 0.0003 V : -0.0083 D : 0.0007 Encrypt Time : 1.242 s
2	Dhakshin Moorthy Vignesh & Santo Banerjee [2]	A Novel ractional Sine Chaotic Map And Its Application To Image Encryption And Watermarking And Hyperchaptic System ,2023	Key Generation : Sine chaotic map Encryption method: Sine chaoticmap with fractional-difference operator Entropy :7.9977 Correlation-H :-0.0043 V :-0.0103 D :-0.0004
3	Sourab Kumar, Jaishree Jain [3]	Improved Security Of E-healthcare Image Using Hyper driven Robust Zero & Hyperchaotic System,2022.	Key Generation : Hyperchaotic map Encryption method: Hyperchaotic map with gray code conversion technique Entropy : 1.44 Correlation-H : 0.0045 V : 0.0056 D: 0.0034
4	Syed Saqlain & Zeshan Iqbal [4]	Henon Chaotic Map Based Image Encryption Scheme Using Bit-level Circular Shift,2022	Key Generation : Key generated from Henon map Encryption method: Bit level circular shift Entropy : 7.9717 Correlation-H : -0.0125 V : 0.0649 D : -0.03 Key Space : 10^70
5	Xiuli Chai & Xiaoyu Zheng [5]	An Image Encryption Algorithm Based On Chaotic System And Compressive Sensing,2018	Key Generation : Key generated from chaotic map Encryption method: DWT operation Entropy : 7.9992 Encrypt Time : 0.58
6	Yousef Alghamdi & Arslan Munir [6]	A Lightweight Image Encryption Algorithm Based On Chaotic Map And Random Substitution,2022	Key Generation : Key generated from logistic map Encryption method: XOR & AES

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

			operation Entropy : 7.9997 Correlation-H : -0.0001 V : 0.0006 D : -0.0021 Encrypt Time : 0.63
7	M.Essaid& A.Saaidi [7]	A new image encryption scheme Basedon confusion-diffusion using an enhanced skew tent map,2021	Key Generation : Key generated from new chaotic map Encryption method: Bitwise XOR operation Entropy : 7.9990 Correlation-H : 0.0035 V : 0.0037 D : -0.0095 Encrypt Time : 1.5 s

III. SUMMARY OF LITERATURE REVIEW

Based on the literature review conducted we came to the conclusion that, chaos-based image encryption techniques leverage chaotic systems to enhance security in image encryption. These methods typically involve chaotic maps or systems to generate encryption keys, which are then applied to images for encryption. The main advantages include high sensitivity to initial conditions, which improves security, and the ability to achieve complex transformations with relatively simple algorithms. However, challenges remain in achieving a balance between security and efficiency, as well as ensuring robustness against attacks such as cryptanalysis.

Chaos-based image encryption utilises chaotic systems to enhance security. By employing chaotic maps or systems, encryption keys are generated and applied to images for encryption. Advantages include heightened sensitivity to initial conditions, improving security, and the ability to achieve complex transformations with simple algorithms. However, challenges persist in balancing security and efficiency, as well as ensuring robustness against attacks like cryptanalysis and noise interference.

IV. PROBLEM STATEMENT

Image encryption and decryption is used to transmit confidential images like medical, military images, etc, so it is necessary to protect sensitive and confidential information from unauthorised use and modification. To achieve this objective, encryption is one of the best method among hiding information like AES[advanced encryption standard]and XOR operation to increase entropy, decrease correlation and encryption time.

V. METHODOLOGY

We propose two novel 2D chaotic maps for a robust medical images and data encryption pipeline. The proposed framework is a discrete-time, nonlinear approach with unique dynamical chaotic behaviour. Because of chaos inherent unrepeatability and ergodicity proprieties, searches at higher speeds can be performed compared with probability distribution-based algorithms, i.e., AES. Among different possible maps, Henon chaotic map is proposed and investigated for medical image encryption.

By definition, a chaotic map is any function that exhibit chaotic behaviour. The chaotic nature of the proposed maps defining the mapping of a given point (x_n,y_n) to a new position (x_{n+1},y_{n+1}) is controlled mathematically by:

$X[n+1] = 1 - a * x[n]^2 + y[n]$ _____(2.1)
$Y[n+1] = b * x[n]$ _____(2.2) where n is the iteration number.

The first proposed map, Eq. (2.1), represents a novel 2D financial model and is shown in Fig. 3.1 (a), it represents a new non-linear dynamic model. On the other hand, the second proposed map (Fig. 2.1 (b)) is considered as a novel

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

extension of the well-known logistic map, and its chaotic nature is close to the Henon map mathematical expression, but with two control parameters a andb. The generation of the such maps starts by selecting one of the models defined by Eqs. (2.1) or (2.2) and setting initial system parameters (n, the upper and lower limits, the number of dimensions, and the fitness function). Then, maps initial positions x_0, and y_0 are randomly initialized. Finally, an iterative process of n times is followed to update x_{n+1} and y_{n+1}.

The Henon map is a two-dimensional discrete-time dynamical system that exhibits chaotic behavior. It is often used as a source of randomness for encryption due to its high sensitivity to initial conditions and its unpredictability. Here is a general methodology for implementing the Henon chaotic map in an encryption scheme:

1. Initialization: Choose initial values for the Henon map parameters a and b, as well as the initial x and y values.
2. Henon map iteration: Iterate the Henon map equation over a number of iterations to generate a sequence of random numbers. The Henon map equation is given by:
X[n+1] = 1 – a * x[n]^2 + y[n] _____(1)
Y[n+1] = b * x[n] _____(2)
Where n is the iteration number.
3. Key generation: Use the sequence of random numbers generated by the Henon map as the encryption key. The length of the key will depend on the number of iterations performed in step 2.
4. Image encryption: Use the encryption key to encrypt the medical image using a symmetric encryption algorithm. The encryption algorithm should be chosen based on its security and speed.
5. Key management: The encryption key must be securely stored and transmitted to authorized users to ensure that they can decrypt the image.
6. Image decryption: To decrypt the image, the authorized user must have access to the encryption key and use it to reverse the encryption process.
7. Image post-processing: Once the image has been decrypted, any post-processing steps that were applied during the pre processing step can be reversed to restore the original image.
data retrieved by chaotic.

VI. RESULTS AND DISCUSSION

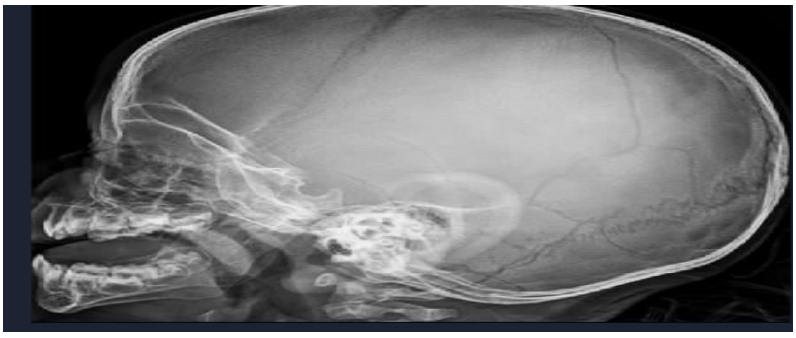


FIG 1 Input original image

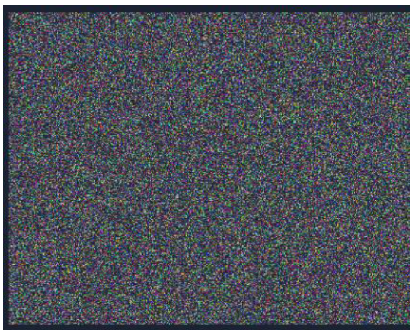


FIG 2 . Encrypted image

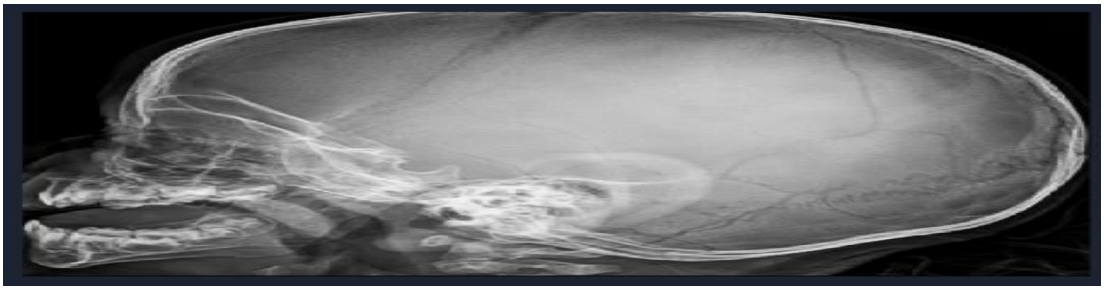


FIG 3 Decrypted image

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

Above mentioned figures show our experimental results in which Fig 8, is the input medical image, Fig 9 is the encrypted image of the input image obtained using chaotic maps and our encryption algorithm and Fig 10 , is the decrypted image obtained by decrypting the encrypted (cipher) image with our decryption algorithm.

ANALYSIS OF IMAGE ENCRYPTION

Image encryption is a vital component in security of images during transmission and storage. Hence, the encrypted image's secrecy(confidentiality) and robustness are analysed based on its algorithm selection, key management, pixel correlation and histogram analysis are performed for ensuring level of encryption.

ENTROPY

Entropy analysis is a crucial technique in image encryption for assessing the randomness or unpredictability of pixel values within an image. By calculating the entropy of an image, one can gauge how much information is present and how uniformly it's distributed. Higher entropy implies greater randomness and hence stronger encryption.In image encryption, entropy analysis helps in designing encryption algorithms that maximize randomness, making it harder for adversaries to extract meaningful information from the encrypted image without the decryption key. Techniques such as shuffling pixels, applying chaotic maps, or employing encryption keys derived from entropy sources can enhance the security of image encryption schemes by increasing entropy levels.

Another perfect metric to evaluate the encryption randomness, beside pixel distributions and R, is information entropy (E), which can be computed by eq

$$E(m) = -\sum_{i=0}^{2N-1} p(m_i)\log_2\left(p(m_i)\right) \quad \text{(4.2)}$$

Where,

$\mathbf{p}(\mathbf{m_i})$ is the probability of symbol $\mathbf{m_i}$ and N represents the number of bits for each symbol

TABULATION OF RESULT:

TABLE 2: ENTROPY VALUES OF IMAGE

Image Type	Entropy
Original image	7.35
Encrypted image	7.63
Decrypted image	7.35

TABLE 3: COMPARISION OF ENTROPY VALUES

Sl.no	Entropy	Original image	Encrypted image	Decrypted image
1.	Proposed	7.35	7.63	7.35
2.	Ref [8]	7.7562	7.9990	7.7562
3.	Ref [4]	7.6698	7.9911	7.6698
4.	Ref [14]	7.5593	7.9926	7.5593

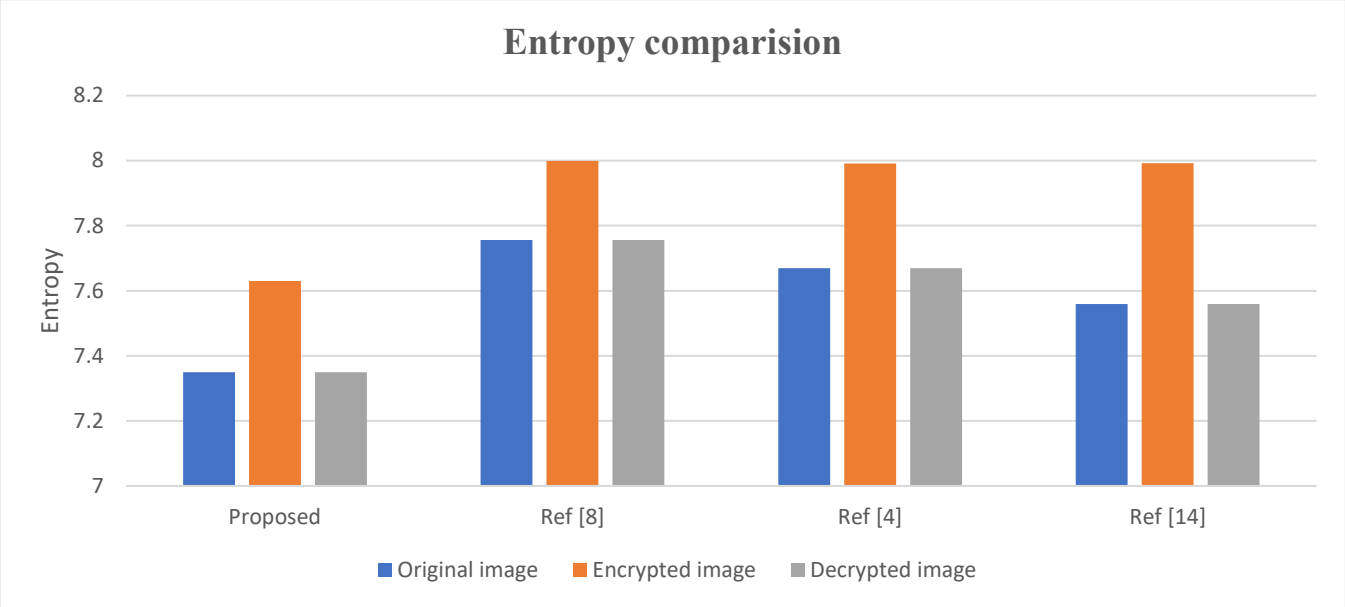
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|



When comparing tables containing entropy values of different images, you're essentially assessing the complexity or randomness within each image and how they differ. Higher entropy values indicate more randomness or complexity within the image, while lower values suggest more uniformity or predictability. By comparing these tables side by side, you can observe how the entropy distributions vary between the images. This analysis can provide insights into the diversity of content or the level of detail present in each image. For example, if one image has consistently higher entropy values across various regions compared to another, it may indicate that the first image contains more diverse or detailed content. Conversely, if one image has lower entropy values overall, it may suggest that the content is more uniform or repetitive.

VII. CONCLUSION

Our paper has introduced a medical image encryption scheme that can integrated in cloud-based internet-of-heath systems (IoHS). The proposed pipeline introduced two novel chaotic maps, which demonstrated strong and effective chaotic behaviours, unpredictability, and extreme sensitive to initial seeds. To improve encryption quality and performance, our encryption scheme is based on an effective permutation-substitution framework with good confusion and diffusion properties. Experiments using various test medical images advantage of the proposed scheme. Additional companion with state-of-the-art encryption scheme using benchmark images highlighted the high effectiveness and robustness of the proposed scheme to prevent many existing cryptography attacks and cryptanalysis techniques.

REFERENCES

1. Vinod Patidar and Gurpreet Kaur, “A Novel Conservative Chaos Driven Dynamic DNA Coding For Image Encryption”, Dynamic Systems, vol 8,1100839,2023.
2. Dhanakshinamoorty Vignesh and Santo Banerjee, presents “A Novel Fractional Sine Chaotic Map And Its Application To Image Encryption And Watermarking”, Mathematical Sciences, vol 13, 6556, 2023.
3. Sourab Kumar and Jaishree Jain, presents “Improved Security Of E-Healthcare Images Using Hybridized Robust Zero-Watermarking And Hyper-Chaotic System Along With RSA, Deprtment of Electrical and Computer Science Engineering, vol 10, 1071, 2022.
4. Syed Saqlain & Zeshan Iqbal presents, “Henon Chaotic Map Based Image Encryption Scheme Using Bit-level Circular Shift”, Department of Computer Science Engineering vol 100,1992-8645, 2022.
5. Xiuli Chai &Xiaoyu Zhengpresents, “An image encryption algorithm based on chaotic system and compressive sensing”, Department of Electrical and Computer Science Engineering, 2018.
6. Yousef Alghamdi & Arslan Munir presents, “A Lightweight Image Encryption Algorithm Based On Chaotic Map And Random Substitution” vol 24, 1344, 2022.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 12, December 2024

|DOI: 10.15680/IJIRSET.2024.1312192|

7. M.Essaid&A.Saaidi presents, “A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map” Department of Mathematics and Computer Science vol 57,3670,2018.
8. Jameel Arif & Baraq Ghaleb presents, “A novel chaotic permutation -substitution image encryption scheme based on logistic map and random substitution”Department of Computer Science vol 10, 12966– 12982,2022.
9. Qun Ding & Chen Yang presents, “Image encryption scheme based on mixed chaotic bernoulli measurement, matrix block compressive sensing” Department of Electronic Engineering, vol 24(2), 273, 2022.
10. Mohamed Gabr and Wassim Alexan presents, “Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption”, Department of Computer Science Engineering vol 15,1081, 2023.
11. Jannatul Ferdush& Mahbuba Begum presents, “Chaotic Lightweight Cryptosystem for Image Encryption”, Department of Computer Science and Engineering, vol 10,1155,2019.
12. Jian Zhang & Honge Ren presents, “Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps”, Department of Mathematics, 917147, 2014.
13. Neeraj Dhanraj &ShradSalunke, presents, “5D Gauss Map Perspective to Image Encryption with Transfer Learning Validation”, Department of Electronics and Communication Engineering, vol 12(11), 5321, 2022.
14. Lina Zhang &Xianhua Song presents, “Reversibly selective encryption for medical images based on coupled chaotic maps and steganography”, Complex & Intelligent Systems vol 10(6), 2.23
15. Cong Xu &Jingru Sun presents, “A novel image encryption algorithm based on bit-plane matrix rotation andhyper chaotic systems”, Multimedia Tools and Applications, Department of Computer Science and Electronic Engineering, 2020.
16. Jian Zhang & Honge Ren presents, “Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps”, Department of Mathematics, 917147, 2014.
17. Kwok-Wo Wongand Wing-Shing Law presents, “A Fast Image Encryption Scheme based on Chaotic Standard Map”, Department of Electronic Engineering, 2020
18. Shenyong Xiao &YaShuang Deng presents, “Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism”, Malware Analysis and Vulnerability Detection Using Machine Learning, 7913061, 2020.
19. Ramesh Premkumar and Miroslav Mahdal presents, “An Efficient Chaos-Based Image Encryption Technique Using Bitplane Decay And Genetic Operators”, Sensors, vol 22,8044, 2022.
20. Mimgfang Jiang and Hengfu Yang presents, “Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation”, Department of Computer Science and Engineering, vol 25(11), 1516,2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details