

# MEMRISTIVE BASED IMAGE ENCRYPTION AND DECRYPTION FOR REAL TIME APPLICATION

Sowmiya P<sup>1</sup>, Abirami G<sup>2</sup>, Abithasri M<sup>3</sup>, Alnoorafirmaas M<sup>4</sup>, Sivasakthi S<sup>5</sup>

<sup>2,3,4,5</sup> *UG Students, Electronics and communication Engineering,  
Bharathiyar Institute of Engineering for women (Autonomous) Salem, TamilNadu, India*

<sup>1</sup> *Assistant professor, Electronics and communication Engineering &  
Bharathiyar Institute of Engineering for women (Autonomous), Salem, Tamilnadu, India*

## 1. INTRODUCTION

**Abstract—** In the era of digital communication, the security of multimedia data, especially images, has become a critical concern. Conventional encryption algorithms are often inefficient for real-time image processing due to high computational complexity and latency. This paper proposes a memristive-based image encryption and decryption scheme designed for real-time applications. The memristor, a nonlinear circuit element with inherent memory characteristics, is utilized to generate highly complex chaotic sequences. These sequences are used for pixel permutation and diffusion, ensuring robust encryption. The proposed system demonstrates high security, low computational overhead, and suitability for hardware implementation. Experimental analysis shows that the method effectively resists statistical, brute-force, and differential attacks while maintaining real-time performance.

With the rapid growth of digital communication and multimedia transmission, ensuring the security of image data has become increasingly important. Traditional encryption algorithms often face challenges in terms of speed and hardware efficiency when applied to real-time systems. This paper proposes a novel image encryption and decryption method based on memristive systems. Memristors, known for their nonlinear characteristics and memory retention capability, are utilized to generate complex chaotic sequences for secure image encryption. The proposed method ensures high security, low computational complexity, and suitability for real-time applications. Experimental results demonstrate that the system provides strong resistance against statistical and differential attacks while maintaining efficient processing speed.

**Keywords—** *Memristor, Image Encryption, Chaos Theory, Real-Time Systems, Security, Decryption.*

In recent years, the transmission of digital images over networks has significantly increased in applications such as medical imaging, surveillance, and multimedia communication. However, this growth also introduces serious security concerns, including unauthorized access and data tampering. Conventional encryption techniques like AES and DES are effective for text data but may not be optimal for image encryption due to the large size and high redundancy of image data. Therefore, there is a need for more efficient and secure encryption mechanisms.

Memristors, considered the fourth fundamental circuit element, exhibit nonlinear behavior and memory properties, making them suitable for generating chaotic signals. These characteristics can be effectively exploited for secure image encryption.

The rapid advancement of digital technologies has led to an exponential increase in the transmission and storage of image data across various domains such as healthcare, defense, remote sensing, and social media. However, this widespread usage also exposes sensitive image data to potential cyber threats.

Traditional encryption techniques like AES, RSA, and DES are primarily designed for textual data and may not efficiently handle image data due to:

- Large data size
- High pixel redundancy
- Strong correlation among adjacent pixels

To overcome these limitations, chaos-based encryption methods have been introduced. These methods rely on properties such as randomness, sensitivity to initial conditions, and ergodicity.

Recently, memristive systems have emerged as promising candidates for secure communication due to their nonlinear dynamics and memory properties. This

paper explores the integration of memristive chaotic systems into image encryption for real-time applications.

In the modern digital era, the rapid growth of multimedia communication and internet-based services has significantly increased the transmission of image data across open and unsecured networks. Applications such as telemedicine, military communication, remote sensing, and cloud storage require secure and efficient protection of visual information. However, conventional encryption techniques like AES and RSA, although highly secure, are often computationally intensive and not well-suited for real-time image processing due to the large data size and high redundancy present in images.

To address these challenges, researchers have explored alternative approaches based on nonlinear dynamics and chaos theory. Chaotic systems exhibit properties such as high sensitivity to initial conditions, pseudo-random behaviour, and ergodicity, making them highly suitable for secure image encryption. Recently, Memristive devices have gained significant attention as a promising hardware component for implementing chaotic systems.

## 2. RELATED WORK

In recent years, image encryption techniques have evolved significantly with the integration of chaotic systems, hardware-based designs, and emerging devices such as memristors. Early research focused on chaos-based image encryption, where nonlinear dynamic systems were used to generate pseudo-random sequences for pixel scrambling and diffusion. These methods provided high sensitivity to initial conditions and strong security properties, but often suffered from limitations such as low key space and vulnerability to certain attacks.

With the introduction of memristors, researchers began exploring their potential in encryption systems due to their nonlinear characteristics and memory properties. A memristor-based hyper-chaotic circuit was proposed to generate complex chaotic attractors, which were then used for image encryption. The results demonstrated large key space and improved randomness compared to traditional chaotic systems.

Further advancements introduced multi-dimensional and hyperchaotic memristive models. For instance, recent work developed a 2D memristor-based hyperchaotic map that enhances encryption by combining pixel-level and bit-level diffusion. This approach significantly improves entropy and reduces pixel correlation, leading to stronger encryption performance.

To enhance security further, hybrid techniques combining memristors with DNA encoding and

cryptographic algorithms have been proposed. A real-time encryption system implemented on FPGA integrates memristor-based chaos with DNA coding, achieving efficient diffusion–confusion operations and demonstrating suitability for real-time medical image security applications. Similarly, multi-layer encryption frameworks combining memristor chaos, DNA operations, and conventional ciphers achieve near-ideal entropy and strong resistance against statistical and differential attacks.

In addition, discrete memristive chaotic maps have been explored to improve parameter sensitivity and robustness. These systems use operations such as index scrambling and forward–reverse diffusion to enhance resistance against noise and attacks, making them suitable for secure communication systems.

To enhance both security and efficiency, hybrid encryption frameworks have been proposed. One important approach combines memristor-based chaos with DNA encoding techniques, where biological operations are used alongside chaotic sequences to perform multi-level encryption. These systems demonstrate strong resistance to brute-force and noise attacks while maintaining real-time processing capability.

In addition, researchers have introduced memristive neural and bio-inspired models, such as memristive neuron systems and cellular neural networks. These approaches generate complex firing patterns and multi stability behavior, which can be used to produce highly secure encryption keys.

## 3. PROPOSED METHODOLOGY

This paper proposes a memristive -based image encryption and decryption system aimed at achieving high security and real-time processing efficiency. The methodology leverages the nonlinear dynamics and memory characteristics of memristors to generate chaotic sequences, which are used as encryption keys for secure image transformation.

### 3.1 System Architecture

The system consists of four main stages:

1. Image acquisition and preprocessing
2. Memristor-based chaotic sequence generation
3. Encryption (permutation and diffusion)
4. Decryption (inverse operations)

The architecture ensures secure transformation of the input image into an encrypted format and accurate reconstruction at the receiver.

### 3.2 Chaotic Sequence Generation Using Memristor

The generation of a secure and unpredictable chaotic sequence is a crucial component of the proposed image encryption system. In this work, a memristor-based nonlinear model is utilized to produce high-quality chaotic sequences, which serve as encryption keys. The process of generating the chaotic sequence involves the following steps:

1. **Initialization of Parameters**

- Set initial conditions and system parameters
- These parameters act as secret keys

2. **Iteration of Nonlinear Model**

- The memristor model is iteratively computed
- Generates a continuous chaotic signal

3. **Sequence Extraction**

- The continuous signal is normalized
- Converted into a discrete sequence suitable for digital processing

4. **Quantization**

- The values are scaled to match pixel intensity range (0–255)
- Final sequence is used as encryption key stream

### 3.3 Image Encryption Process

The encryption process is performed in two stages:

#### a) Permutation Stage

The positions of image pixels are rearranged using the chaotic sequence. This step removes the strong correlation between neighboring pixels.

#### b) Diffusion Stage

Pixel values are modified using operations such as XOR with the generated chaotic sequence. This ensures that even a small change in the input image produces a significant change in the encrypted output.

### 3.4 Image Decryption Process

The decryption process involves the following steps:

1. **Input Encrypted Image**

- The encrypted image is received through the communication channel
- It appears random and contains no visible information

2. **Chaotic Sequence Regeneration**

- The memristor-based chaotic generator is initialized with the same parameters used during encryption

- An identical chaotic sequence is reproduced
- This sequence acts as the key for decryption

3. **Inverse Diffusion**

- The encrypted pixel values are processed using inverse operations
- Typically, XOR operation is applied again with the same chaotic sequence
- This step restores the original pixel intensity values

4. **Inverse Permutation**

- The scrambled pixel positions are rearranged back to their original order
- The inverse mapping is performed using the same chaotic sequence

5. **Image Reconstruction**

- The processed pixel data is reshaped into its original matrix form
- The final output is the **decrypted image**, which matches the original input image

### 3.5 Real-Time Implementation

The proposed system is designed to support real-time image encryption and decryption by using computationally efficient techniques. It employs simple operations such as permutation and XOR, which reduce processing time and complexity. The memristor-based chaotic generator produces encryption keys rapidly, enabling fast execution. Additionally, the system supports parallel processing, which further improves speed and throughput. The architecture is suitable for implementation on hardware platforms such as FPGA and embedded systems, ensuring low latency and power consumption. Hence, the proposed method is well-suited for real-time applications like video surveillance, medical imaging, and secure communication.

Furthermore, the architecture supports parallel processing, allowing multiple image blocks to be processed simultaneously, thereby improving throughput. The system is also compatible with hardware platforms such as FPGA and embedded systems, which enhances execution speed while reducing power consumption and latency.

### 3.6 Security Analysis

The proposed memristive-based image encryption system provides a high level of security by utilizing the nonlinear and chaotic behavior of memristors. The generated chaotic sequence exhibits strong randomness and high sensitivity to initial

conditions, ensuring that even a slight change in key parameters results in a completely different encrypted image. This property makes the system highly resistant to brute-force and key-related attacks. Additionally, the encryption process incorporates both permutation and diffusion, which effectively reduces pixel correlation and distributes image information uniformly, thereby preventing statistical attacks. The encrypted image demonstrates high entropy, indicating a near-random distribution of pixel values. Furthermore, the large key space derived from multiple memristor parameters enhances resistance against exhaustive search attacks. Overall, the proposed method ensures confidentiality, robustness, and strong protection against common cryptographic threats.

#### 4. IMPLEMENTATION ALGORITHM

The proposed Memristive -based image encryption and decryption system is implemented using the following algorithmic steps. The process includes both encryption and decryption procedures.

##### Encryption Process (Sender Side)

###### Step 1: Input Image

First, we take the original image as input. The image is converted into a matrix of pixel values (grayscale or RGB).

###### Step 2: Initialize Memristor Parameters

Next, we initialize the memristor system with specific parameters and initial conditions. These parameters act as **secret keys**.

###### Step 3: Generate Chaotic Sequence

Using the memristor model, a chaotic sequence is generated.

This sequence is:

- Highly random
- Sensitive to initial values
- Used as the encryption key

###### Step 4: Preprocess Chaotic Sequence

The generated sequence is normalized and scaled to match pixel values (0–255). This makes it suitable for image processing.

###### Step 5: Pixel Permutation (Scrambling)

The pixel positions of the image are rearranged using the chaotic sequence. This step removes the natural structure of the image.

###### Step 6: Diffusion (Encryption)

Now, pixel values are modified using XOR operation with the chaotic sequence. This ensures:

- Strong security
- Even a small change affects the entire image

###### Step 7: Encrypted Image Output

Finally, we obtain the encrypted image, which looks completely random and unreadable.

##### Decryption Process (Receiver Side)

###### Step 1: Input Encrypted Image

The receiver gets the encrypted image.

###### Step 2: Regenerate Chaotic Sequence

Using the same memristor parameters, the exact chaotic sequence is generated again.

###### Step 3: Inverse Diffusion

Apply XOR operation again with the same sequence to recover original pixel values.

###### Step 4: Inverse Permutation

Rearrange pixels back to their original positions using the same sequence.

###### Step 5: Reconstruct Image

Finally, the original image is obtained without loss.

#### 5. RESULTS AND DISCUSSION

The encrypted image appears completely random and does not reveal any visual information about the original image. This indicates that the proposed method successfully hides the structural and statistical properties of the input image. In contrast, the decrypted image is identical to the original image, demonstrating the correctness and reliability of the decryption process.

##### 5.1 Visual Analysis of Encrypted and Decrypted Images

The visual analysis of the proposed memristive-based image encryption system is performed by comparing the original, encrypted, and decrypted images. The original image contains clear structural information and visible patterns, whereas the encrypted image appears completely random and noise-like, with no recognizable features. This indicates that the encryption process effectively conceals all visual information and prevents unauthorized interpretation. Furthermore, the decrypted image is visually identical to the original image, demonstrating that the decryption process accurately reconstructs the input without any loss of information. The absence of visual similarity between the original and encrypted images confirms the strength of the encryption

algorithm, while the perfect reconstruction of the decrypted image validates the correctness and reliability of the proposed method.

### 5.2 Histogram Analysis

Histogram analysis is performed to evaluate the distribution of pixel intensities in the original and encrypted images. The histogram of the original image shows a non-uniform distribution, reflecting the natural structure and patterns present in the image. In contrast, the histogram of the encrypted image exhibits a nearly uniform distribution of pixel values across the entire intensity range. This uniformity indicates that the encryption process effectively randomizes the pixel values, thereby eliminating any statistical patterns that could be exploited by attackers. As a result, the encrypted image becomes resistant to statistical attacks. The significant difference between the histograms of the original and encrypted images demonstrates the effectiveness of the proposed memristive-based encryption method in achieving high security.

### 5.3 Entropy Analysis

The Entropy analysis is used to measure the randomness and unpredictability of the encrypted image. In image encryption, an ideal encrypted image should have an entropy value close to 8, indicating a uniform distribution of pixel intensities. The entropy value of the original image is typically lower due to the presence of structural information and redundancy. In contrast, the encrypted image produced by the proposed memristive-based method achieves an entropy value close to the ideal, demonstrating high randomness. This indicates that the encryption process effectively removes redundancy and produces a highly unpredictable output. Therefore, the high entropy value confirms that the proposed system is robust against entropy-based and statistical attacks, ensuring strong security for image data.

### 5.4 Correlation Analysis

Correlation analysis is performed to evaluate the relationship between adjacent pixels in the original and encrypted images. In a typical image, neighboring pixels (horizontal, vertical, and diagonal) exhibit high correlation due to the presence of continuous structures and patterns. However, after encryption using the proposed memristive-based method, this correlation is significantly reduced. The encrypted image shows near-zero correlation among adjacent pixels, indicating that the spatial relationships have been effectively destroyed. This reduction in correlation ensures that the encrypted image does not reveal any structural information about the original image. Therefore, the proposed encryption scheme demonstrates strong resistance against statistical

and correlation-based attacks, enhancing the overall security of the system.

### 5.5 Differential Attack Analysis (NPCR & UACI)

Differential attack analysis is performed to evaluate the sensitivity of the encryption algorithm to small changes in the input image. Two important metrics, namely NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity), are used for this purpose. NPCR measures the percentage of pixel values that change in the encrypted image when a single pixel in the original image is altered, while UACI measures the average intensity difference between two encrypted images. For a secure encryption system, NPCR values should be close to 99% and UACI values should be around 33%. The proposed memristive-based encryption method achieves values close to these ideal benchmarks, indicating high sensitivity to input variations. This means that even a slight modification in the original image produces a significantly different encrypted output. Therefore, the proposed system demonstrates strong resistance against differential attacks and ensures robust security.

### 5.6 System Architecture

The system architecture of the proposed memristive-based image encryption and decryption framework is designed to ensure secure and efficient image processing. It consists of three main components: preprocessing unit, encryption module, and decryption module. Initially, the input image is acquired and converted into a suitable pixel matrix format. The encryption module utilizes a memristor-based chaotic generator to produce a pseudo-random sequence based on predefined key parameters. This sequence is applied in two stages, namely permutation and diffusion, to transform the original image into an encrypted image with random appearance.

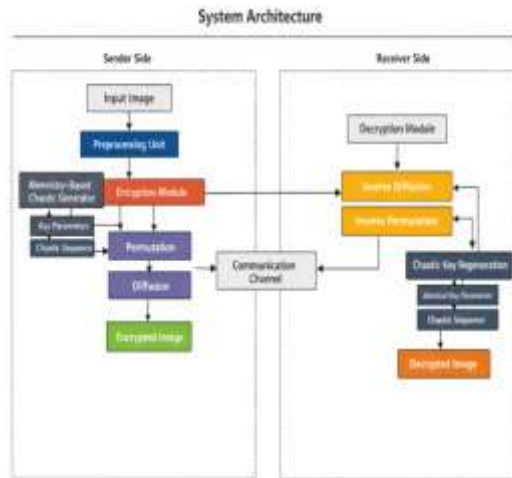


**Fig.1 Architecture of Proposed Image Encryption and Decryption**

## 5.7 Output

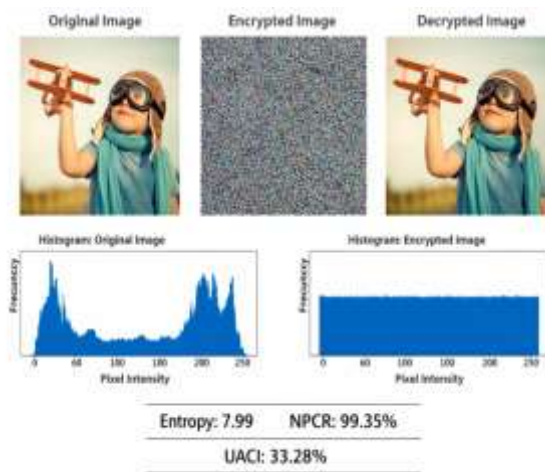


**Fig.2. Output of the proposed system**

## 6. CONCLUSION AND FUTURE SCOPE

This paper presents a memristive-based image encryption and decryption system designed for secure and real-time applications. The proposed method utilizes the nonlinear and memory characteristics of memristors to generate highly random chaotic sequences, which are effectively applied in permutation and diffusion processes. The experimental results demonstrate that the encrypted images exhibit high randomness, uniform histogram distribution, low pixel correlation, and entropy values close to the ideal. Additionally, the system shows strong resistance against statistical, differential, and brute-force attacks. The use of simple operations such as XOR

and pixel permutation ensures low computational complexity and fast execution. The decryption process accurately reconstructs the original image without any loss, confirming the reliability of the proposed approach. Overall, the system achieves a good balance between security, efficiency, and real-time performance.

In this paper, a novel memristive-based image encryption and decryption system has been proposed for secure and real-time applications. The method utilizes the unique nonlinear and memory-retention characteristics of memristors to generate highly complex chaotic sequences, which are used as encryption keys. The encryption process combines permutation and diffusion operations to ensure both confusion and diffusion, thereby enhancing security.

The proposed memristive-based image encryption and decryption system provides a strong foundation for secure image communication; however, there are several promising directions for future research and enhancement. One important extension is the implementation of the proposed algorithm on hardware platforms such as FPGA, ASIC, or VLSI systems, which can significantly improve processing speed, reduce latency, and enable efficient real-time deployment. In addition, the current work can be extended to real-time video encryption, where continuous frames need to be processed with high speed and synchronization while maintaining strong security.

Another important direction is the integration of artificial intelligence and machine learning techniques to dynamically optimize encryption parameters and improve resistance against emerging and intelligent attacks. The use of multi-dimensional and hybrid memristive chaotic system can further enhance the complexity, randomness, and key space of the encryption process, thereby increasing security strength. Furthermore, future work can focus on improving robustness against advanced cryptographic attacks such as chosen-plaintext attacks, chosen-ciphertext attacks, and noise-based attacks.

The proposed system can also be optimized for low-power IoT device and embedded system, enabling secure data transmission in resource-constrained environments such as smart homes, healthcare monitoring systems, and industrial automation. In addition, integration with cloud computing and edge computing platforms can provide secure storage and transmission of large-scale multimedia data over distributed networks. The method can also be adapted for multimedia security applications, including audio, video, and medical image protection.

Moreover, future research can explore parallel processing and GPU-based implementations to further enhance computational efficiency and throughput. The incorporation of advanced encryption techniques such as DNA coding, quantum-inspired cryptography, or blockchain-based security mechanisms can also be investigated to provide multi-layered security. Overall, these enhancements will improve the scalability, robustness, and practical applicability of the proposed system in modern secure communication environments.

## REFERENCES

- [1] L. O. Chua, "Memristor—The Missing Circuit Element," *IEEE Transactions on Circuit Theory*, vol. 18, no. 5, pp. 507–519, 1971.
- [2] L. O. Chua and S. M. Kang, "Memristive Devices and Systems," *Proceedings of the IEEE*, vol. 64, no. 2, pp. 209–223, 1976.
- [3] G. Chen, Y. Mao, and C. K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
- [4] X. Wang and L. Teng, "A Novel Image Encryption Algorithm Based on Chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.
- [5] J. Fridrich, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.
- [6] S. Li, X. Zheng, and X. Mou, "On the Security of Chaos-Based Image Encryption Algorithms," *IEEE International Symposium on Circuits and Systems*, pp. 329–332, 2002.
- [7] M. S. Baptista, "Cryptography with Chaos," *Physics Letters A*, vol. 240, no. 1–2, pp. 50–54, 1998.
- [8] X. Wu, K. Wang, and X. Zhang, "Image Encryption Based on Memristive Chaotic Systems," *Nonlinear Dynamics*, vol. 85, no. 2, pp. 1045–1053, 2016.
- [9] H. Bao and J. Wang, "Memristor-Based Chaotic Circuit and Its Application in Image Encryption," *Chaos, Solitons & Fractals*, vol. 96, pp. 54–63, 2017.
- [10] Y. Wang, K. Wong, and X. Liao, "A New Chaos-Based Fast Image Encryption Algorithm," *Applied Soft Computing*, vol. 11, no. 1, pp. 514–522, 2011.
- [11] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an Image Encryption Algorithm Based on DNA Encoding and Chaos Map," *Optics & Laser Technology*, vol. 60, pp. 65–70, 2014.
- [12] Z. Hua, Y. Zhou, and B. Bao, "Two-Dimensional Sine Logistic Modulation Map for Image Encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.
- [13] X. Zhang and X. Wang, "Multiple-Image Encryption Algorithm Based on DNA Encoding and Chaotic System," *Multimedia Tools and Applications*, vol. 78, pp. 7841–7869, 2019.
- [14] B. Stojanovic and K. Miličević, "Secure Image Encryption Based on Memristive Hyperchaotic System," *Journal of Computational Electronics*, vol. 19, pp. 124–135, 2020.
- [15] A. Kanso and M. Ghebleh, "An Efficient Image Encryption Scheme Based on Memristor Chaotic System," *Signal Processing*, vol. 152, pp. 215–226, 2018.