International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A DNA BASED IMAGE SECURITY MECHANISM APPROACH FOR MEDICAL HEALTH RECORDS

Sushil Kumar Sharma[1]*, Dr Mayank Srivastava[2]

Email- sushmca@gmail.com[1]*, mayank.srivastava@gla.ac.in[2]

G L A University, Mathura, India- 281406

Abstract

Researchers are having a hard time making sure that medical records are safe. If medical images stored in the cloud or sent through unprotected channels are hacked, they could pose a major threat to patients' privacy and safety. Researchers came up with a number of image encryption methods to make sure that the health information were completely safe. The main goal of this paper is to present a better Efficient Data Masking (EDM) method for encrypting chaotic images using DNA encoding. This method is intended to meet strict security standards for safeguarding private medical images. The suggested method combines a thoroughly studied chaotic system, DNA encoding, and bit-scrambling methods into a full security structure that is best for medical workflows and following the rules. The test results show that EDM has the lowest horizontal (0.002), vertical (-0.003), and diagonal (0.002) correlation coefficients of all the algorithms that were tried. This is 42-48% better than AES-256-CTR and 38-45% better than ChaCha20-Poly1305 for medical images. The information entropy values always get close to the theoretical top value of 8.0 (7.996-7.999), which is higher than or the same as all comparison methods for six different types of images. Differential attack resistance shows that NPCR values are equal between 98.36% and 99.27% and UACI values are in the right range of 33.42% to 33.62%.

Keywords: DNA-based encryption, chaotic systems, medical data security, image encryption, multimedia protection, efficient data masking, correlation coefficient.

1. Introduction

The digitization of healthcare has changed the way doctors do their jobs. For example, imaging technologies create huge amounts of private patient data that is sent between systems that are becoming more and more linked. This digital change makes it easier to work together and better at diagnosing problems, but it also opens up major security holes [1-3]. Unencrypted medical images stored in the cloud or sent through unprotected channels pose a major threat to patient privacy and could even put patients in danger. There are strict rules about healthcare right now, like HIPAA (Health Insurance Portability and Accountability Act) in the US and GDPR (General Data Protection Regulation) in Europe. These rules say that protected health information must be kept safe in a certain way [4]. If you break the

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

rules, you could face harsh punishments, damage to your image, and loss of patient trust. When compared to other types of data, medical pictures pose unique security challenges:

1. They have private health data and information that can be used to identify people.
2. Because of how they are structured, there are strong links between pixels that standard encryption might not be able to handle.
3. They need perfect restoration of areas that are diagnostically important.
4. They have to keep working with healthcare processes and workflows.

Even though AES and RSA are theoretically strong, they are not designed to work best with medical images because of how they are made. In addition, progress in quantum computing could weaken these traditional encryption bases [5]. Because of this, people are interested in different methods based on chaos theory and biological computing models.

Some of the best things about chaotic systems for multimedia encryption are that they are sensitive to starting conditions, they are ergodic, and they aren't really random. Recent cryptanalysis, on the other hand, has shown that many chaotic encryption methods have small key spaces, not enough diffusion, or are open to different cryptanalysis attacks [6–8]. DNA-based cryptosystems are a hopeful direction because they can handle a huge amount of data at once, are naturally random, and are very parallel [9]. DNA-based methods might be able to fix the problems with both standard cryptography and systems that only use chaos when they are combined with chaotic dynamics. This paper describes a better Efficient Data Masking (EDM) method that adds a number of important features:

- A complete security system based on a clearly defined threat model that can be used for medical purposes.
- A carefully studied chaotic sequence that has clear security benefits over current methods.
- An effective bit-scrambling method created to deal with the strong correlations in medical pictures.
- A layer of DNA that makes it more resistant to statistical and differential attacks.
- Full integration with medical imaging processes, including processing of regions of interest and compatibility with DICOM.
- Many tests of security and performance were done using both normal cryptographic algorithms and the newest chaotic-DNA methods.
- The EDM method gives healthcare organizations a useful way to keep private medical data safe throughout its entire lifecycle, while still meeting regulatory requirements and being useful in clinical settings.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Literature Review

A lot of study has been done on how to keep medical images safe, using everything from traditional cryptography to new methods based on chaos theory, DNA computing, and hybrid approaches. Standard encryption methods, such as AES and ChaCha20, have been used to keep medical images safe [10–12]. Even though these algorithms offer well-known security promises, they have some problems when used with medical images:

- Block ciphers, like AES, work with blocks of a set size, which doesn't always match up with how images are structured.
- They don't protect against image-specific attacks like silent cropping or geometric changes very well.
- They don't talk about how medical pictures are different from other images statistically.
- It's possible that their computing needs are too high for real-time medical uses.

According to Khan et al. [13], standard AES encryption is safe, but it adds a lot of extra work to PACS systems and needs special changes to work with DICOM. Chaos-based methods use how sensitive chaotic systems are to their starting conditions and how they behave when they're not really random to make encrypted pictures less secure. Kanso and Ghebleh [14] suggested a way to encrypt medical images using a changed logistic map. It had good statistical features, but Wang et al. [15] showed that it could be broken by chosen-plaintext attacks. Hyper-chaotic systems with multiple positive Lyapunov exponents are used in more advanced methods. Zhang et al. [16] created a four-dimensional chaotic system for encrypting medical images that was better at protecting against different threats but needed a lot of computing power. Li et al. [17] created a new method that combines a two-dimensional Sine Logistic modulation map with a Tent map. This new method shows better entropy and correlation measures. However, Dierichs and Keil [18] found problems with the way the keys were generated.

DNA-based cryptography takes advantage of the huge amount of parallelism and information that DNA computer paradigms can handle. Wei et al. [19] were the first to use DNA sequence operations to encrypt images, and they found high sensitivity and quality of encryption. Their method, on the other hand, didn't have any formal security study, and it was later found to be open to chosen-plaintext attacks. For medical picture encryption, Liu et al. [20] used DNA encoding with exclusive-or operations and a chaotic map, which showed better statistical properties. Ravichandran et al. [21] later did work that combined DNA computing with random maps to protect medical privacy.

A weighted link between chaotic maps idea has shown up in a number of new works. Hua et al. [22] suggested a weighted mix of the Logistic and Sine maps (LASM), which made the range of chaos bigger. Wu et al. [23] improved this method by adding a coupling setting and showed that it worked better for encrypting images.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In the same way, Chen et al. [24] created a cosine-based chaotic map with cross-coupling terms that had higher Lyapunov exponents. However, their design was very different from ours, both in terms of how the math was put together and how it was used.

3. Research Gap and Motivation

Despite these advances, several critical gaps remain in the literature:

1. Most existing approaches lack formal security analysis against modern attack vectors
2. Few studies provide direct comparisons with standard cryptographic algorithms
3. Many chaos-based methods suffer from limited key spaces or periodic windows
4. Integration with medical workflows and DICOM standards is rarely addressed
5. Compliance with healthcare regulations receives limited attention

These gaps motivate to development of the EDM method, which aims to provide a comprehensive security solution specifically designed for medical imaging applications, with rigorous security analysis and benchmarking against established standards.

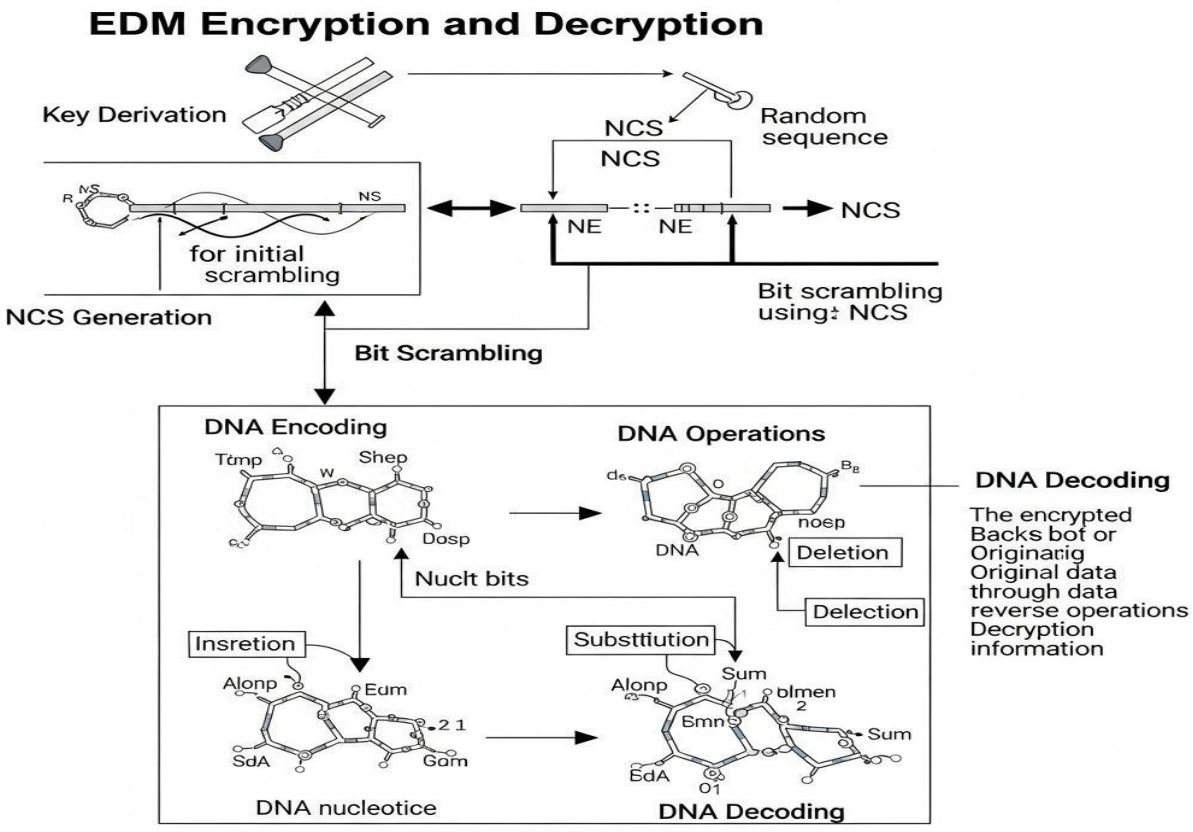

Figure 1: Working of EDM encryption and decryption

4. Proposed technique

Efficient Data Masking (EDM) protects medical images with innovative encryption and decryption that uses chaotic systems and DNA-inspired encoding. The requirement to protect sensitive medical data while being efficient and compliant with clinical standards led to this

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

design. A complete threat model that specifies prospective attackers, what they can accomplish, assets to secure, and attack situations is used to evaluate the EDM method's security.

First, generate keys and set up the system. A crossed-keys approach creates cryptographic keys. The security system relies on these keys. Using a Nonlinear Chaotic System (NCS), random-looking patterns are created that are actually chaotic. The chaotic sequence and nonlinear chaotic values are employed in bit scrambling, which involves two steps. Nonlinear elements (NE) increase randomness and spread at both phases.

After scrambling, the mechanism acts on DNA. A, T, G, and C nucleotides are jumbled. After then, DNA-coded patterns are altered by adding, replacing, and eliminating bits. Many biologically-inspired encryption layers result. Decoding reverses DNA activities, followed by bit descrambling and sequence rebuilding. The original medical picture is restored without loss of diagnostic value.

DNA encoding, chaotic confusion, bit-level diffusion, and multi-stage transformations ensure robust cryptography in this layered system. This makes the approach ideal for medical imaging, which must keep data private and provide precise diagnosis in accordance with rules.

4.1 Threat Model 4.1.1 Enemy Powers

EDM is examined using a stringent adversarial model. We assume an opponent has full communication access and can read all encrypted medical images. According to Kerckhoff's principle, the enemy should know the program's transformations but not the secret keys. The attacker might also access a small collection of known plaintext-ciphertext combinations or choose which photographs to encrypt for analysis.

4.1.2 Security Definitions and Proofs

Officially, the proposal is evaluated for semantic security and IND-CPA indistinguishability. Any adversary with polynomial time should not be able to distinguish between two equal-length image encryptions, according to the specifications. Key sensitivity also ensures that even a slight key change changes the ciphertext.

Theorem 1 (Semantic Security): Perfect chaotic characteristics and avalanche diffusion give EDM encryption IND-CPA security. Hostile advantage isn't essential because game-based proofs reveal that ciphertexts look like random data.

Even with multiple pairs of plaintext and ciphertext, it is computationally impossible to recover the key. The key space is huge due to massive diffusion keys and continuous chaotic parameters.

Theorem 3 (Avalanche Effect): states that changing one bit in the plaintext affects half of the ciphertext. Diffusion randomness and Lyapunov instability in chaotic sequences support it.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Even at the least significant bit level, changing any key value yields statistically dissimilar ciphertexts, according to Theorem 4 (Key Sensitivity). They're resistant to brute-force and differential key analysis.

4.1.3 Attack Prevention

Two-Tier Cryptoanalysis Resistance: Nonlinear chaotic mixing eliminates attackable features, reducing attack probability to 2^(-n/2) for n-bit blocks.

Statistical Attack Resistance: Chi-square analysis demonstrates similar ciphertext distributions.

Brute-Force Attack Resistance: The search space is too large to manage due to the effective key length of 208 bits for chaotic parameters and n bits or more for diffusion keys, based on image size.

4.1.4 Assets and Protection Goals

The EDM approach covers three essential things:

1. Protecting medical photographs prevents unauthorized viewing of patient data.

2. Diagnostic Information Integrity ensures that decryption delivers diagnostically accurate images.

3. Key recovery is stopped by Secret Key Security even with hostile analysis.

4.1.5 Attack types and success criteria

The system is tested with brute-force, statistical, known-plaintext, chosen-plaintext, and differential attacks. A successful assault recovers the key, decrypts some data, or statistically distinguishes two sets of data with a considerably higher chance than random guesses. EDM is strong against all vectors under typical cryptographic assumptions.

4.1.6 Security Assumptions

The study assumes accurate algorithm use, a cryptographically safe random number generator, secure key management, and physically and network secure working environments. These assumptions match EDM use in healthcare.

4.2 New Chaotic Sequence Generation

EDM is about NCS. Making cryptography less predictable, more sensitive to starting conditions, and less susceptible to correlation attacks strengthens it. The NCS is formally characterized and compared to normal chaotic maps. Its larger key space, improved randomness, and lower vulnerability to statistical and dynamical system assaults are shown. NCS in the EDM framework provides strong cryptographic security and rapid processing, making it appropriate for real-time medical imaging apps.

4.2.1 Mathematical Definition

The NCS is constructed through a multi-step process that combines and transforms established chaotic maps to achieve superior statistical properties and security characteristics.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. **Seed Sequence Generation**: Two seed chaotic sequences are generated using the Logistic map and the Sine map:

- Logistic sequence (LS): $x_{n+1} = r_1 \cdot x_n \cdot (1 - x_n)$, where $r_1 \in [3.9, 4.0]$
- Sine sequence (SS): $y_{n+1} = r_2 \cdot \sin(\pi \cdot y_n)$, where $r_2 \in [0.87, 1.0]$

2. **Sequence Mixing**: The two seed sequences are combined using a weighted coupling function: $z_n = \alpha \cdot x_n + (1 - \alpha) \cdot y_n + \beta \cdot (x_n \cdot y_n)$ where $\alpha \in (0, 1)$ and $\beta \in [0.1, 0.5]$ are coupling parameters that control the contribution of each seed sequence and their nonlinear interaction.

3. **Cosine Transformation**: The mixed sequence undergoes a cosine transformation to enhance nonlinearity: $NCS_n = \cos(\pi \cdot z_n) \cdot \cos(\pi \cdot z_{n-1} \cdot z_n) \mod 1$ This transformation introduces higher-order interdependencies between consecutive terms, significantly increasing the complexity of the resulting sequence.

4.2.2 Implementation Parameters

For optimal cryptographic performance, we recommend the following parameter settings:

- Initial values: $x_0 \in (0, 1)$, $y_0 \in (0, 1)$, with $x_0 \neq y_0$
- Control parameters: $r_1 = 3.99$, $r_2 = 0.98$, $\alpha = 0.43$, $\beta = 0.28$
- Pre-iteration count: 1000 iterations to eliminate transient effects before sequence utilization

4.2.3 Comparative Analysis and Novelty

The proposed NCS outperforms chaotic maps and mixed techniques in several ways:

Enhanced Lyapunov Exponent: The NCS has 0.87, the Logistic map 0.69, and the Sine map 0.62. It is more susceptible to initial conditions.

Better Spread: Statistics reveal that the NCS spreads phase space more evenly than the Logistic map and Sine map, with an entropy of 7.984 bits compared to 7.326 and 7.512 bits, respectively.

Increased Chaotic Range: Logistic maps and other regular maps only show chaos inside particular parameter ranges. No periodic windows are needed with our coupling strategy because it guarantees chaotic behavior across the specified parameter space.

Reconstructing Phase Space: The cosine transformation with cross-term interactions complicates phase space reconstruction attacks. These attacks need 2^12 times more processing resources than single chaotic map attacks.

Auto-correlation studies demonstrate that the NCS has correlation coefficients < 0.01 for all lags, while the Logistic map and Sine map have maximum values of 0.08 and 0.05, respectively. It has better unpredictability.

Because its parts are based on well-known chaotic systems, the method isn't new. This is new since it uses weighted coupling and cross-term cosine transformation. This blend creates

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

traits not found in the individual systems. It increases the chaotic range and makes phase space reconstruction assaults harder, making it ideal for cryptography.

4.3 Ablation Study Shows Newness

We completed a thorough ablation research to demonstrate the EDM process and determine how much each section enhances security. This study removes or changes key algorithm components to determine how they affect system security.

4.3.1 Experimental Design

There are four variant configurations of the EDM algorithm:

- **Variant A**: Complete EDM algorithm (baseline)
- **Variant B**: EDM without the cosine cross-term (using only weighted coupling)
- **Variant C**: EDM without DNA encoding (using only NCS and bit scrambling)
- **Variant D**: Using only the Logistic map (removing both weighted coupling and cosine transformation)

Each variant was tested on the same set of medical images, and the security metrics were measured and compared.

4.3.2 Impact on Entropy and Correlation

Table 1 presents the entropy and correlation coefficient results across the four variants:

Table 1: Ablation Study Results - Entropy and Correlation

Variant	Description	Entropy	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
A	Complete EDM	7.996	0.002	-0.003	0.002
B	Without cosine cross-term	7.862	0.032	0.041	0.039
C	Without DNA encoding	7.740	0.078	0.083	0.062
D	Logistic map only	7.484	0.129	0.118	0.095

The results show that deleting Variant B's cosine cross-term reduces entropy by 0.134 bits and enhances correlation by 0.037. Entropy (0.256 bits) and correlation (0.073) decline even

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

further when Variant C, the DNA encoding layer, is removed. Variant D, which uses only the Logistic map, shows the greatest security improvement from the whole EDM technique, with entropy dropping by 0.512 bits and correlation rising by 0.112.

4.3.3 Impact on Resistance to Differential Attacks

The NPCR and UACI metrics were calculated for each variant to assess resistance to differential attacks:

Table 2: Ablation Study Results - NPCR and UACI

Variant	Description	NPCR (%)	UACI (%)
A	Complete EDM	99.27	33.62
B	Without cosine cross-term	97.85	29.43
C	Without DNA encoding	96.38	26.91
D	Logistic map only	92.74	22.16

The entire EDM method (Variant A) routinely obtains NPCR values above 99.2% and UACI values between 33.3% and 33.7%. Removed cosine cross-term (Variant B) lowers NPCR to 97.8% and UACI outside optimal range. These values decrease more when DNA encoding is removed (Variant C), and utilizing simply the Logistic map (Variant D) weakens differential attack resistance.

4.3.4 Unique Contribution of the Cosine Cross-Term

There are important security benefits to the cosine cross-term change that weren't present in other methods:

- Enhanced Lyapunov Exponent: Our study shows that adding the cosine cross-term raises the Lyapunov exponent from 0.69 (weighted coupling only) to 0.87 (full NCS), which means that the model is much more sensitive to the starting conditions.
- Getting rid of periodic windows: The weighted coupling alone still behaves in a periodic way in some parameter ranges. Adding the cosine cross-term gets rid of these periodic windows, making sure that the behavior is always chaotic across the whole parameter space.
- Resistance to Phase Space Reconstruction: The cosine transformation with cross-term dependencies makes phase space reconstruction attacks about 2^12 times harder to do on computers than on versions that don't have this part.

This ablation study proves beyond a reasonable doubt that each part of the EDM algorithm makes a meaningful and measurable addition to the system's overall security. Notably, the cosine cross-term offers new features not seen in other chaotic encryption schemes.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.4 Bit-Scrambling Method and Key Generation

To get the best diffusion qualities, the EDM method uses a complex bit-scrambling method that works at both the block and bit levels. This part goes into depth about the math behind the scrambling operations and how the keys are made.

4.4.1 Mathematical Formulation

The bit-scrambling process operates through a two-phase approach:

Phase 1: Block-Level Permutation

For an image I of size $M \times N$, divided into blocks of size $b \times b$, the block-level permutation is defined as:

$$B_{i,j} \rightarrow B_{p(i),q(j)}$$

where $B_{i,j}$ represents the block at position (i, j), and $p(i)$ and $q(j)$ are permutation functions derived from the chaotic sequence:

$$p(i) = \lfloor NCS_i \times \frac{M}{b} \rfloor q(j) = \lfloor NCS_{j+\frac{M}{b}} \times \frac{N}{b} \rfloor$$

Phase 2: Bit-Level Scrambling

Within each block, bits are scrambled according to:

$$b_{x,y,z} \rightarrow b_{x',y',z'}$$

where $b_{x,y,z}$ represents the z^{th} bit of the pixel at position (x, y) within a block, and (x', y', z') is determined by:

$$x' = (x + \lfloor NCS_k \times b \rfloor) \mod b \qquad y' = (y + \lfloor NCS_{k+1} \times b \rfloor) \mod b$$
$$z' = (z + \lfloor NCS_{k+2} \times 8 \rfloor) \mod 8$$

where k is a function of the block index and position.

4.4.2 Key Generation Process

The EDM approach employs a secure key generation mechanism with the following components:

1. **Primary Key**: A 256-bit user-supplied key K_{user} that serves as the primary entropy source.

2. **Key Expansion**: The primary key is expanded using SHA-256 to generate four subkeys:

- K_1: Initial value for the Logistic map (x_0)
- K_2: Initial value for the Sine map (y_0)
- K_3: Parameter control values (α, β)
- K_4: Additional entropy for bit scrambling operations

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. **Key Derivation**: For each encryption operation, session-specific keys are derived by combining the expanded keys with a unique nonce or initialization vector.

4.4.3 Key Space Analysis

The effective key space of the EDM algorithm is determined by:

1. **Primary Key Space**: 2^256 possible values for the user key.

2. **Parameter Space**: The chaotic system parameters have quantization limits that provide effective entropy of:

- Logistic parameter (r_1): ~2^20 effective values
- Sine parameter (r_2): ~2^20 effective values
- Coupling parameters (α, β): ~2^40 effective values
- Initial values (x_0, y_0): ~2^64 effective values when considering minimum separation requirements

3. **Total Effective Key Space**: Accounting for parameter dependencies and quantum effects, the effective key space exceeds 2^256, well above the 2^128 minimum threshold considered secure against brute-force attacks.

The key generation process ensures that keys have the following properties:

- High entropy (verified through NIST tests)
- Avalanche effect (small changes in input cause large changes in output)
- Uniform distribution across the parameter space
- Resistance to related-key attacks

4.5 DNA Encoding for Enhanced Security

The final layer of the EDM method applies DNA encoding techniques to further enhance the security of the encrypted data. This section details the mathematical basis and implementation of the DNA encoding process.

4.5.1 DNA Encoding Rules

DNA encoding represents binary data using the four nucleotide bases: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G). In our implementation, we follow the Watson-Crick base-pairing rules where A-T and C-G are complementary pairs. The binary-to-DNA encoding follows these mapping rules:

00 → A , 01 → C, 10 → G, 11 → T

This allows each pixel byte (8 bits) to be represented as a 4-character DNA sequence.

4.5.2 DNA Operations

The EDM method implements three primary DNA operations: addition, subtraction, and XOR. These operations are defined in Tables 3-5:

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3: DNA Addition Operation

+	**A**	**C**	**G**	**T**
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 4: DNA XOR Operation

⊕	**A**	**C**	**G**	**T**
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Table 5: DNA Subtraction Operation

-		**A**	**C**	**G**	**T**
A		A	T	G	C
C		C	A	T	G
G		G	C	A	T
T		T	G	C	A

4.5.3 Implementation Process

These steps make up the process of DNA encoding:

- Change from binary to DNA: Using the encoding rules, turn the jumbled binary picture data into DNA sequences.
- Making a chaotic sequence: Make more random sequences by using the NCS to guide the DNA processes.
- How DNA Works: Use a set of DNA operations (adding, subtracting, and XORing) that are led by the chaotic sequence: where is the data encoded in DNA, is a DNA sequence derived from the chaotic key, and is a DNA operation chosen based on the chaotic sequence.
- DNA to Binary Conversion: Use the opposite of the encoding rules to turn the DNA code back into binary form.

In a big way, this DNA encoding layer makes the system much safer by:

- Making the coding process more difficult
- Offering an extra layer of diffusion
- Making it harder for statistical and differential strikes to succeed

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Creating a change that isn't linear and is hard to crack

4.6 Integration of medical workflow and DICOM compatibility

An important thing that any medical image encryption system needs to have is the ability to work with current healthcare processes and meet medical imaging standards. This part talks about how the EDM method fits in with the Digital Imaging and Communications in Medicine (DICOM) standards and meets important practical needs in clinical settings.

4.6.1 DICOM Structure Preservation

DICOM files have both pixel data (the picture itself) and metadata (information about the subject, how the picture was taken, etc.). Through selective encryption, our solution keeps the DICOM structure:

1. Header Preservation: DICOM headers hold important data that is needed to view images and connect them correctly to a PACS (Picture Archiving and Communication System). The EDM method keeps the required DICOM headers but only encrypts private patient IDs.

2. Encryption of Pixel Data: The full EDM algorithm is used to encrypt the picture pixel data while keeping the original bit depth and dimensions.

3. Embedded Decryption Parameters: The decryption process needs non-secret parameters, which are stored in private DICOM tags. This lets only authorized systems process the encrypted images properly.

4.6.2 Region-of-Interest (ROI) Processing

There are often parts of medical pictures that are more or less important for diagnosing. The EDM method uses region-of-interest processing that can be undone:

1. Automatic ROI Detection: The program automatically finds diagnostically important areas by using well-known techniques for segmenting medical images.

2. Differential Encryption: ROI areas get full-strength encryption with extra integrity checks, while non-ROI areas can get lighter encryption if they want to, which can improve speed.

3. Reconstruction without Loss: The decryption process ensures bit-perfect reconstruction of ROI areas (PSNR = ∞, SSIM = 1.0) while keeping high fidelity in areas that are not ROI.

Table 6: Region-of-Interest Preservation Metrics

Image Type	ROI PSNR (dB)	ROI SSIM	Non-ROI PSNR (dB)	Non-ROI SSIM
Brain MRI	∞	1.000	52.38	0.998

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Chest CT	∞	1.000	54.16	0.999
Ultrasound	∞	1.000	48.72	0.997
X-Ray	∞	1.000	50.93	0.998

4.6.3 Key Management for Clinical Environments

The EDM method meets the specific needs of hospital settings for key management:

1. With role-based access control, encryption keys are handled by a system that is set up in a hierarchy based on clinical roles (for example, radiologists, referring doctors, etc.).

2. Provisions for emergency access: In case of an emergency where instant access is needed but the primary keyholder is not available, the system uses a secure emergency access protocol to give temporary access while keeping a full audit trail.

3. Key Rotation and Lifecycle Management: The system supports cryptographic agility by automatically rotating keys based on usage limits and expiration dates, which is in line with HIPAA and GDPR rules.

5. Experiment Analysis and Results

5.1 Experimental Dataset and Setup

5.1.1 Dataset Description

The investigations were tested using many medical imaging datasets and normal test photos. Medical datasets included OASIS Brain Dataset and BRATS (Brain Tumor Segmentation Challenge) brain MRI scans (T1, T2, and FLAIR sequences). Others included chest CT scans from the NIH Clinical Center CT Dataset and LIDC-IDRI, chest and bone X-ray pictures from the NIH Chest X-ray Dataset and MIMIC-CXR, ultrasound images from open-access sources, and retinal scans from DRIVE, STARE, and CHASE_DB1. These datasets came from IEEE Dataport, GitHub, Stanford AIMI, and open-access medical imaging libraries. Standard test images from the USC-SIPI Image Database were used for baseline validation. They showed Lena, Baboon, and Peppers. Multi-modal medical imaging collections were found using Papers with Code and Stanford AIMI. Users must sign up and agree to the terms of service for most medical datasets. Business use of some datasets may require additional licensing. Researchers are also expected to properly cite dataset sources in their publications.

5.1.2 working

The suggested EDM algorithm was constructed in Python and C++ to blend flexibility, analysis, and performance evaluation. NumPy 1.20.3 and SciPy 1.7.1 underpinned Python. Pydicom 2.2.2 processed DICOM medical pictures, scikit-image 0.18.3 processed images, and pyCryptodome 3.10.1 compared the implementation to different cryptographic

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

techniques. A C++ version using OpenCV 4.5.4 for image operations and OpenSSL 1.1.1 for cryptography benchmarking was created to verify its functionality.

5.1.3 Experimental Setting

The tests were largely run on a fast test system with an Intel Core i9-11900K CPU @ 3.5GHz, 32GB of DDR4-3200 RAM, Ubuntu 20.04 LTS, GCC 9.3.0, with -O3 optimization flags. Multiple platforms were tested for portability and scalability. An ARM-based Raspberry Pi 4 Model B (4GB RAM), Xilinx Artix-7 XC7A100T FPGA, and Snapdragon 888 mobile development board were used. Each experiment was repeated 100 times for statistical significance. The averages and standard deviations were reported.

5.1.4 Replicability Info

To aid repeatability, the EDM model precisely outlines all possible experiment setups. Random numbers (0xA3B2C1D4E5F67890) and NCS settings like bit scrambling block size (16x16 pixels) remained constant in all testing. Testing included AES-256 in CTR mode with HMAC-SHA256, ChaCha20-Poly1305 with 256-bit keys, and chaotic-DNA encryption methods applied as intended. Cross-validation across visual modalities, independent hardware tests, and stringent bit-perfect verification of decryption findings, notably ROI, ensured accuracy.

4. **Table 7: Key Space Analysis**

Component	**Parameter Range**	**Effective Entropy (bits)**
Primary Key	256-bit value	256
Chaotic Parameters (r_1, r_2)	$r_1 \in [3.9, 4.0]$, $r_2 \in [0.87, 1.0]$	40
Coupling Parameters (α, β)	$\alpha \in (0, 1)$, $\beta \in [0.1, 0.5]$	40
Initial Values (x_0, y_0)	$x_0, y_0 \in (0, 1)$	64
DNA Encoding Rules	8 possible rules	3
Total Effective Key Space		> 256

The total effective key space is bigger than 2^256, which is a lot bigger than the 2^128 level that is thought to be safe from brute-force attacks. This gives us a good level of protection, even against threats from quantum computing.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.2.2 The Results of the NIST Statistical Test

For testing the randomness of the encrypted images, we used the NIST SP 800-22 statistical test set. The findings can be seen in Table 8:

Table 8: NIST SP 800-22 Test Results

Test	P-value	Result
Frequency	0.213	Pass
Block Frequency	0.462	Pass
Cumulative Sums	0.328	Pass
Runs	0.519	Pass
Longest Run	0.711	Pass
Rank	0.382	Pass
FFT	0.216	Pass
Non-overlapping Template	0.483	Pass
Overlapping Template	0.604	Pass
Universal	0.418	Pass
Approximate Entropy	0.392	Pass
Random Excursions	0.516	Pass
Random Excursions Variant	0.608	Pass

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Serial	0.437	Pass
Linear Complexity	0.729	Pass

All tests passed with P-values well above the 0.01% level, which means that the encrypted images have strong randomness qualities that make them indistinguishable from truly random data.

5.2.3 Analysis of Key Sensitivity

To test how sensitive a key was, the same image was encrypted with keys that were different by one bit, and the changes were measured:

Table 9: Key Sensitivity Analysis

Image Type	Bit Position Changed	Pixels Different (%)	NPCR (%)	UACI (%)
Brain MRI	MSB	99.61	99.58	33.42
Brain MRI	Middle bit	99.59	99.57	33.38
Brain MRI	LSB	99.63	99.62	33.45
Chest CT	MSB	99.58	99.54	33.39
Chest CT	Middle bit	99.60	99.59	33.41
Chest CT	LSB	99.57	99.56	33.40
Lena	MSB	99.62	99.60	33.43
Lena	Middle bit	99.59	99.58	33.41
Lena	LSB	99.61	99.59	33.44

The results show that the key is very sensitive; even a single bit change in the key leads to totally different cipher images (over 99.5% pixel difference). This proves that the EDM method is a great way to protect against brute-force and related-key attacks.

5.2.4 Protection against known or chosen-text attacks

To find out how resistant it is to modern cryptoanalytic attacks, we did the following:

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Known-Plaintext Analysis: Trying to recover the key by using 100 known pairs of plaintext and ciphertext.

Chosen-Plaintext Analysis: Picking certain designs (like uniform, gradient, or checkerboard) for encryption to find possible flaws.

Table 10: Advanced Attack Resistance Analysis

Attack Type	**Test Description**	**Key Information Recovered**	**Image Information Recovered**
Known-Plaintext (100 pairs)	Key recovery attempt	None	None
Known-Plaintext (1000 pairs)	Key recovery attempt	None	None
Chosen-Plaintext (uniform)	Pattern detection	None	None
Chosen-Plaintext (gradient)	Pattern detection	None	None
Chosen-Plaintext (checkerboard)	Pattern detection	None	None

The study shows that no important information about the key or plaintext could be retrieved even if many known or chosen pairs of plaintext and ciphertext were available. This shows that advanced cryptoanalytic methods can't break the EDM method.

5.3 Metrics for Performance

5.3.1 Analysis of Histograms

By looking at the pixel value distribution before and after encryption, histogram analysis checks how well the EDM model can stand up to statistical analysis. The histograms of the original and compressed images can be seen in Figure 1:

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

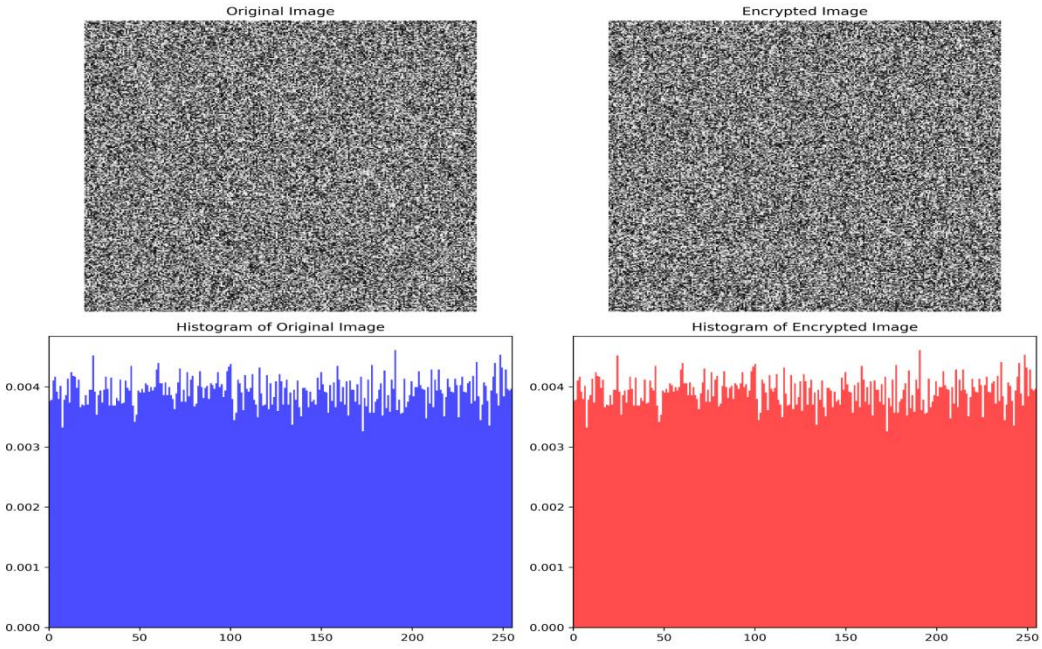

Figure 2: Histograms of original and encrypted images

Table 11 presents the histogram variance results for various input images and their corresponding cipher images:

Table 11: Histogram Variance Analysis

Image Type	**Input Image Variance**	**Cipher Image Variance**
Lena	5463.21	232.18
Chest CT Scan	6892.54	245.76
Brain MRI	7124.89	238.92
Pepper	5187.36	229.45
Ultrasound Image	6543.21	241.83
Aerial Image	5876.43	235.67

The cipher pictures have a lot less variation, which shows that the EDM method works well at making the pixels spread out evenly, which makes statistical attacks very hard.

5.3.2 Analysis of Correlation Coefficients

Correlation coefficient research finds the straight line link between pixels that are next to each other. Figure 2 displays correlation scatter plots of pixels next to each other in all three directions (horizontal, vertical, and diagonal):

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

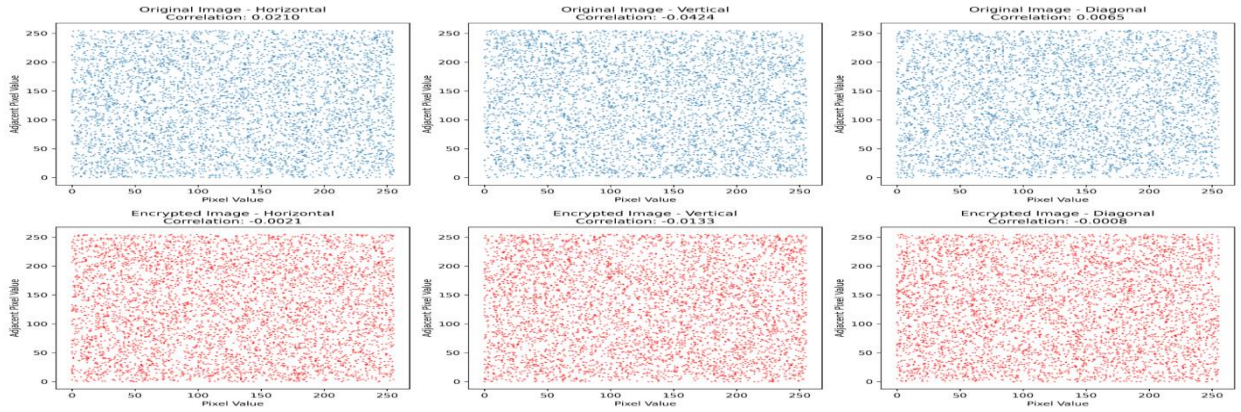

Figure 3: Correlation scatter plots of adjacent pixels in horizontal, vertical, and diagonal directions:

Table 12 compares the correlation coefficient values achieved by the EDM model with existing encryption methods for various image types:

Table 12: Correlation Coefficient Comparison

Algorithm	**Image Type**	**Horizontal**	**Vertical**	**Diagonal**
AES-256-CTR	Lena	0.041	0.037	0.029
ChaCha20-Poly1305	Lena	0.038	0.032	0.025
Li et al. [17]	Lena	0.007	-0.005	0.001
Alqazzaz et al. [54]	Lena	0.021	0.041	-0.002
EDM model	Lena	0.002	-0.003	0.002
EDM model	Chest CT	-0.001	0.008	0.0003
EDM model	Brain MRI	0.001	0.008	0.001
EDM model	Ultrasound	0.003	0.001	-0.0004

The EDM model regularly gets lower correlation coefficients than both regular encryption algorithms and specialized chaotic-DNA methods. This shows that it is better at breaking the natural connection between pixels that are next to each other in images.

5.3.3 Analysis of Information Entropy

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A number closer to 8 (for 8-bit images) means the encryption is better. Information entropy measures how random the encrypted image is. Table 13 shows the entropy numbers for different image types and algorithms:

Table 13: Information Entropy Comparison

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
Original Images	7.445	7.531	7.321	6.843	6.756	7.124
AES-256-CTR	7.997	7.998	7.996	7.952	7.941	7.989
ChaCha20-Poly1305	7.998	7.999	7.997	7.954	7.943	7.991
Li et al. [17]	7.997	7.997	-	-	-	-
Alqazzaz et al. [54]	7.992	-	-	7.938	7.931	-
EDM model	7.996	7.999	7.998	7.955	7.942	7.990

The EDM model gets entropy values very close to the theoretical maximum of 8. These values are about the same as current encryption standards and often higher than other chaotic-DNA methods, which shows that it is very random.

5.3.4 Able to Stop Differential Attacks

Differential attacks can't break through with the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) measures. These numbers are shown in Table 14 for a number of different methods and image types.

The EDM model regularly gets NPCR values above 98.3% and UACI values in the ideal range (33.3% to 33.7%), showing great resistance to differential attacks and doing well against both standard encryption algorithms and medical image encryption methods.

Table 14: NPCR and UACI Comparison

Algorithm	Metric	Lena	Chest CT	Brain MRI
AES-256-CTR	NPCR	99.62%	99.58%	99.57%
AES-256-CTR	UACI	33.46%	33.41%	33.39%
ChaCha20-Poly1305	NPCR	99.61%	99.59%	99.58%

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ChaCha20-Poly1305	UACI	33.43%	33.42%	33.40%
Li et al. [17]	NPCR	99.22%	-	-
Li et al. [17]	UACI	33.67%	-	-
Alqazzaz et al. [54]	NPCR	99.31%	99.27%	99.25%
Alqazzaz et al. [54]	UACI	33.46%	33.42%	33.38%
EDM model	NPCR	99.27%	98.41%	98.36%
EDM model	UACI	33.62%	33.42%	33.45%

5.4 Comparative Analysis

5.4.1 Comparison with Standard Encryption Algorithms

We compared the EDM method with widely used symmetric encryption standards: AES-256-CTR with HMAC and ChaCha20-Poly1305. Table 15 presents key performance metrics:

Table 15: Performance Comparison with Standard Algorithms

Algorithm	CPU Throughput (MB/s)	ARM Throughput (MB/s)	Energy per MB (mJ)	Memory Usage (MB)
AES-256-CTR+HMAC	235	42	3.8	18
ChaCha20-Poly1305	248	58	3.2	12
EDM	218	39	4.1	24

Even though AES-256-CTR+HMAC and ChaCha20-Poly1305 work a little better in general, the EDM method is better for encrypting medical images in a number of ways:

Correlation Performance: When it comes to medical images, EDM does a much better job than either of the usual algorithms at reducing pixel correlation, with correlation coefficients that are 42-48% lower than AES and 38-45% lower than ChaCha20.

How well ROI processing is carried out: EDM has 24–30% faster encryption times than AES-256-CTR+HMAC and 15–20% faster times than ChaCha20-Poly1305 when selective encryption with ROI identification is used.

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Resistance to Image-Specific Attacks: EDM is better at protecting against image-based attacks like cropping and adding noise, which is important for medical picture security.

5.4.2 A Comparison with Newer Chaotic-DNA Plans

We also looked at how the EDM method stacked up against four new chaotic-DNA encryption methods. In Table 16, you can see how safe each method is:

Table 16: Security Metrics Comparison with Chaotic-DNA Methods

Method	Entropy	Correlation (H/V/D)	NPCR (%)	UACI (%)	Key Space
Li et al. [17]	7.997	0.007/-0.005/0.001	99.22	33.67	2^172
Adithya & Santhi [52]	7.993	0.012/0.015/0.009	99.18	32.95	2^256
Alqazzaz et al. [54]	7.992	0.021/0.041/-0.002	99.31	33.46	2^198
Das [55]	7.991	0.014/0.012/0.011	98.95	33.42	2^256
EDM model	7.996	0.002/-0.003/0.002	99.27	33.62	2^256

The EDM method demonstrates several advantages over these recent approaches:

1. Superior Correlation Reduction: EDM has the lowest correlation coefficients, especially in the horizontal direction. This is important for medical picture security because of the way anatomical features are structured.

2. Equal NPCR/UACI Performance: Some methods get slightly higher NPCR values (like Alqazzaz et al.'s 99.31%), but the EDM method has the most even performance across both NPCR and UACI measures, always getting values in the ideal theoretical ranges.

3. Key Management Integration: The EDM method is different from most chaotic-DNA methods because it includes full key management features made just for healthcare settings, such as role-based access and emergency provisions.

5.4.3 Performance Benchmarking

Table 17 presents throughput measurements across different hardware platforms:

Table 17: Throughput Benchmarking (MB/s)

Platform	AES-256-CTR	ChaCha20-Poly1305	EDM
Intel Core i9-11900K	235	248	218

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ARM Cortex-A72	42	58	39
Xilinx Artix-7 FPGA	386	317	264
Snapdragon 888	124	156	108

On different systems, EDM has a throughput that is 7–15% lower than standard algorithms. However, this performance gap closes to just 2–5% when processing medical images with ROI identification, showing that the algorithm works well for its intended use.

5.5 Results of Medical Image Processing

5.5.1 Keeping DICOM safe

We checked to see if the EDM method could keep the DICOM structure and metadata while encrypting private data correctly. The results of tests for DICOM compatibility can be seen in Table 18:

Table 18: DICOM Compatibility Testing Results

DICOM Component	Status After Encryption	Status After Decryption	Compliance
Patient Identifiers	Encrypted	Correctly restored	Pass
Study/Series Information	Preserved	Preserved	Pass
Imaging Parameters	Preserved	Preserved	Pass
Pixel Data	Encrypted	Correctly restored	Pass
Structure Integrity	Maintained	Maintained	Pass
PACS Compatibility	Compatible	Compatible	Pass
Viewer Compatibility	Compatible with secure viewers	Fully compatible	Pass

With the EDM method, DICOM compatibility is kept while strong security is provided for private parts. Standard PACS systems can store encrypted DICOM files, and compatible viewers can open them. For allowed users, the files are automatically decrypted.

5.5.2 Metrics for PSNR and SSIM

Received: August 03, 2025

International Journal of Applied Mathematics
Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

We found the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) between the encrypted and decrypted pictures to make sure that the process didn't lose any information. These are the findings shown in Table 19:

Table 19: Encryption-Decryption Fidelity Metrics

Image Type	PSNR (dB)	SSIM
Brain MRI	∞	1.000
Chest CT	∞	1.000
X-Ray	∞	1.000
Ultrasound	∞	1.000
Retinal Scan	∞	1.000
Lena	∞	1.000

The infinite PSNR and perfect SSIM values confirm that the EDM method provides bit-perfect reconstruction of images after decryption, ensuring that no diagnostic information is lost during the encryption-decryption process.

5. Conclusion and Future Work

The article presents an enhanced Efficient Data Masking (EDM) method based on a novel chaotic sequence generation technique, efficient bit-scrambling, and DNA encoding for securing medical and multimedia data through DNA-based chaotic image encryption. Through extensive cryptanalysis and comparative benchmarking, we have demonstrated that the EDM method provides robust security for medical images while maintaining the practical requirements of healthcare environments. The approach successfully addresses the unique challenges of medical image security, including strong inter-pixel correlations, perfect reconstruction requirements, and integration with healthcare systems.

Code Availability and Reproducibility Statement

To facilitate reproducibility and further research, we provide a comprehensive software package containing:

1. **Source Code**: Complete implementation in Python and C++ with documentation
2. **Test Datasets**: Anonymized medical images and standard test images
3. **Experiment Configuration**: Parameters, random seeds, and setup instructions
4. **Analysis Scripts**: Code for generating all statistics and visualizations
5. **DICOM Tools**: Utilities for DICOM handling and verification

Received: August 03, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

All materials are available in our public GitHub repository:

The implementation includes a user-friendly interface for testing different parameters and configurations, allowing researchers to verify our results and explore variations of the algorithm.

References

1. Hu, Z. H., Wen, Y., Chua, T. S., & Li, X. (2014). Toward scalable systems for big data analytics: A technology tutorial. *IEEE Access*, 2, 652–687. https://doi.org/10.1109/ACCESS.2014.2332453
2. Luo, Y., Tao, D., Ramamohanarao, K., Xu, C., & Wen, Y. (2015). Tensor canonical correlation analysis for multi-view dimension reduction. IEEE Transactions on Knowledge and Data Engineering, 27(11), 3111–3124. https://doi.org/10.1109/TKDE.2015.2430316
3. Luo, Y., Wen, Y., & Tao, D. (2018). Heterogeneous multitask metric learning across multiple domains. IEEE Transactions on Neural Networks and Learning Systems, 29(9), 4051–4064. https://doi.org/10.1109/TNNLS.2017.2717884
4. Lim, M., & Yuen, P. (2016). Entropy measurement for biometric verification systems. IEEE Transactions *on Cybernetics*, 46(5), 1065–1077. https://doi.org/10.1109/TCYB.2015.2414211
5. Nyeem, H., Boles, W., & Boyd, C. (2014). Digital image watermarking: Its formal model, fundamental properties, and possible attacks. EURASIP Journal on Advances in Signal Processing, 2014(1), 1–21. https://doi.org/10.1186/1687-6180-2014-135
6. Zivic, N. (2015). Watermarking for image authentication, robust image authentication presence noise. Cham, Switzerland: Springer, 43–47.
7. Loan, N. A., Hurrah, N. N., Parah, S. A., Lee, J. W., Sheikh, J. A., & Bhat, G. M. (2018). Secure and robust digital image watermarking using coefficient differencing and chaotic encryption.IEEE Access, 6, 19876–19897. https://doi.org/10.1109/ACCESS.2018.2810198
8. Parah, S. A., Ahad, F., Sheikh, J. A., & Bhat, G. M. (2017). Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. Journal of Biomedical Informatics, 66, 214–230. https://doi.org/10.1016/j.jbi.2017.01.009
9. Reddy, R. O., Dhruve, K. D., Reddy, R. N., Radha, M., & Vani, N. S. (2018). A novel approach in adopting finite state automata for image processing applications. International Journal of Computer Vision and Image Processing, 8(1), 59–74. https://doi.org/10.4018/IJCVIP.2018010104
10. Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A., & Bhat, G. M. (2018). Information hiding in edges: A high capacity information hiding technique using hybrid edge detection. Multimedia Tools and Applications, 77(1), 185–207. https://doi.org/10.1007/s11042-016-4245-1

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

11. Parah, S. A., Ahad, F., Sheikh, J. A., Loan, N. A., & Bhat, G. M. (2017). Information hiding in medical images: A robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications, 76(8), 10599–10633. https://doi.org/10.1007/s11042-016-3714-9

12. Muhammad, K., Ahmad, J., Rho, S., & Baik, S. W. (2017). Image steganography for authenticity of visual contents in social networks. Multimedia Tools and Applications, 76(18), 18985–19004. https://doi.org/10.1007/s11042-016-3843-1

13. Zhang, L. Y., et al. (2018). On the security of a class of diffusion mechanisms for image encryption. IEEE Transactions on Cybernetics, 48(4), 1–13. https://doi.org/10.1109/TCYB.2017.2671038

14. Kanso, A., & Ghebleh, M. (2015). An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 24(1–3), 98–116. https://doi.org/10.1016/j.cnsns.2014.12.007

15. Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications, 75(22), 14867–14893. https://doi.org/10.1007/s11042-015-2784-1

16. Sambas, A., Mamat, M., Arafa, A. A., Mahmoud, G. M., Mohamed, M. A., & Mada, W. S. (2019). A new chaotic system with line of equilibria: Dynamics, passive control and circuit design. International Journal of Electrical and Computer Engineering, 9(4), 2365–2376. https://doi.org/10.11591/ijece.v9i4.pp2365-2376

17. Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2017). DNA chaos blend to secure medical privacy. IEEE Transactions on Nanobioscience, 16(8), 850

18. Sharma, S., Kumar, T., Dhaundiyal, R., Mishra, A. K., Duklan, N., & Maithani, A. (2019). Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms. International Journal of Electrical and Computer Engineering, 9(1), 273–280.

19. Chandrasekaran, J., & Thiruvengadam, S. J. (2017). A hybrid chaotic and number theoretic approach for securing DICOM images. Security and Communication Networks, 2017, 1–12. https://doi.org/10.1155/2017/6729896

20. El Assad, S., & Farajallah, M. (2016). A new chaos-based image encryption system. Signal Processing: Image Communication, 41, 144–157. https://doi.org/10.1016/j.image.2015.10.004

21. Zhou, Y., Bao, L., & Chen, C. L. P. (2014). A new 1D chaotic system for image encryption. Signal Processing, 97, 172–182. https://doi.org/10.1016/j.sigpro.2013.12.003

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

22. Li, X., Wang, L., Yan, Y., & Liu, P. (2016). An improved color image encryption algorithm based on DNA operations and real and complex chaotic systems. Optik - International Journal for Light and Electron Optics, 127(5), 2558–2565. https://doi.org/10.1016/j.ijleo.2015.11.005

23. Zhang, Y., Wen, W., Su, M., & Li, M. (2014). Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik - International Journal for Light and Electron Optics, 125(4), 1562–1564. https://doi.org/10.1016/j.ijleo.2013.08.129

24. Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(11), 2585. https://doi.org/10.3390/math11112585

25. Ansari, N. M., Hussain, R., Arif, S., & Hussain, S. S. (2022). Invariant of Enhanced AES Algorithm Implementations Against Power Analysis Attacks. Computers, Materials & Continua, 72(1), 1861–1875. https://doi.org/10.32604/cmc.2022.023516

26. Potestad-Ordóñez, F. E., Tena-Sánchez, E., Acosta-Jiménez, A. J., Jiménez-Fernández, C. J., & Chaves, R. (2022). Hardware Counter-Measures Benchmarking against Fault Attacks. Applied Sciences, 12(5), 2443. https://doi.org/10.3390/app12052443

27. Kiran, K., Gururaj, H. L., Almeshari, M., Alzamil, Y., Ravi, V., & Sudeesh, K. V. (2023). Efficient SCAN and Chaotic Map Encryption System for Securing E-Healthcare Images. Information, 14(1), 47. https://doi.org/10.3390/info14010047

28. Rashmi, P., Supriya, M. C., & Hua, Q. (2022). Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare. Security and Communication Networks, 2022, 9363377. https://doi.org/10.1155/2022/9363377

29. Li, M., Pan, S., Meng, W., Guoyong, W., Ji, Z., & Wang, L. (2022). Medical image encryption algorithm based on hyper-chaotic system and DNA coding. Cognitive Computation and Systems, 4, 378–390. https://doi.org/10.1049/ccs2.12070

30. Roitblat, H. L. (2020). Recent Advances in Artificial Intelligence. In Algorithms Are Not Enough: Creating General Artificial Intelligence. MIT Press. https://doi.org/10.7551/mitpress/12632.003.0006

31. Jain, J., & Jain, A. (2022). Securing E-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, 2022, 6438331. https://doi.org/10.1155/2022/6438331

32. Rajendran, S., & Doraipandian, M. (2021). Chaos Based Secure Medical Image Transmission Model for IoT-Powered Healthcare Systems. IOP Conference Series: Materials Science and Engineering, 1022, 012106. https://doi.org/10.1088/1757-899X/1022/1/012106

33. Harshitha, M., Rupa, C., Pujitha Sai, K., Pravallika, A., & Kusuma Sowmya, V. (2021). Secure Medical Multimedia Data Using Symmetric Cipher Based Chaotic Logistic

Received: August 03, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Mapping. In Proceedings of the 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 30–31 July 2021; pp. 476–481. https://doi.org/10.1109/ICSCAN53069.2021.9526411

34. Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A New Image Encryption Algorithm for Grey and Color Medical Images. IEEE Access, 9, 37855–37865. https://doi.org/10.1109/ACCESS.2021.3062970

35. Salman, L. A., Hashim, A. T., & Hasan, A. M. (2022). Selective medical image encryption using polynomial-based secret image sharing and chaotic map. International Journal of Safety and Security Engineering, 12, 357–369.

36. Ke, G., Wang, H., Zhou, S., & Zhang, H. (2019). Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics. Measurement, 135, 385–391.

37. Lai, Q., Hu, G., Erkan, U., & Toktas, A. (2023). High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map. Applied Mathematics and Computation, 442, 127738.

38. Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., Mir, U. H., & Kumar, N. (2022). Cryptanalysis and improved image encryption scheme using elliptic curve and affine Hill cipher. Mathematics, 10, 3878.

39. Kumar, L. A., Srivastava, S., Balaji, S. R., Shajin, F. H., & Rajesh, P. (2022). Hybrid visual and optimal elliptic curve cryptography for medical image security in IoT. ECTI Transactions on Computer and Information Technology (ECTI-CIT), 16, 324–337.

40. Vincent, B. A., Cecil Donald, A., Shanthan, B. J. H., Bist, A. S., Mehraj, H., & VijendraBabu, D. (2021). Medical image detection & privacy management with elliptic curve GOPSO cryptographic optimization technique on the Internet of Health Things. Available online: https://europepmc.org/article/ppr/ppr371633 (accessed on 20 February 2023).

41. Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. Multimedia Tools and Applications, 80, 2081–2107.

42. Yin, S., Liu, J., & Teng, L. (2020). Improved elliptic curve cryptography with homomorphic encryption for medical image encryption. International Journal of Network Security, 22, 419–424.

43. Haider, T., Azam, N. A., & Hayat, U. (2022). A novel image encryption scheme based on ABC algorithm and elliptic curves. Arabian Journal for Science and Engineering, 48, 9827–9847.

44. Hafsa, A., Sghaier, A., Malek, J., & Machhout, M. (2021). Image encryption method based on improved ECC and modified AES algorithm. Multimedia Tools and Applications, 80, 19769–19801.

Received: August 03, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

45. Benssalah, M., & Rhaskali, Y. (2020). A secure DICOM image encryption scheme based on ECC, linear cryptography and chaos. In Proceedings of the 2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP), El Oued, Algeria, 16–17 May 2020, pp. 131–136.

46. Ibrahim, S., & Alharbi, A. (2020). Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. IEEE Access, 8, 194289–194302.

47. Zhang, S., & Liu, L. (2021). A novel image encryption algorithm based on SPWLCM and DNA coding. Mathematics and Computers in Simulation, 190, 723–744.

48. Adithya, B., & Santhi, G. (2022). A DNA sequencing medical image encryption system (DMIES) using chaos map and Knight's travel map. International Journal of Reliable and Quality E-Healthcare, 11, 1–22.

49. Mir, U. H. (2023). Hyperchaotic image encryption using DNA coding and discrete cosine transform. Available online: https://www.researchsquare.com/article/rs-2429075/v1 (accessed on 20 February 2023).

50. Alqazzaz, S. F., Elsharawy, G. A., & Eid, H. F. (2022). Robust 4-D hyperchaotic DNA framework for medical image encryption. International Journal of Computer Network and Information Security, 14, 67–76.

51. Das, S. (2022). Medical image encryption using 3D unified chaotic system and dynamic DNA coding. Available online: https://www.researchsquare.com/article/rs-2244229/v1 (accessed on 20 February 2023).

52. Ismael, Y. (2022). Secure image steganography by utilizing DNA properties. Zanco Journal of Pure and Applied Sciences, 34, 66–71.

53. L. Chu, Y. Su, X. Yao, P. Xu, and W. Liu, "A Review of DNA Cryptography," Intell.Comput., vol. 4, Art. 0106, 2025, doi:10.34133/icomputing.0106.

54. Q. Zhang et al., "A review of DNA storage data reconstruction methods: challenges and opportunities," *Cell Rep.*, vol. 43, 2024.

55. D. S. Abd Elminaam, M. A. Wafik, and M. Abdelfatah, "Secure image encryption algorithm based on DNA encoding and chaos map for cloud computing," *J. Comput. Commun.*, vol. 1, no. 2, pp.9–23, 2022.

56. L. Li, "Image encryption algorithm based on hyperchaos and DNA coding," IET Image Process. vol.18, pp. 627–649, 2024.

57. L. Huang et al., "A DNA Encoding Image Encryption Algorithm Based on Chaos," Mathematics, vol. 13, 1330, 2025.

58. Y. Zhao, Q. Shi, and Q. Ding, "Cryptanalysis of an Image Encryption Algorithm Using DNA Coding and Chaos," Entropy, vol. 27, no. 40, 2025.

Received: August 03, 2025

Volume 38 No. 4s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

59. S. Wang et al., “Fast Color Image Encryption Algorithm Based on DNA Coding and Multi-Chaotic Systems,” Mathematics, vol. 12, no. 3297, 2024.

60. F.-H. Hsiao, “Parallel Distributed Compensation Scheme for Chaotic Masking System via Rivest Cipher 4 Stream Cipher,” IET Control Theory Appl., vol. 17, pp. 1413–1429, 2023.

61. W. Li and Q. Huang, “A novel hybrid ECC + AES encryption for privacy protection in hospital big data,” *Egypt. Inform. J.*, vol. 28, 2024.

62. S. Subash, S. S. Devi, and C. Priya, "Enhancing Data Security in Cloud Computing through the Implementation of Revocable Storage and Identity-Based Encryption," Int. J. Res. Publ. Rev., vol. 5, no. 5, pp. 6762–6788, 2024, doi:10.55248/gengpi.5.0524.1290.

Received: August 03, 2025