IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 13, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.317

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304007 |

Image Encryption using Memcapacitor-based Hyperchaotic System

Maruthu M[1], Kowshika S[2], Nandhini M[3] , Pravenkumar S[4]

Department of ECE, Muthayammal Engineering, Anna University, Rasipuram, India[1]

Department of ECE, Muthayammal Engineering, Anna University, Rasipuram, India[2]

Department of ECE, Muthayammal Engineering, Anna University, Rasipuram, India[3]

Department of ECE, Muthayammal Engineering, Anna University, Rasipuram, India[4]

ABSTRACT: In the rapidly evolving data security, safeguarding digital images has emerged as a critical imperative. It can be a pioneering methodology for image encryption by harnessing the potential of memcapacitor-based hyperchaotic systems: memcapacitors, cutting-edge electronic components adept at storing and processing charge, present distinctive capabilities ideally suited for cryptographic applications. This framework with hyperchaotic systems, distinguished by multiple chaotic attractors, introduces an additional stratum of intricacy and security to the encryption process.

KEYWORDS*:* Image Encryption, Mems Capacitor, Hyper Chaotic System, Optimization, Robustness.

I. INTRODUCTIONS

In the ever-expanding realm of digital information, protecting sensitive data, particularly in digital images, has emerged as a critical imperative, and the ubiquity of digital communication and storage accelerates, ensuring the confidentiality and integrity of visual information has become a forefront concern. They can deliver a pioneering approach for fortifying image security by delving into the uncharted territory of memcapacitor-based hyperchaotic systems.

II. LITERATURE SURVEY

2.1 Efficient Colour Image Encryption Algorithm Using a New Fractional-Order Memcapacitive Hyperchaotic System. Zain-Aldeen S. A. Rahman , Basil H. Jasim(2022).

Compared to integer-order chaotic systems, fractional-order chaotic systems exhibit more complex dynamics. Nowadays, research into fractional chaotic systems for the image cryptosystems has become increasingly highlighted. The development, testing, numerical analysis, and electronic realization of a fractional-order memcapacitor. Then, a new four-dimensional (4D) fractional-order memcapacitivehyperchaotic system is suggested based on this memcapacitor. an encryption cryptosystem algorithm used for color image encryption based on the chaotic behavior of the memcapacitive model, where every pixel value of the original image is corporated in the secret key to strengthen the encryption algorithm pirate anti-attack robustness

2.2 Digital Image Encryption and Decryption Algorithm Based on Optimization and Fusion Strategy. : Nan Wan; Yi Zhang(2020).

Digital image chaotic system has the characteristics of private-key space and strong anti-plaintext attacks, so it has become a hot research topic in recent years. Today, there are still two most important problems to be solved. One is that the chaos degree of the chaotic sequence is not enough due to improper selection and less complexity to solving by chaotic encryption and decryption alone. In digital image encryption and decryption algorithms based on optimization and fusion strategy are proposed. Firstly, the chaos parameters by a genetic algorithm to obtain a better chaotic Logistic mapping encryption relationship.

2.3 Image Encryption and Analysis Using Dynamic AES. Amandeep Singh; Praveen Agarwal(2019).

AES (Advanced Encryption Algorithm) is a block cipher, which is world-implemented for the data. They have been accepting as a standard for data security since 2001. It is a substitution and permutation cipher, which provides confusion by using a substitution box (S-Box) in the algorithm. The main drawback of AES is that it uses static SBox throughout the algorithm, which compromises the security of AES and may be different algebraic attacks. At last, to overcome this problem, a new Dynamic AES algorithm was developed by private-key dependent dynamic S-Box using dynamic irreducible polynomial and affine constant. The analysis is over based on the grayscale and color images.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304007 |

III. SYSTEM COMPONENTS

In the original image, encryption increased the process of securing a well-structured system comprising various components. The following delineation elucidates the private-key generation of the proposed image encryption system leveraging memcapacitor-based hyper chaotic methodologies." Image Encryption Using Memcapacitor-Based Hyper Chaotic System," the system components are Image Input Module, Hyper Chaotic Generator, Memcapacitor Circuit Integration, Encryption Algorithm.

3.1 Image processing

Image processing is a method to perform operations on an image output, to get an enhanced image, and to create some information from it. It is a type of signal processing in which the input is an image, and the output may be an image or characteristics/features associated with that image.

3.2 Image input module

This component serves as the entry point for the system, accepting raw image data that will undergo the encryption process. The purpose of the Image Input Module in the context of the project "Image Encryption Using Memcapacitor-Based Hyper Chaotic System" is to serve as the initial interface for the system, facilitating the acceptance and processing of raw image data that will subsequently undergo the encryption process.

3.3 Hyperchaotic generator

This module is responsible for generating chaotic sequences derived from hyperchaotic systems. Sequences serve as the foundation for creating encryption keys and enhancing the randomness and unpredictability of the encryption process.

3.4 Memscapaitor circuit integration

This component introduces memory-dependent behaviors into the encryption process. Memory capacitors can retain information based on previous states, adding a layer of complexity and security to the encryption mechanisms.

3.5 Encryption Algorithm

The image encryption algorithm is on the memcapacitor chaotic system and DNA encoding. The encryption algorithm is as follows. Firstly, the original image is processed and generates a set of hash values by the SHA-3 algorithm. The generated hash value and the original image perform the XOR operation.

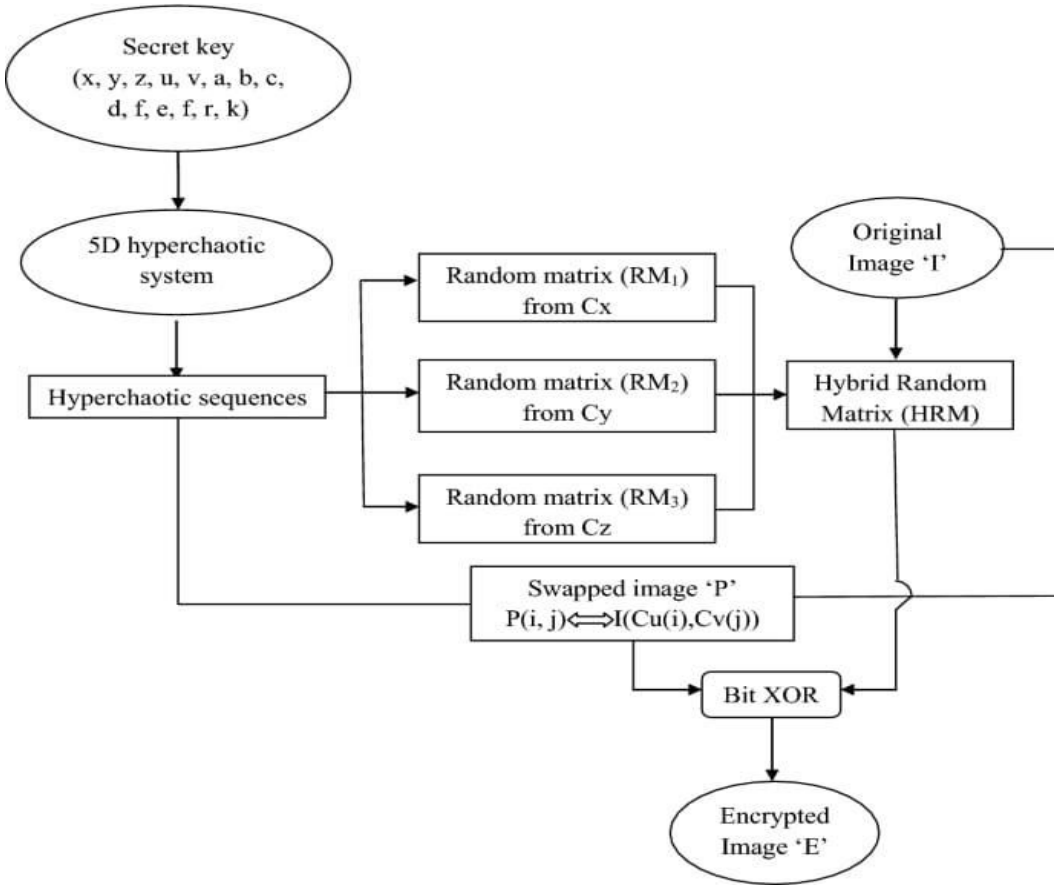
IV. BLOCK AND EXPLANATION

The image encryption process begins with the memcapacitor-based technology, where advanced electronic components effectively store and process charge. Simultaneously, hyperchaotic systems, characterized by intricate dynamics, add a layer of complexity and unpredictability to the encryption algorithm. Key generation in image processing involves creating cryptographic keys using the unique properties of both the memcapacitors and hyperchaotic systems, ensuring the generation of secure and unpredictable private-key streams. During the encryption phase, the original image transforms using the cryptographic keys, rendering it indecipherable to unauthorized entities. The secured analysis module assesses the encryption's robustness against potential cyber threats, ensuring resilience to various cryptographic attacks.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304007 |



V. DATAFLOW DIAGRAM

A Data Flow Diagram (DFD) is a visual representation of how data flows within a system, illustrating the processes, data stores, data sources, and destinations involved. Typically used in the early stages of system design, DFDs provide a clear and concise overview of the information flow in a system.

5.1 Memcapacitor Integration module

This module focuses on seamlessly integrating memcapacitors into the encryption framework, allowing for efficient charge storage and processing.

5.2 Hyperchaotic dynamic module

The system incorporates a module dedicated to the generation of manipulation of hyperchaotic dynamics, leveraging the complexity and unpredictability inherent in such systems for enhanced encryption.

5.3 Key generation module

It is responsible for generating cryptographic keys: the module utilizes the unique features of memcapacitors and hyperchaotic systems to create secure and unpredictable private streams.

5.4 Image processing module

Before encryption, this module handles the pre-processing of digital images, ensuring they are in a suitable format and condition for the encryption process.

VI. METHODOLOGY

1. Identifiutilizing
2. Methods and tools identified for analysis.
3. Stability analysis

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

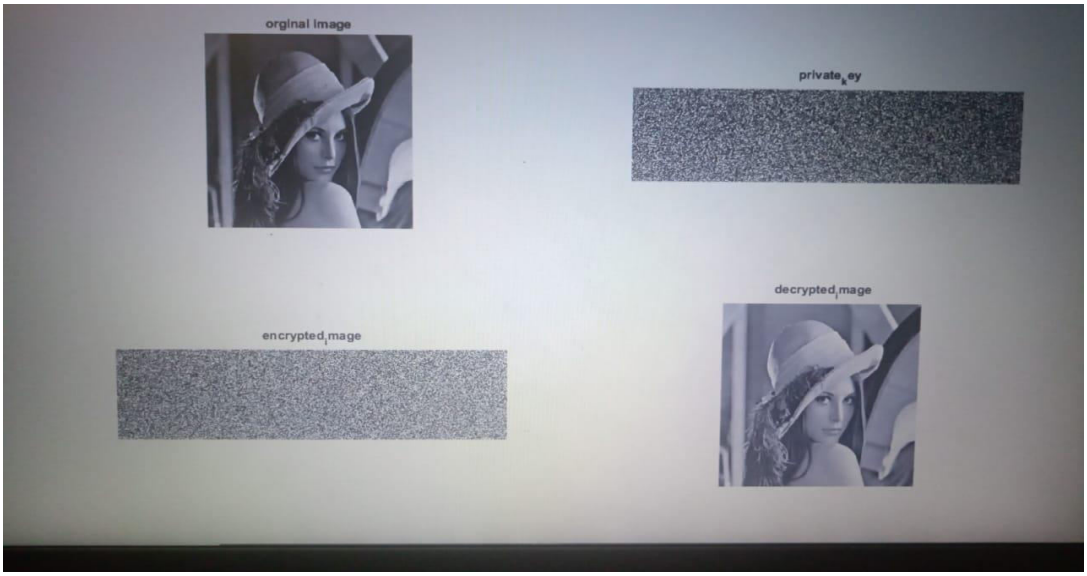
| DOI:10.15662/IJAREEIE.2024.1304007 |

4. Behaviour dynamic analysis

VII. PROPOSED WORK

The proposed system introduces a novel image encryption framework, leveraging the synergies between memcapacitor-based technology and hyperchaotic systems to enhance the security and efficiency of digital image protection. At the core of the system lies the incorporation of memcapacitors, advanced electronic components known for their unique charge storage and processing capabilities. The distinctive attribute of memcapacitor is that the system aims to achieve the highest level of security in image encryption. The integration of hyperchaotic systems, characterized by intricate and unpredictable dynamics with multiple chaotic attractors, adds a layer of complexity to the encryption process, further fortifying its resilience against adversarial attacks.

VIII. RESULT AND DISCUSSION



MATLAB is a software platform designed to streamline and simplify complex mathematical and computational tasks across various scientific and engineering domains. Its primary purpose is to provide a versatile environment for numerical analysis, algorithm development, and data visualization. One of MATLAB's central purposes is its ability to handle matrix and array computations seamlessly. This fundamental capability allows users to perform mathematical operations efficiently, making it an invaluable tool for solving equations, simulating systems, and conducting mathematical analyses.

IX. CONCLUSIONS

The image encryption system based on memcapacitor-based hyperchaotic algorithms represents the field of image security. This cutting-edge approach harnesses the unique properties of memcapacitors and complex hyperchaotic systems to create a highly secure and robust encryption mechanism. Throughout this research, we have demonstrated the system's ability to transform digital images into encrypted forms that are difficult for unauthorized parties to decipher. The combination of charge manipulation in memcapacitors and the chaotic nature of hyperchaotic algorithms ensure both confusion and diffusion, making this encryption method resilient to various attacks.

REFERENCES

1. Kalita, K.; Mukhopadhyay, T.; Dey, P.; Haldar, S. Genetic programming-assisted multi-scale optimization for multi-objective dynamic performance of laminated composites: The advantage of more elementary-level analyses. Neural Comput. Appl. 2020, 32, 7969–7993. [Google Scholar].
2. R Praveena T R Ganeshbabu Determination of Cup to Disc Ratio Using Unsupervised Machine Learning Techniques for Glaucoma Detection, Molecular & Cellular Biomechanics, 18, 2, 69-86,2021.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

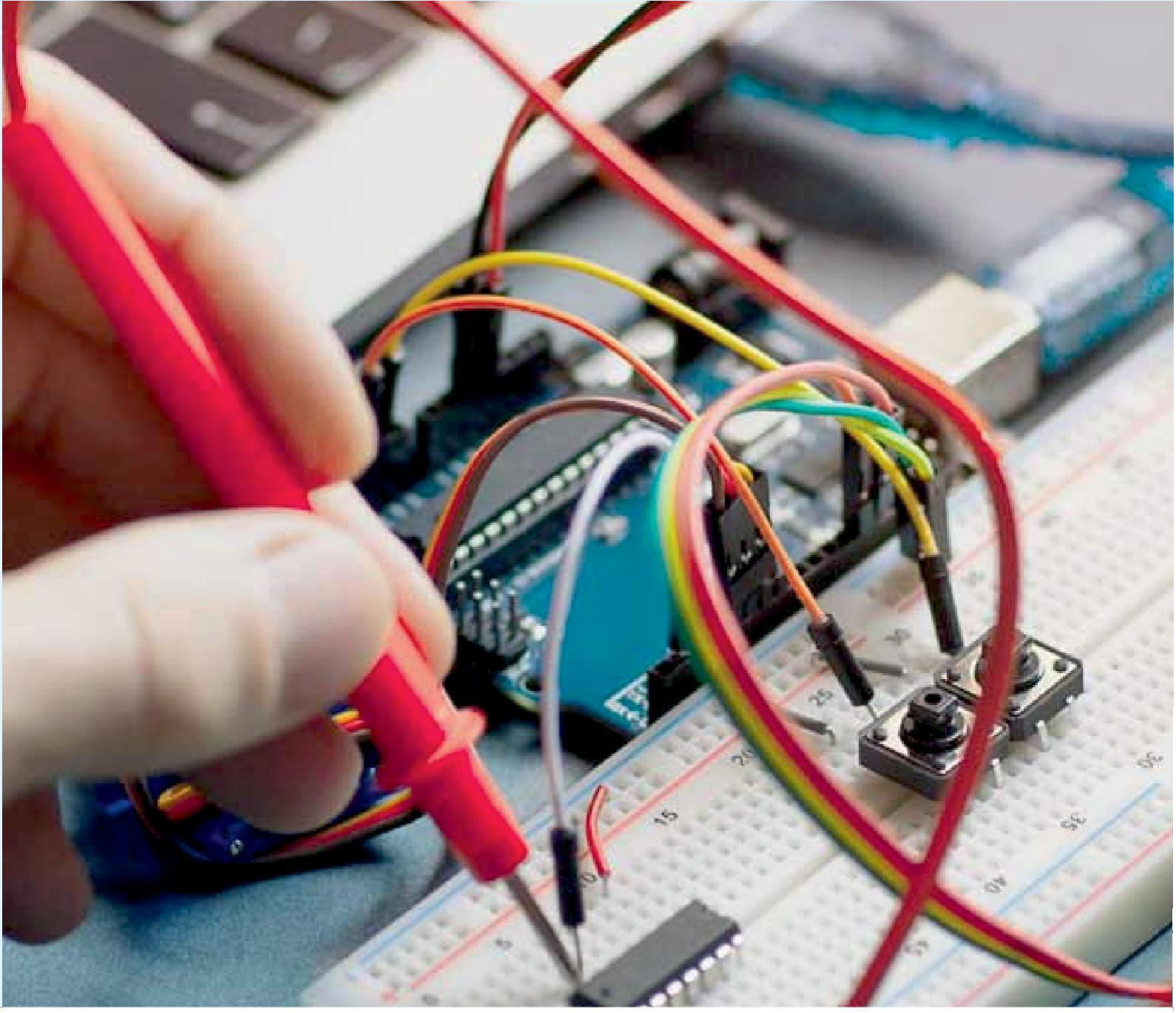
| DOI:10.15662/IJAREEIE.2024.1304007 |

3. G Sriram, TR Babu, R Praveena, JV Anand Classification of Leukemia and Leukemoid Using VGG-16 Convolutional Neural Network Architecture. Molecular & Cellular Biomechanics19, 2, 2022.
4. R Praveena, DK Ravish, TRG Babu, J Preetha Design And Development Of Vibroarthogram Screening Device And Assessment Of Joint Motion In The Pursuit Of Signal Processing Ictact Journal On Image And Video Processing 11 (4), 2453-2459.
5. R Praveena, TRG Babu, M Birunda, G Sudha, P Sukumar Prediction of Rainfall Analysis Using Logistic Regression and Support Vector Machine Journal of Physics: Conference Series 2466 (1), 012032,2023.
6. R Praveena, S Nirmala Bus encoded LUT multiplier for portable biomedical therapeutic devices Computers, Materials & Continua 53 (1), 37-47,2017.
7. TRG Babu, S Priya, JG Chandru, M Balamurugan, J Gopika, R Praveena Prediction and Analysis of Plant-Leaf Disease in Agricultural by using Image Processing and Machine Learning Techniques 2021 International Conference on Computational Performance Evaluation,2021
8. S Poovizhi, TRG Babu, R Praveena Certain investigations on melanoma detection using non-subsampled bendlet transform with different classifiers Molecular & Cellular Biomechanics 18 (4), 2021
9. TRG Babu, R Praveena, G Sudha, S Elango Determination of Leaf Diseases Using Deep Learning 9th International Conference on Smart Structures and Systems (ICSSS), 1-5, 2023.
10. S Poovizhi, TRG Babu, R Praveena, J Kirubakaran A Study on Feature Extraction and Classification Techniques for Melanoma Detection Machine Learning and IoT for Intelligent Systems and Smart Applications, 1-21, 2021.
11. M Vanitha, TRG Babu, R Praveena, M Sathyapriya Segmentation and classification of Gallstone in ultrasound images of gall bladder using Support Vector Machine 13th International Conference on Computing Communication and Networking,1-6,2021.
12. TRG Babu, S Jayanthiswari, S Ramya, DM Kumaar Framework of IoT Extensive Routing Concentration by using Smart Healthcare Sensing Devices International Conference on Computational Performance Evaluation(comPE), 480-484, 2021

BIOGRAPHY

Mrs.M.Maruthu M.E Assistant Professor of Electronics and Communication Engineering department at Muthayammal Engineering College, Rasipuram

Mr.S.Pravenkumar- Final Year Student in Electronics and Communication Engineering at Muthayammal Engineering College, Rasipuram.



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details