BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **24**, No 4
Sofia • 2024 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2024-0038

New Image Crypto-Compression Scheme Based on Ecc and Chaos Theory for High-Speed and Reliable Transmission of Medical Images in the IOMT

Khadija El Kinani[1], *Fatima Amounas*[1], *Salma Bendaoud*[1], *Mourade Azrour*[2], *Mohamed Badiy*[1]

[1]*R.O.AL&I Group, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismaïl University of Meknes, Errachidia, Morocco*
[2]*IDMS Team, Faculty of Sciences and Techniques Moulay Ismail University of Meknes, Errachidia, Morocco*
E-mails: k.elkinani@edu.umi.ac.ma f.amounas@umi.ac.ma salma.bendaoud2@gmail.com mo.azrour@umi.ac.ma m.badiy@edu.umi.ac.ma

***Abstract*:** *The rapid advancement of IoT has significantly transformed the healthcare sector, leading to the emergence of the Internet of Medical Things* (*IoMT*). *Ensuring the security and privacy of medical data is crucial when integrating with smart and intelligent sensor devices within the hospital environment. In this context, we propose a lightweight crypto-compression scheme based on Elliptic Curve Cryptography* (*ECC*) *and Chaos theory to secure the medical images in IoMT Applications. The primary innovation in this method involves generating dynamic S-box and keys using the ECC mechanism and PieceWise Linear Chaotic Map* (*PWLCM*). *The Wavelet Transform Technology is employed in compression, and the compressed images are secured within an IoT framework. The proposed methodology has been performed in the experiments on various medical images. The findings and Security analysis reveal that the proposed method is more powerful and useful for secure medical image transmission in the IoT ecosystem.*

***Keywords*:** *IoT security, Medical image, Encryption, Wavelet transform, Vector Quantization* (*VQ*), *Healthcare.*

1. Introduction

During the last few years, the Internet of Things (IoT) has emerged as a crucial discussion topic in research and its applications in practice [1]. Integration of the Internet of Things with healthcare has led to the development of an efficient and intelligent system. The extensive use of IoT devices has greatly altered the delivery of healthcare services. Collecting and transmitting medical data, such as medical images, has become increasingly efficient and accessible. However, it still requires enhanced security mechanisms to protect patient privacy. Several issues with medical image security in the IoMT ecosystem must be addressed to guarantee the privacy,

availability, and integrity of medical images. Securing the transmission of medical images and information is a critical requirement in healthcare systems. Various methods have been developed and studied to protect the data and privacy of patients [2-4]. Encryption is among the most effective methods to secure IoMT networks and protect valuable information from unwanted readers [5]. Current digital healthcare image security mechanisms primarily rely on traditional encryption methods such as DES, AES, and RSA. Designing an effective encryption scheme for healthcare images is especially important for real-time teleradiology and other remote internet-based evaluations, where large medical images are transmitted over public networks. Medical images are acquired using various techniques such as computed tomography, X-ray imaging, ultrasound scanning, magnetic resonance imaging, and positron emission tomography [6]. Patient information is private and should remain confidential. However, doctors often transmit patient information in the form of images through public networks for consultation with other medical professionals. Therefore, ensuring security is vital when sending such information over the Internet. In light of this, effective image protection has become increasingly important in recent years. To practically enhance the security of medical images, compression is joined to encryption to obtain a hybrid system called a crypto-compression scheme. The basic idea is to use a hybrid algorithm to encrypt efficiently these images so that the sensitive data cannot be decoded by an attacker using the IoMT network. Medical image encryption is a hot field in cryptography, requiring efficient algorithms that optimize both cost and processing time. Recently, ECC has emerged as a reliable encryption method for safeguarding medical images due to its smaller key sizes, which enable quicker computations and require less storage space. Compression and encryption methods are highly interrelated and often work together. Initially, compression is used to reduce redundant data, while data encryption is performed to achieve a better level of security. Various approaches have been introduced by integrating compression and encryption techniques, including Encryption-Compression, Compression-Encryption, and Hybrid Compression-Encryption. The integration of compression and encryption techniques into medical image analysis has revolutionized the field of IoMT. Research on this topic typically intersects the fields of cryptography, data compression, and medical imaging. UltraSonography (US), Computed Tomography (CT), CT scans, X-rays, PET scan, and Magnetic Resonance Imaging (MRI), are the most commonly used medical imaging techniques. These imaging techniques generate various types of medical images, including X-ray images, CT scans, MRI images, and so on. Few survey publications [7-10] have explored the application of crypto-compression techniques for safeguarding medical images within the Internet of Things (IoT) framework. This paper proposes an efficient hybrid crypto-compression scheme based on Elliptic curve cryptography and Chaos theory to secure the medical images in IoMT Applications. Table 1 presents a comparison between different encryption algorithms and our approach.

Table 1. Comparison of encryption methods for medical images in IoMT environment

Criteria	Algorithm	Description
Processing complexity	RSA	High: $O(n^3)$ for modular exponentiation in RSA encryption, making it costly in terms of computation, especially for large images
	ECC	Moderate: $O(n^2)$ for elliptic curve operations, efficient for key generation but heavy for encrypting entire images
	Our approach	Low: DWT and VQ at $O(n \log n)$ and $O(n)$ respectively, efficiently reduce data; AES and Dynamic S-Box work quickly on reduced data, with ECC key generation at $O(n^2)$
Energy consumption	RSA	Very High: The complexity of RSA implies significant energy usage, challenging for resource-limited IoMT devices
	ECC	Moderate: ECC requires less energy than RSA but remains costly for encrypting large images
	Our approach	Very Low: DWT + Vector Quantization (VQ) efficiently compress data, minimizing energy consumption for AES and PWLCM; minimal consumption in IoMT
Transmission efficiency	RSA	Low: Large uncompressed data leads to costly transmission in time and bandwidth, making RSA less ideal for IoMT
	ECC	Moderate: ECC keys transmit quickly, but the transmission of uncompressed images remains slow
	Our approach	Very High: DWT + VQ maximize compression, accelerating transmission and optimizing bandwidth for IoMT devices
Latency and responsiveness	RSA	High: RSA is very slow, especially for images; significant latency makes it unsuitable for real-time IoMT applications
	ECC	Moderate: ECC is quick for keys but slow for complete images, resulting in noticeable latency
	Our approach	Low: AES has low latency, particularly effective for real-time data processing
Adaptability to IoMT environment	RSA	Low: RSA is poorly suited due to slowness and high energy consumption for large medical images
	ECC	Moderate: ECC alone is suitable for key exchange, but encrypting complete images is too costly
	Our approach	Excellent: DWT + VQ compress data further, minimizing latency and energy consumption; AES and dynamic S-Box secure efficiently, perfect for IoMT

The main idea is to integrate Discrete Wavelet Transform (DWT) and Vector Quantization (VQ) for data compression, and then apply the modified AES algorithm for encryption. This algorithm is effective for large data volumes, with a computational complexity of $O(n)$ and minimal energy consumption, making it ideal for IoMT devices. It provides low latency and optimized transmission efficiency when encrypting compressed data. Overall, AES ensures robust security for sensitive medical images with appropriately sized keys. Our findings suggest that this method optimizes security through a dynamic S-Box and reduces data size through compression, making it well-suited for protecting medical images in the IoMT environment.

1.1. Research contributions

The principal contributions of this paper are as follows:

- A New crypto-compression approach is suggested to enhance medical image security in an IoT environment.

- An efficient IoT framework is developed using AES with a dynamic-Sbox for the medical image encryption algorithm.
- The compression is achieved using the DWT technique combined with Vector Quantization (VQ).
- The model's security and compression capabilities were validated with various medical images, including MRI, CT scans, and X-rays.

1.2. Paper's structure

The rest part of the article is structured as follows: Section 2 reviews related works on the encryption and compression of medical images. Section 3 gives the background information. Section 4 introduces the proposed approach. Section 5 is devoted to the simulation results. Section 6 shows the performance validation. Finally, Section 7 highlights the conclusions and indicates possible future improvements to this approach.

2. Related works

The IoMT has become a strategic priority for future healthcare because of its ability to improve patient care and its scope to provide more reliable clinical data, increase efficiency, and reduce costs. Healthcare organizations have reaped significant benefits from the IoMT. However, the widespread adoption of IoMT has also brought about security threats that pose challenges to the security and privacy of organizations utilizing this innovation. Security aspects of medical images must be considered when transmitting data over an IoT network. Medical images often contain sensitive and private information about patients, and ensuring the confidentiality, integrity, and availability of this data is crucial. Researchers have recognized these security threats and suggested various image encryption techniques to address the security issues [11, 12]. Recent literature includes surveys reporting security and privacy concerns, along with proposed solutions across various research domains [13]. The latest studies examine the security of medical images in IoMT systems from multiple perspectives [14]. Many of the relevant studies focus on software implementations of cryptographic models, which also have high computational complexity. Another facet concerning the security of medical images in IoMT systems involves encryption and compression [15]. The majority of research studies employ a combined strategy of encryption and compression to ensure the security of medical imaging data. For instance, H a j j a j i, D r i d i and M t i b a a [16] proposed a novel approach to medical image security and compression. Their approach combines neural networks with PWLCM to improve both encryption and compression processes. The neural network is used for compressing images, capitalizing on its capability to learn from and adjust to intricate data patterns. Meanwhile, PWLCM is applied for encryption, offering a chaotic-based technique to protect the image data from unauthorized access. Their research offers a valuable contribution to the field by combining advanced neural network techniques with chaotic encryption to improve both data security and efficiency in managing medical images. After that, M a s h a t et al. [17] presented a novel method that merges encryption and compression for transmitting medical

images. Their proposed crypto-compression scheme integrates encryption and compression techniques, such as discrete cosine transform, steganography, and watermarking, to improve both the security and efficiency of medical image transmission. Their approach seeks to protect sensitive medical information while reducing the size of the data for more efficient transmission, addressing key challenges in secure and effective medical image transfer. The research conducted by Pooranakala and Jaitly [18] explores methods to enhance the security of medical images. The authors introduced a method that combines compression techniques, encryption, and image steganography. This comprehensive approach aims to protect medical images from unauthorized access and ensure secure transmission, utilizing multiple security measures to protect sensitive medical data. The authors of this article [19] suggest another recent study that examines various image compression techniques. They discuss both traditional compression methods and newer approaches that focus on compressing regions of interest within images. Their study offers a comprehensive overview of advancements and trends in image compression, highlighting the effectiveness and applications of these techniques in recent research.

2.1. Limitations of related work

Although notable advancements have been achieved in securing medical images within IoMT systems, several challenges persist. These challenges include high computational complexity, efficiency trade-offs, integration difficulties, scalability issues, and real-time constraints. Additionally, the high computational complexity of several models cited in the literature has been observed. Our brief review of recently proposed crypto-compression schemes for securing medical images in the IoT environment highlights the need to reduce computational costs to effectively address key security concerns.

2.2. Proposed solution

To address the current issue identified in the existing works, we propose a novel approach that combines Elliptic Curve Cryptography, Piecewise Linear Chaotic Map, and Discrete Wavelet Transform compression to secure medical images in IoMT systems. Recently, ECC has been considered one of the most promising technologies for IoT devices with limited resources due to its high security with shorter keys, lower computational requirements, reduced memory usage, energy efficiency, and scalability. Many recent image encryption methods rely on dynamic S-boxes [20]. The focus of the proposed research is to use the ECC mechanism and PWLCM to produce the dynamic SBox and keys. Then, the plain image is compressed using the Discrete Wavelet Transform (DWT) technique and Vector Quantization (VQ). Subsequently, the compressed image is encrypted using the AES Algorithm.

3. Preliminaries

In this section, we provide some basic details related to Elliptic curve cryptography, PWLCM, and DWT technique.

3.1. Theory of elliptic curve

Let F_p be a prime field of characteristics different from 2 and 3.

An elliptic curve E over this field is the set of points defined by the form:

(1) $$E=\{\Omega\}\cup\{(x, y) \in F_p\times F_p / y^2 = (x^3 + ax+b)(\text{mod } p)\},$$

where $a, b \in F_p$, $p \neq 2, 3$, and satisfy $\Delta = 4a^3 + 27b^2 \neq 0(\text{mod } p)$ and is the point at infinity.

The set $E(F_p)$ consists of all points (x, y) that satisfy the elliptic curve E along with a point at infinity Ω.

Theorem 1. The properties of addition law on elliptic curves:

a. Identity law: $M + \Omega = \Omega + M = M$ for every $M \in E$,

b. Inverse law: $M + (-M) = \Omega$ for every $M \in E$,

c. Associative law: $(M + N) + R = M + (N + R)$ for all $M, N, R \in E$,

d. Commutative law: $M + N = N + M$ for all $M, N \in E$,

Theorem 2. Algorithm of the elliptic curve addition and the multiplication.

Let E: $y^2 = x^3 + ax + b$ be an elliptic curve and let $M= (x_1, y_1)$ and $N = (x_2, y_2)$ be points on E, where $M \neq N$ and k is an integer.

Adding the two points M and N gives a point R that should lie on the same curve E,

$$R = M + N =(x_3, y_3),$$

where

$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } M \neq N, \\ \frac{3x_1^2+a}{2a} & \text{if } M = N. \end{cases}$$

The scalar multiplication kM is the addition of the point $M = (x_M, y_M)$ to itself k times, which can be written as

$$kM = M + \ldots + M \ (k \text{ times}).$$

ECC is considered one of the most promising technologies for IoT devices with limited resources due to its high security with shorter keys, lower computational requirements, reduced memory usage, energy efficiency, and scalability [21].

3.2. PWLCM: Piecewise linear chaotic map

The Piecewise Linear Chaotic Map (PWLCM) is a type of chaotic system characterized by its piecewise linear nature. It is employed in a variety of applications, such as cryptography and image processing, due to its ability to produce complex, unpredictable behavior from simple, linear rules [22]. The mathematical expression for the PWLCM is given as follows equation

$$x_{n+1} = \begin{cases} \frac{x_n}{\mu} & \text{if } x_n < \mu, \\ \frac{I - x_n}{1 - \mu} & \text{if } x_n \geq \mu, \end{cases}$$

where μ is a parameter of the system that controls the behavior of the map, typically $0<\mu<1$.

3.3. DWT (Discrete Wavelet Transform)

DWT is a mathematical technique utilized in signal processing and image compression. It converts a signal from the time domain to the frequency domain, facilitating multi-resolution analysis. It decomposes a signal into wavelet components, where large wavelets capture broad features and small wavelets capture fine details. This technique is widely used in image compression due to its ability to represent image data efficiently and effectively [23]. So, it can provide high compression ratios while preserving image quality, making it a powerful tool in various image compression applications.

4. Methodology

The emergence of new technologies like IoMT without addressing security concerns can leave users exposed to threats and vulnerabilities. Most health centers use IoMT for the exchange of medical images, but patient privacy cannot be guaranteed for these images inside these settings. Therefore, securing medical images in IoMT systems is a great challenge for the protection of medical privacy. Although various studies have shown that these approaches provide better security features, there is still scope to improve the previous methods. In this research, we propose a Lightweight crypto-compression scheme for securing medical images as shown in Fig. 1. A lightweight crypto-compression scheme refers to a method that combines cryptographic algorithms with data compression techniques, specifically crafted to function efficiently and securely on devices or platforms with constrained resources. This algorithm integrates elliptic curves, Advanced Encryption Standard (AES), and PWLCM to create a secure image encryption system. It consists of three main phases: Generation of a Dynamic S-Box and keys, Image Compression, and Encryption with AES.

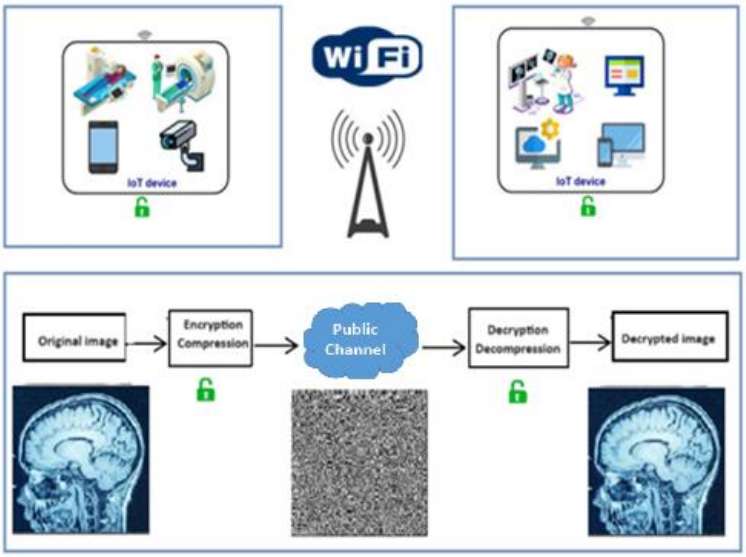

Fig. 1. Proposed IoT framework

Each phase is crucial for ensuring the security and efficiency of the image encryption process.

4.1. Generation of a dynamic S-Box and keys using ECC and PWLCM

This phase focuses on creating a dynamic substitution box (S-Box) and cryptographic keys essential for AES encryption. The S-Box is generated using the combined properties of elliptic curves and PWLCM to ensure high non-linearity, unpredictability, and cryptographic strength. The keys are generated solely using elliptic curve cryptography, leveraging the mathematical complexity of elliptic curves for secure key exchange and encryption.

1) Elliptic curve point generation:
- Choose a prime p and define the elliptic curve equation

$$E: y^2 = (x^3 + ax + b) \bmod \{p\};$$

- Compute points on the elliptic curve for each x in the range $[0,\ p-1\ ]$;
- Collect valid (x, y) pairs ensuring at least n^2 distinct points.

2) Generate public and private keys using ECC:
- Select a base point on the elliptic curve;
- Compute the public and private keys using ECC algorithms, which are essential for secure key exchange and encryption.

3) Generate chaotic sequence using PWLCM:
- Set chaotic map parameters μ and initial value x_0;

$$x_0 = \text{hash}(\text{secret\_key}) \bmod 1;$$

$$\mu = \text{some}_{\text{function}(\text{secret}_{\text{key}})};$$

- Apply the PWLCM formula (Equation (1)) to generate a chaotic sequence.

4) Reorder elliptic curve points using chaotic sequence:
- Normalize chaotic values to indices for sorting;
- Reorder elliptic curve points based on these indices.

5) Construct the *n*×*n* S-Box:
- Extract n^2 unique values from the reordered points;
- Arrange these values into a *n*×*n* matrix to form the S-Box.

4.2. Image compression

This phase compresses the image data to reduce its size before encryption, using DWT and VQ.

1) Transformation of medical image into matrix:
- Convert the medical image into a matrix form suitable for processing.

2) Apply DWT:
- Perform DWT on the image to decompose it into subbands: LL, LH, HL, and HH.

3) Perform VQ:
- Apply VQ [24] to the DWT coefficients;
- Encode the quantized coefficients for compression.

4.3. Encryption with AES

This phase encrypts the compressed image using AES, utilizing the dynamically generated S-Box to enhance security.

1) Initialize AES
- Set up the AES encryption algorithm using the dynamic S-Box.

2) Encrypt data
- Encrypt the compressed image data with AES.

The pseudo-code for the crypto-compression system is given in Algorithm 1, including three functions.

Algorithm 1. **Global Crypto-Compression Algorithm**
Input: Medical image
Output: ENCImag
Begin
Generate_DynamicSBox_Keys()
CImag ← Compress_Image_DWT_VQ (image)
ENCImag ← Encrypt_Compress_Image (CImag)
return ENCImag
End Algorithm
Function Generate_DynamicSBox_Keys
Input: *p*, *a*, *b*
Output: sbox, publicKey, privateKey
Begin
for *x* from 0 to *p*–1 do
$y^2 \leftarrow (x^3 + a*x + b) \bmod p$
y ← FindValidY(y^2, *p*)
if *y* exists **then**
ellipticCurvePoints ← ellipticCurvePoints + (*x*, *y*)
end if
end for
basePoint ← SelectBasePoint(ellipticCurvePoints)
privateKey ← GeneratePrivateKey()
publicKey ← GeneratePublicKey(basePoint, privateKey)
x_0 ← hash(secret_key)mod1
μ ← some_function(secret_key)
chaoticSequence ← [ ]
$x \leftarrow x_0$
for i **from** 1 **to** *N* **do**
if $x < \mu$ **then**
$x \leftarrow x / \mu$
else
$x \leftarrow (1 - x) / (1 - \mu)$
end if
chaoticSequence ← chaoticSequence + *x*
end for

```
        indices ← NormalizeChaoticSequence(chaoticSequence,
length(ellipticCurvePoints))
        reorderedPoints ← [ ]
        for i from 1 to length(indices) do
          reorderedPoints ← reorderedPoints + ellipticCurvePoints[indices[i]]
        end for
        sbox ← [ ]
        for i from 1 to n^2 do
          sbox ← sbox + reorderedPoints[i]
        end for
        sbox ← ReshapeToMatrix(sbox, n, n)
        return sbox, publicKey, privateKey
      End Function
      Function CompressImage_DWT_VQ
      Input: Image
      Output: Compressed image
      Begin
        Imag_Matrix ← TransformImageToMatrix(Image)
        dwtCoefficients ← ApplyDWT(imag_Matrix)
        CImag ← ApplyVectorQuantization (dwtCoefficients)
        return CImag
      End Function
      Function Encrypt_Compress_Image
      Input: CImage
      Output: ENCImage
      Begin
        aes ← InitializeAES(sbox)
       ENCImage ← AES_Encrypt (aes, CImage)
       return ENCImage
      End Function
```

5. Simulation results

In this research, our most significant contribution is to suggest a new lightweight crypto-compression technique for providing security, and confidentiality and optimizing encryption cost by combining ECC with the DWT technique in an IoT environment. This section presents a detailed simulation analysis conducted to validate the effectiveness of the proposed model. Several simulations have been conducted on a wide variety of medical images to ensure that our method is protected against known attacks. This includes images from X-ray imaging, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and other types.

After executing this algorithm on several medical images (10 images), we observe that the encrypted images appear completely scrambled as shown in Figs 2 and 3. This indicates that the encryption process has successfully disrupted the pixel arrangement of the original images, making any visual information indiscernible. In

terms of security, this means that the encrypted images do not convey any clear data, which is a strong indicator of the encryption algorithm's robustness.

The medical images used in this paper were obtained from the DICOM Library: **https://www.dicomlibrary.com/**.

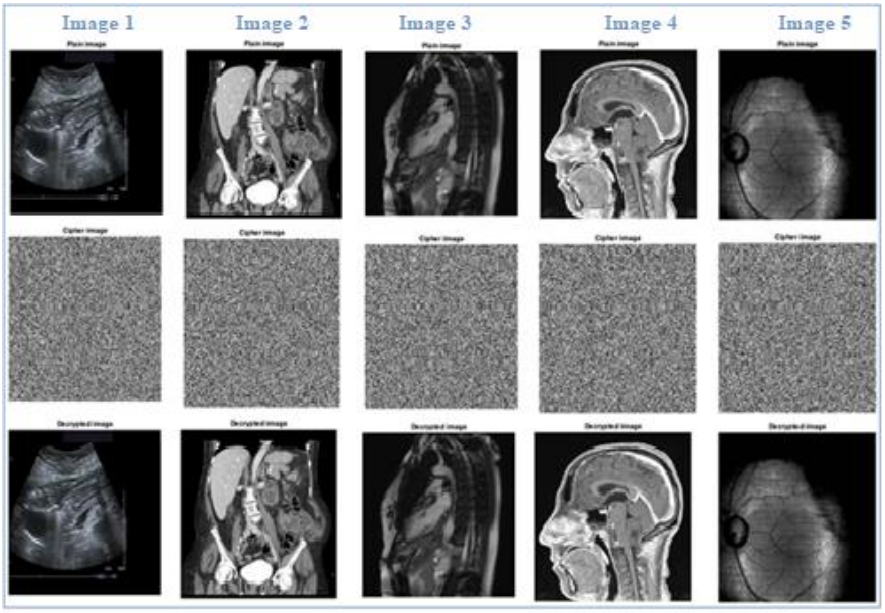

Fig. 2. Simulation results of plain, encrypted, and decrypted images for Image 1 to Image 5

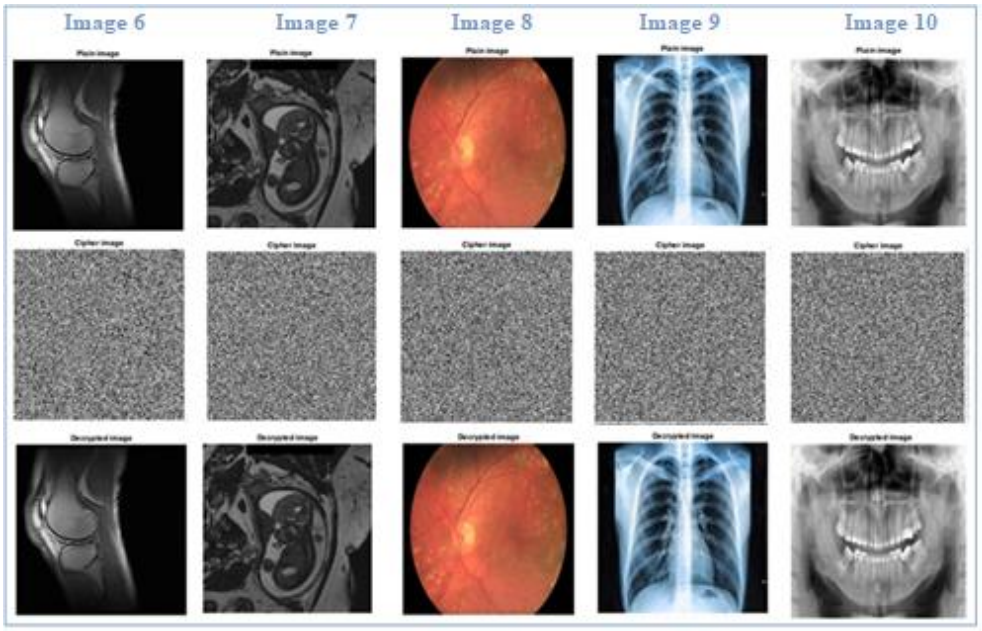

Fig. 3. Simulation results of plain, encrypted, and decrypted images for Image 6 to Image 10

6. Performance analysis

The efficiency of the proposed method is evaluated using a range of security analyses, such as histogram, correlation, and entropy.

6.1. Histogram analysis

The histogram of the original image displays the statistical distribution of the values of each pixel. For the plain image, this distribution is generally quite irregular and spread out because of the vast amount of information present in the plain image. The distribution of pixel values in encrypted images should follow a relatively uniform pattern to thwart attackers from deciphering the grayscale distribution of pixels by analyzing the histogram of the encrypted images. Fig. 4 displays the histograms of the plain image and the cipher image. The most effective defense against a cipher attack is to ensure that the histogram distribution of the encrypted image is highly uniform, making it difficult for external parties to extract the original information from the encrypted image through cipher analysis.

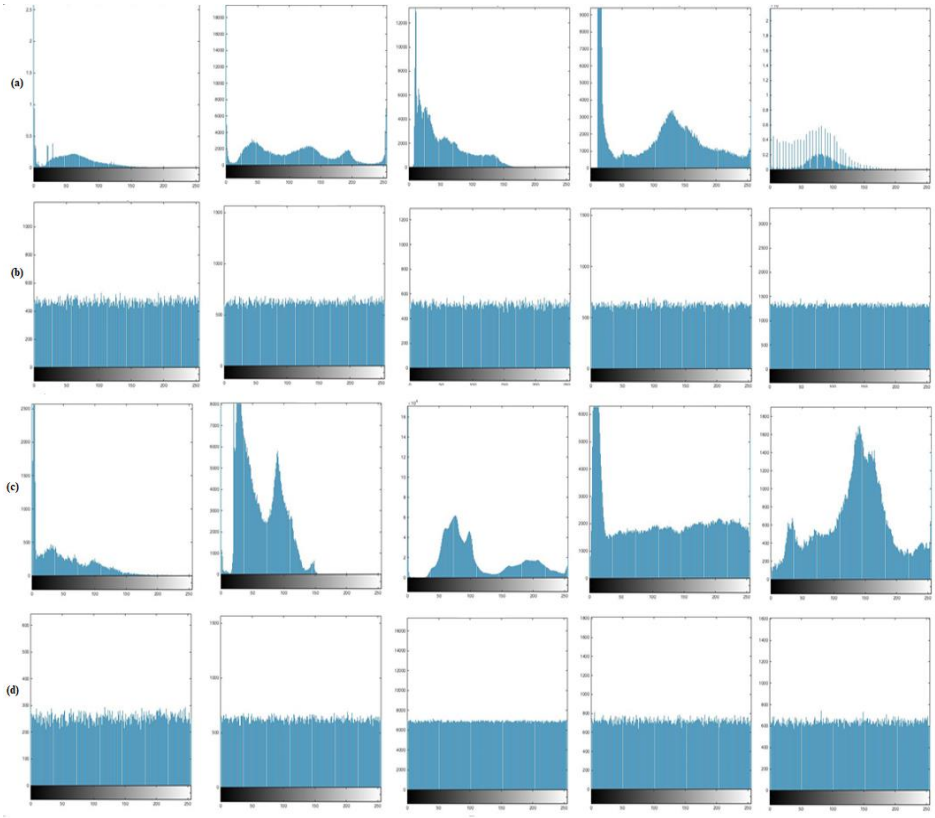

Fig. 4. Histogram of the original image (a), (c) and encrypted image (b), (d) for the ten images, respectively

The histogram analysis of the encrypted images shows a uniform distribution of pixel intensities as shown in Fig. 4(b), (d). Unlike the original images (Fig. 4 (a), (c)),

whose histograms typically display peaks and valleys corresponding to intensity variations and visual details, the histograms of the encrypted images exhibit a flat and homogeneous distribution. This uniformity suggests that the pixel values have been spread out in a manner that eliminates any recognizable structure or pattern, further underscoring the effectiveness of the encryption. From the findings, these plots indicate the histogram of the cipher image is more evenly distributed than that of the original image.

6.2. Pixel correlation analysis

We calculated the correlation coefficients for horizontal, vertical, and diagonal adjacent pixels for both the plain and cipher images. The results in Table 2 indicate a stark contrast between the plain and encrypted images. The plain images exhibit high correlation coefficients, reflecting the natural continuity and predictable structure of pixel values. For instance, Image 3 shows correlation coefficients of 0.9851 (horizontal), 0.9799 (diagonal), and 0.9926 (vertical). In contrast, the encrypted images display correlation coefficients close to zero, such as –0.0026 (horizontal), –0.0016 (diagonal), and 0.1010 (vertical) for Image 3, indicating that the encryption algorithm effectively disrupts the pixel relationships, resulting in an image that appears random.

Table 2. Correlation coefficients among fifteen images

Image	Plain image			Cipher image		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Image 1	0.9819	0.9403	0.9521	0.0063	0.0024	0.0072
Image 2	0.9807	0.9712	0.9881	–0.0020	0.0037	0.0019
Image 3	0.9851	0.9799	0.9926	–0.0026	–0.0016	0.1010
Image 4	0.9812	0.9656	0.9787	0.0044	-8.2927×10^{-4}	0.0716
Image 5	0.9732	0.9565	0.9763	-7.1979×10^{-4}	0.0019	0.0470
Image 6	0.9868	0.9781	0.9892	0.0039	-9.2496×10^{-4}	0.0553
Image 7	0.9808	0.9693	0.9839	–0.0036	0.0021	0.0236
Image 8	0.9990	0.9987	0.9992	-6.0331×10^{-4}	-8.7834×10^{-4}	–0.0039
Image 9	0.9908	0.9880	0.9942	0.0023	–0.0013	0.0363
Image 10	0.9870	0.9832	0.9952	–0.0047	1.8425×10^{-4}	0.0310

We also plotted the correlation distributions of adjacent pixels for plain Image 3 and its cipher image along horizontal, vertical, and diagonal directions (Fig. 5).

The plain image plots show a strong linear relationship between adjacent pixels, highlighting high correlation and continuity. However, the plots for the cipher image display a random scatter of points, with no discernible pattern, demonstrating that the encryption process successfully removes the correlation between adjacent pixels in all directions.

Additionally, we plotted the normalized cross-correlation for plain Image 3 and its cipher image (Fig. 6). The normalized cross-correlation plot for the plain image shows high values, indicating strong similarity between adjacent pixel values. Conversely, the normalized cross-correlation plot for the cipher image exhibits low

values, signifying that the encrypted image has little to no similarity between adjacent pixels. This low similarity confirms the encryption algorithm's effectiveness in disrupting pixel relationships and rendering the encrypted image data random and secure.

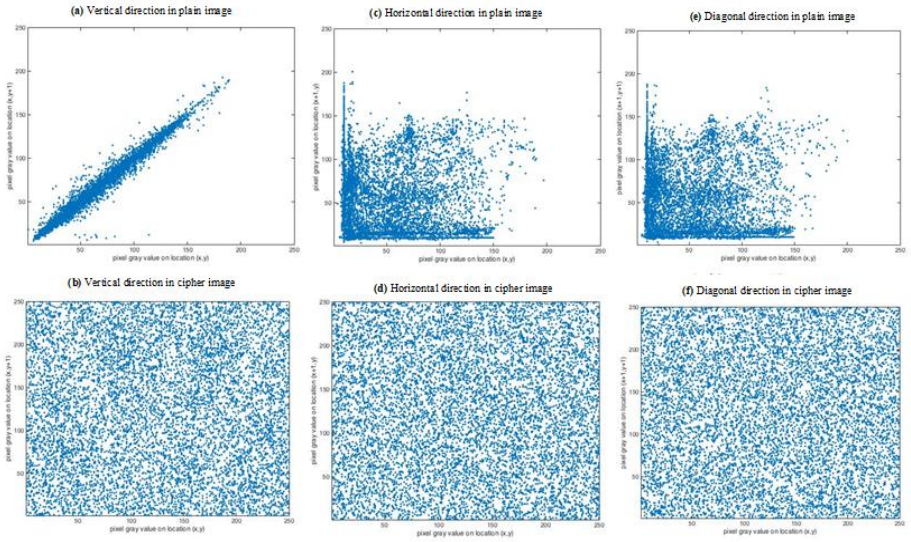

Fig. 5. Plot of correlation of Image 3

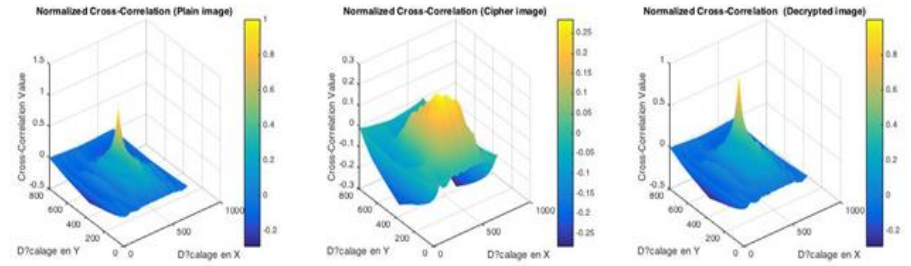

Fig. 6. Plot of normalized cross-correlation of Image 3

6.3. Key sensitivity analysis

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Change Intensity) are key metrics used in image encryption to measure the sensitivity of the encryption algorithm to slight changes in the plaintext image. These metrics are crucial for evaluating the strength of cryptographic algorithms, particularly their resistance to differential attacks. NPCR evaluates the degree of variation in pixel values, aiming for an optimal target of 100%. A value nearing 100% indicates a greater disparity between cipher images generated by the encryption algorithm when there are slight variations in the plain images. UACI, which measures the average intensity of these variations in a normalized manner, evaluates the average change density between different cipher images. A value near 33.3333% indicates a stronger

resistance of the algorithm to differential attacks. These metrics are calculated as follows [25]:

$$\text{NPCR} = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} \delta_{ij},$$

$$\text{UACI} = \frac{1}{255 \times N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} |E_{ij} - F_{ij}|.$$

The parameters *M* and *N* refer to the image's width and height and δi,j represents the change in pixel intensity at the coordinates (*i*, *j*); $E_{i,j}$ represents the pixel value of the original image at coordinates (*i*, *j*), whereas $F_{i,j}$ denotes the pixel value of the encrypted image at the same coordinates.

In this study, we evaluate the effectiveness of our proposed algorithm in resisting differential attacks by examining the NPCR and UACI values between two encrypted images, as shown in Table 3. The values are near the ideal values, indicating that our algorithm is highly effective at resisting differential attacks.

PSNR and MSE are two metrics that can help evaluate the impact of key changes on image quality. PSNR and MSE between two images are evaluated by the following equations:

$$\text{MSE} = \frac{1}{uv} \sum_{x=1}^{u} \sum_{y=1}^{v} [I(x,y) - \hat{I}(x,y)]^2,$$

$$\text{PSNR} = 10 \log_2 \frac{255^2}{\text{MSE}},$$

where $I(x, y)$ and $\hat{I}(x, y)$ represent two images, and *u* and *v* denote the number of pixels in the frame. A lower PSNR value indicates that the encryption is stronger.

Table 3. Evaluation of key sensitivity based on NPCR, UACI, and PSNR

Image No	NPCR	UACI	PSNR
Image 1	0.9963	0.4161	6.0238
Image 2	0.9961	0.3695	6.9223
Image 3	0.9961	0.3777	6.7478
Image 4	0.9961	0.3452	7.4780
Image 5	0.9961	0.3617	7.0936
Image 6	0.9962	0.4143	6.0575
Image 7	0.9961	0.3380	7.6564
Image 8	0.9984	0.3077	8.5082
Image 9	0.9960	0.3457	7.4690
Image 10	0.9961	0.3031	8.6486

From Table 3 the findings are:

- NPCR values are very high (0.9960 to 0.9963), indicating that the encryption method effectively changes a large portion of the image pixels, enhancing security.
- UACI values range from 0.3031 to 0.4476, showing significant changes in pixel intensity, which contributes to the randomness of the encrypted images.
- PSNR values are relatively low (5.5068-8.6486), suggesting that while the encryption strengthens security, it also introduces noticeable distortion in the images.

These results suggest that the encryption method effectively improves security by altering pixel values and intensities, although it does result in some degradation of image quality.

6.4. Information entropy analysis

Entropy is a measure of randomness or unpredictability in an image. Higher entropy values indicate greater complexity and less predictability. In the context of image encryption, an effective encryption algorithm should significantly increase the entropy of the original image, making the encrypted image appear random and resistant to statistical attacks.

Table 4 shows the entropy values for both plain (original) images and their corresponding cipher (encrypted) images. The results indicate a notable increase in entropy after encryption. The entropy of the original images ranges from 4.0667 up to 7.1786, whereas the entropy of the ciphered images is consistently high, between 7.9967 and 7.9995. This significant increase demonstrates that the encryption algorithm has effectively enhanced the randomness and complexity of the images, making them much more resistant to analysis and attacks.

Table 4. Information entropy of ten images

Image No	Plain image	Cipher image
Image 1	4.6989	7.9981
Image 2	6.5656	7.9987
Image 3	6.1294	7.9985
Image 4	7.1786	7.9989
Image 5	6.3576	7.9987
Image 6	5.7881	7.9967
Image 7	6.7031	7.9988
Image 8	6.6641	7.9999
Image 9	7.7978	7.9989
Image 10	7.7339	7.9989

6.5. Comparison and discussion

This section provides a comprehensive assessment that compares the proposed solution with some existing methods, emphasizing security aspects. Here, the proposed scheme is evaluated by using different metrics like information entropy, NPCR, and UACI. As a result, our scheme demonstrates better performance, as illustrated in Table 5.

Table 5. Comparison of the proposed scheme with the latest existing methods

Metric	[26]	[27]	[28]	[29]	Proposed method
NPCR	99.6208	99,64	0.9961	0.9982	0.9984
UACI	0.3341	0.4156	0.3346	03351	0.3380
Entropy	7.9970	7.9980	7.9973	7.90	7.9999

In summary, our solution presents a distinct advantage over others by combining the security and efficiency of ECC with the lightweight, adaptable encryption capabilities of chaos theory, specifically the PWLCM. This method enables robust security with minimal computational overhead, which is ideal for resource-constrained IoT devices in the IoMT environment. Additionally, our integration of Wavelet Transform and Vector Quantization not only compresses data before encryption enhancing transmission speed and reducing latency, but also preserves the quality of medical images for accurate diagnostics. These features collectively result in a faster, more efficient, and highly secure solution compared to existing methods, making our solution a valuable contribution to secure healthcare technology.

7. Conclusion

Research on the benefits of the Internet of Medical Things is heavily focused on healthcare settings, including hospitals. Implementing advanced cryptographic solutions in existing hospital systems can be complex and resource-intensive. This study proposes a novel approach for securing medical images within the IoT ecosystem, addressing the critical need for enhanced security measures in the transmission and storage of sensitive medical data. The key contribution of this study is the generation of dynamic S-box and keys using Elliptic Curve Cryptography and Piecewise Linear Chaotic Map. The scheme utilizes a dynamic S-box to introduce variability and complexity, thereby strengthening resistance to attacks and boosting overall security. Additionally, our approach utilizes the DWT technique and Vector Quantization for compression purposes and follows this, employs an AES-based encryption algorithm for securing medical images. Objective metrics like entropy and histogram analysis, as well as NPCR, UACI and PSNR, reveal the effectiveness of our method in resisting statistical, differential, and ciphertext attacks. The simulation results confirm that the proposed approach delivers improved security and reliable performance. As a future work, we can extend the proposed approach to other IoT applications beyond healthcare, evaluating its effectiveness in securing data across various domains. We also intend to explore the integration of this approach with emerging technologies, such as artificial intelligence, to enhance real-time data security and optimize performance. The integration of IA techniques is an interesting challenge that may be the subject of future research.

References

1. Sudha, K. S., N. Jeyanthi. A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT). – Cybernetics and Information Technologies, Vol. **21**, 2021, No 3, pp. 50-72.
2. Rehman, M. U., et al. A Novel Medical Image Data Protection Scheme for Smart Healthcare System. – CAAI Transactions on Intelligence Technology, 2024.
3. Swati, J., P. Nitin. Securing Decentralized Storage in Blockchain: A Hybrid Cryptographic Framework. – Cybernetics and Information Technologies, Vol. **24**, 2024, No 2, pp. 16-31.
4. Singh, P., A. K. Singh. A Survey of Image Encryption for Healthcare Applications. – Evolutionary Intelligence, Vol. **16**, 2023, No 3, pp. 801-818.
5. Suryateja, P. S., K. Venkata Rao. A Survey on Lightweight Cryptographic Algorithms in IoT. – Cybernetics and Information Technologies, Vol. **24**, 2024, No 1, pp. 21-34.
6. Li, Chunyan, et al. A Review of IoT Applications in Healthcare. – Neurocomputing, Vol. **565**, 2023, pp. 127017.
7. Anand, A., et al. Compression-Then-Encryption-Based Secure Watermarking Technique for Smart Healthcare System. – In: IEEE MultiMedia, Vol. **27**, 2020, No 4, pp. 133-143.
8. Pooranakala, K., V. Jaitly. Securing Medical Images Using Compression Techniques with Encryption and Image Steganography. – In: 3rd International Conference on Intelligent Technologies (CONIT'23), IEEE, 2023, pp. 1-7.
9. Saber, H. K., M. A. Shakir. A Review on Medical Image Compression and Encryption Using Compressive Sensing. – In: Proc. of 2022 International Conference on Computer Science and Software Engineering (CSASE'22), IEEE, 2022, pp. 312-318.
10. Cao, Weijia, et al. A Joint Encryption and Compression Algorithm for Multiband Remote Sensing Image Transmission. – Sensors, Vol. **23**, 2023, No 17, 7600.

11. K a n s h i, A., R. S o u n d r a p a n d i y a n, V. S. A n i t a S o f i a, V. R. R a j a s e k a r. Hybridized Cryptographic Encryption and Decryption Using Advanced Encryption Standard and Data Encryption Standard. – Cybernetics and Information Technologies, Vol. **23**, 2023, No 4, pp. 63-78.
12. R a n j a n, K. H. S., S. S. P. F a t h i m a t h, G. A i t h a l, S. S h e t t y. A Survey on Key(s) and Keyless Image Encryption Techniques. – Cybernetics and Information Technologies, Vol. **17**, 2017, No 4, pp. 134-164.
13. L i, N a n, et al. A Review of Security Issues and Solutions for Precision Health in Internet-of-Medical-Things Systems. – Security and Safety, Vol. **2**, 2023, 2022010.
14. L a t a, K., L. R. C e n k e r a m a d d i. Deep Learning for Medical Image Cryptography: A Comprehensive Review. – Applied Sciences, Vol. **13**, 2023, No 14, 8295.
15. R a j e n d r a n, S., M. D o r a i p a n d i a n. Chaos Based Secure Medical Image Transmission Model for IoT-Powered Healthcare Systems. – In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2021, 012106.
16. H a j j a j i, M. A., M., D r i d i, A. M t i b a a. A Medical Image Crypto-Compression Algorithm Based on Neural Network and PWLCM. – Multimedia Tools and Applications, Vol. **78**, 2019, pp. 14379-14396.
17. M a s h a t, A., S. B h a t i a, A. K u m a r et al. Medical Image Transmission Using Novel Crypto-Compression Scheme. – Intelligent Automation & Soft Computing, Vol. **32**, 2022, No 2.
18. P o o r a n a k a l a, K., V. J a i t l y. Securing Medical Images Using Compression Techniques with Encryption and Image Steganography. – In: Proc. of 3rd International Conference on Intelligent Technologies (CONIT'23), IEEE, 2023. pp. 1-7.
19. U n g u r e a n u, V. I., et al. Image-Compression Techniques: Classical and Region-of-Interest-Based Approaches Presented in Recent Papers. – Sensors, Vol. **24**, 2024, No 3, 791.
20. I b r a h i m, S., A. A l h a r b i. Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography. – IEEE Access, Vol. **8**, 2020, pp. 194289-194302.
21. F r a n c i a, A. S., et al. Elliptic Curves Cryptography for Lightweight Devices in IoT Systems. – Emerging Research in Intelligent Systems: Proceedings of the CIT 2021, Volume 1, Vol. **405**, 2022, pp. 71.
22. Y a d a v, A. B., et al. A Joint Medical Image Compression and Encryption Using AMBTC and Hybrid Chaotic System. – Journal of Discrete Mathematical Sciences and Cryptography, Vol. **24**, 2021, No 8, pp. 2233-2244.
23. A b d m o u l e h, M. K., et al. Crypto-Compression Scheme Based on the DWT for Medical Image Security. – International Journal of Computational Vision and Robotics, Vol. **9**, 2019, No 4, pp. 340-350.
24. A m m a h, P. N. T., E. O w u s u O w u s u. Robust Medical Image Compression Based on Wavelet Transform and Vector Quantization. – Informatics in Medicine Unlocked, Vol. **15**, 2019, 100183.
25. L e i, Z., et al. Color Image Encryption Based on a Novel Fourth-Direction Hyperchaotic System. – Electronics, Vol. **13**, 2024, No 12, 2229.
26. L i, X i n s h e n g, et al. Joint Image Compression and Encryption Based on Sparse Bayesian Learning and Bit-Level 3D Arnold Cat Maps. – PLoS One, Vol. **14**, 2019, No 11, e0224382.
27. H a s h i m, A. T., et al. Medical Image Encryption Based on Hybrid AES with Chaotic Map. – In: Journal of Physics: Conference Series. IOP Publishing, 2021, 012037.
28. M a n, Z., et al. Medical Image Encryption Scheme Based on Self-Verification Matrix. – IET Image Processing, Vol. **15**, 2021, No 12, pp. 2787-2798.
29. K a d h i m, A. J., S. T a y s e e r A t i a. Quantum Encryption of Healthcare Images: Enhancing Security and Confidentiality in e-Health Systems. – Security and Privacy, 2024, e391.

Received: 14.08.2024; Second version: 08.10.2024; Third version 17.10.2024; Accepted: 01.11.2024