RESEARCH PAPER

Medical Image Privacy Model Driven by an Enhanced secp256k1 Pseudo-Random Sequence Generator.

Sowmya T K[1], Dr. Sathyanarayana S V[2], Dr. Mohan Naik R[3]

[1]Research Scholar, Department of Electronics and Communication Engineering, JNN College of Engineering, Shimoga, Karnataka, India; k.sowmya.02@gmail.com
[2]Department of Electronics and Communication Engineering, JNN College of Engineering, Shimoga, Karnataka, India; svs@jnnce.ac.in
[3]Department of Electronics and Communication Engineering, S D M Institute of Technology, Ujire, Karnataka, India; mohannaik@sdmit.in

ABSTRACT
Security of medical images over open networks is a serious requirement in modern healthcare systems due to secrecy and confidentiality concerns. This paper presents a novel robust medical image encryption scheme based on elliptic curve cryptography (ECC) over large finite fields, which employs a novel pseudorandom sequence generator (PRSG). The proposed method is implemented in Python, and the generated sequence is evaluated using the statistical test suite NIST. Used these sequences for medical image encryption. Encryption and decryption give strong lossless recovery. This can be analyzed by a histogram, which gives uniform pixel distribution. Adjacent pixel correlation values are nearer to zero in encrypted images, which reveals from the correlation analysis and exhibits strong resistance against differential attacks. The sensitivity analysis with Number of Pixels Change Rate (NPCR) values above 99.60% and Unified Average Changing Intensity (UACI) values exceeding 33%. This proposed scheme attains near ideal entropy values (7.99), improved Peak Signal-to-Noise Ratio (PSNR), lower Mean Absolute Error (MAE), and reduced Mean Squared Error (MSE) compared to other EC based approaches. The proposed PRSG offers enhanced security and efficiency and is suitable for medical images for secure transmission and reception of networked healthcare systems...
Keywords: Elliptic Curve Cryptography (ECC), Secp256k1 Curve, Pseudo-Random Sequence Generator (PRSG), Number of Pixels Change Rate (NPCR), Peak Signal-to-Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), Mean Absolute Error (MAE), Mean Squared Error(MSE)....
How to cite this article*:* Sowmya TK, Sathyanarayana SV, Mohan Naik R. Medical Image Privacy Model Driven by an Enhanced secp256k1 Pseudo-Random Sequence Generator. Int J Drug Deliv Technol. 2026;16(65s): 1629-1639. DOI: 10.25258/ijddt.16.65s.171
Source of support: Nil.
Conflict of interest: Nil.

INTRODUCTION

Medical imaging has become a routine part of modern healthcare, especially with the growing use of digital hospital systems and telemedicine services. X-rays, MRI, CT, and ultrasound images are generated daily and are often shared across departments, hospitals, and remote clinical facilities. These images are critical for diagnosis and treatment related decisions, which makes their reliability extremely important. At the same time, the way medical images are stored and transmitted has changed. Many healthcare systems now rely on networked and cloud based infrastructures, where data may pass through public or semi-public communication channels [1,2]. This creates security concerns. Unauthorized access or even small modifications to medical images can violate patient privacy and may affect clinical interpretation. As a result, protecting medical images from unauthorized use or manipulation has become a necessary requirement rather than an optional feature in current healthcare environments. As medical images are increasingly exchanged through shared and networked systems, security risks have become difficult to ignore.

Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are cryptographically strong and used as conventional text-oriented encryption algorithms. Medical images have inherent characteristics such as large size, high redundancy, and strong correlation among adjacent pixels; due to this, AES and DES are not always suitable and efficient for medical images [3, 4]. Therefore, the image encryption scheme is specially designed to preserve lossless recovery with high security, computational efficiency, and robustness against cryptographic attacks since medical images have sensitive diagnostic information, and even small alterations can compromise the clinical information.
Due to the strong security properties and suitability of chaos-based elliptic curve cryptography (ECC) based image encryption, it has been trending in recent years for multimedia data [5-7]. Chaos-based schemes to achieve confusion and diffusion exploit some nonlinear properties of dynamical systems, such as sensitivity to initial conditions and pseudo-randomness. If chaos-based methods are designed improperly, several studies have reported that many chaos-based schemes suffer from finite precision effects, weak key spaces, and vulnerability to known plaintext or chosen plaintext attacks.

**Author for Correspondence: Sowmya T K.*

The emergence of a powerful public-key cryptographic paradigm offering equivalent security to traditional systems such as RSA but with significantly smaller key sizes is elliptic curve cryptography [10]. ECC has reduced computational overhead, lower memory requirements, and high security per bit and is particularly attractive for networked and resource-constrained environments [11]. Due to this, ECC is well suited for medical image encryption over transmission in telemedicine, wireless body area networks, and cloud-based healthcare systems.

Recent studies extended ECC over finite fields to more generalized algebraic structures, such as finite rings which increases the security and flexibility [12,13]. This introduces more complexity in the structure of algebraic equations; a novel pseudo-random sequence generation makes cryptanalysis more difficult since it's producing key streams that govern pixel permutation and diffusion processes. The encryption scheme provides good statistical quality of these sequences, which directly affects the security strength [14].

Some image encryption applications proposed by ECC-based pseudorandom bit generators (EC-PRBs) [15-17]. The statistical quality of these sequences from these approaches demonstrates promising security characteristics that directly affect the security strength, since many existing schemes show flaws defined by the National Institute of Standards and Technology (NIST) as residual pixel correlation in encrypted images, insufficient diffusion, or suboptimal randomness performance [18]. Some methods of prime field arithmetic limit the diversity and unpredictability of generated sequences.

Medical image encryption using both cryptographic and image quality metrics requires rigorous evaluation. Statistical analysis such as histogram uniformity, correlation coefficients, and information entropy are used to evaluate the resistance against statistical attacks [19]. Resistance of differential attacks [19]. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to evaluate differential attack resistance, which measures the sensitivity of the encryption scheme to minor changes in the plain image [20]. The mandatory requirements for medical applications are the Peak Signal-To-Noise Ratio (PSNR), the Mean Absolute Error (MAE), and the Mean Square Error (MSE), which are used to evaluate image quality metrics, including those essential to ensure accurate and lossless decryption, a mandatory requirement for medical applications [21].

This work proposes a highly secure medical image encryption based on Elliptic Curve over large finite fields using the secp256k, which addresses the limitations of existing approaches. A novel pseudorandom sequence generator is designed based on the EC secp256k1 using ECC arithmetic, and an XOR-based transformation is used to exclude regularities in generated raw sequences. The proposed method is evaluated through comprehensive experimental analysis and implemented using Python.

The NIST statistical test suite validates the generated sequences, a widely recognized randomness assessment as a benchmark for cryptographic applications [18]. Generated sequences from the proposed PRSG pass all the NIST tests, which indicates that they have strong statistical randomness and are suitable for cryptographic applications. It is also evaluated by uniform pixel distribution using histogram analysis in encrypted images, and lossless recovery can be confirmed by near-perfect similarity between original and decrypted images.

The proposed scheme exhibits strong correlation coefficient analysis. To achieve this, it reduces the correlation between adjacent pixels in encrypted images to values close to zero, even though the original images have strong horizontal, vertical, and diagonal correlations. This ensures that it prevents statistical attacks that exploit spatial redundancy in image data.

This method highlights the effectiveness of the scheme in preserving image fidelity after decryption, which can be achieved by improved PSNR, reduced MAE, and lower MSE values compared to benchmark EC PRBG methods. In addition, the proposed cryptographic scheme achieves maximum randomness in encrypted images by evaluating information entropy, which is close to 8 bits per pixel. In medical images, diagnostic information must not be compromised by encryption processes; therefore, these characteristics are important in medical images.

There are a lot of image encryption schemes out there, like chaos-based and EC based schemes. Image encryption is still a big problem. We need to make sure that the encryption is secure and that the medical images stay clear. Many of the methods we have now are not good enough. They have key spaces or precision problems. Sometimes the pixels are still connected, which is bad for security. Some methods are also not good at mixing up the pixels so they are easy to break. Some EC based methods are not random enough, which is something that the NIST evaluations have shown. Image encryption schemes like these need to be improved with EC based image encryption schemes. Moreover, several studies emphasize statistical security metrics without adequately addressing the mandatory requirement of lossless reconstruction and preservation of diagnostic fidelity in medical images. Therefore, there remains a need for a robust, computationally efficient EC based encryption scheme that generates high-quality pseudorandom sequences, eliminates spatial correlation, resists advanced attacks, and guaranties accurate and lossless medical image recovery.

The primary contributions of this work is as follows:

The development of a novel EC based pseudo-random sequence generator over large prime fields using elliptic curve Secp256k1.

Comprehensive randomness validation using the NIST test suite.

Extensive security evaluation through statistical, differential, and correlation analysis.

The remainder of this paper is organized as follows. Section 2 describes the Related Work. Section3 discusses the preliminaries, Section 4 discusses the proposed PRSG, experimental setup, and evaluation metrics. Section 5 presents detailed results and discussions. Finally, Section 6

concludes the paper and highlights potential directions for future research.

Related Work

Medical image encryption has become an important research area because medical data are highly sensitive and are increasingly transmitted through networked and cloud-based healthcare systems. Over time, research in this field has generally followed three main directions:

Chaos-based encryption techniques,

Elliptic Curve Cryptography (ECC) based approaches

Hybrid methods that combine chaos and ECC.

Chaos-Based Medical Image Encryption Schemes

Chaos-based encryption methods rely on nonlinear chaotic maps to generate pseudo random sequences used for pixel permutation and diffusion. Early studies by Fridrich [22] and Chen et al. [23] demonstrated that chaotic maps such as the logistic map and Arnold cat map provide strong confusion and diffusion properties.

However, Alvarez and Li [24] highlighted that chaotic systems degrade under finite precision digital implementation, leading to periodicity and reduced randomness. Further cryptanalysis by Li et al. [25] showed vulnerabilities to known-plaintext and chosen-plaintext attacks in certain chaos-based schemes.

Moreover, several chaos-based encryption methods fail comprehensive randomness evaluations such as the NIST SP 800-22 test suite [26], indicating that statistical image properties alone do not guarantee cryptographic security.

ECC-Based Medical Image Encryption Schemes

Elliptic Curve Cryptography (ECC) offers strong public-key security with smaller key sizes compared to RSA [27], making it suitable for telemedicine and cloud healthcare systems.

Liao et al. [28] proposed an ECC-based image encryption framework, while Zhang and Wang [29] integrated ECC with chaotic maps to enhance performance. However, Patel and Gupta [30] showed that ECC-based pseudo-random generators must be rigorously validated using NIST tests to ensure sufficient randomness.

Hybrid Chaos–ECC Image Encryption Frameworks

Hybrid schemes combining chaos and ECC have been proposed to leverage the strengths of both approaches. Belazi et al. integrated chaotic maps with ECC-based key scheduling and reported improved NPCR/UACI values [31].

However, such hybrid systems inherit finite-precision weaknesses from chaotic components [24] and increase computational complexity. Additionally, many studies do not fully validate pseudo-random sequences using standardized test suites such as NIST SP 800-22 [26].

The preceding review highlights the following gaps:

Chaos-based encryption schemes, while statistically promising, are susceptible to cryptanalysis due to finite precision effects and a lack of cryptographic rigor.

ECC based approaches often operate within limited algebraic environments and employ weak pseudo-random sequence generators that are not fully validated statistically.

Hybrid methods introduce superfluous complexity without adequately addressing known weaknesses or providing comprehensive randomness validation.

Considerations of medical image fidelity (lossless recovery, PSNR, MAE) are frequently under-reported, despite their critical importance in clinical applications.

These gaps underscore the necessity for a robust EC based encryption scheme that employs large prime fields in secp256k1, generates cryptographically strong pseudo random sequences validated via NIST SP 800-22, and concurrently ensures lossless medical image recovery with thorough performance evaluation.

Preliminaries

An Elliptic Curve is a set of points that satisfy a specific mathematical equation. Over a field Elliptic Curve is typically defined by an equation (1) of the form:

$$E: y^2 = x^3 + sx + t(mod)l \quad (1)$$

where s and t are constants that satisfy the condition:

$$4s^3 + 27t^2 \neq 0 \quad (2)$$

The condition in equation (2) ensures that the curve has no singular points.

For the proposed medical image processing, the cryptography is employed using the ECC over finite rings.

The condition in equation (2) ensures that the curve has no singular points.

For the proposed medical image processing, the cryptography is employed using the ECC over large finite fields.

ECC over Prime Fields of small prime

Finite fields have important applications in number theory, algebraic geometry, cryptography, and coding theory. A field is a set equipped with two operations: addition and multiplication, where both operations satisfy the field axioms. A finite field contains a finite number of elements and is signified as H(l), wherein p denotes the prime number. For the prime l, H(l) consists of the set {0,1,2,…l-1} with addition and multiplication defined modulo l. The finite field has no zero divisors and every non-zero element has a multiplicative inverse, making arithmetic operations straight-forward. Also, Finite fields over small finite fields may introduce performance bottle-necks when dealing with very large data sets, as the modulus is restricted to prime numbers, which may not align as efficiently with the data structure. Thus, the ECC over finite fields of large prime secp256 k1 is considered in the proposed secure healthcare information cryptography.

ECC over Finite Fields of large prime

The secp256k1 is an elliptic curve over Fp are specified by the sextuple T=(l, s ,t, Z, v, u). In a finite field (Fp), is given in the equation (1). From this equation 3, l is an integer and is defined as

$$l = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F \quad (3)$$

Where a and b are the elements of elliptic curve, i.e, s, t $\in Fp$ is defined as

s=0 and t=7

(4)

Z is base point of Elliptic Curve and is defined as in compressed format is

$Z(x_{g,}y_{g,})$=0279BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798

(5)

And v is the order of the curve, and u is the cofactor is

v = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8C D0364141

(6)

and

u = 1

(7)

The recommended secp256k1 is 256 bit and is associated with a Koblitz curve [11]. This curve is designed as non-super singular and cyclic.

Elliptic curve group operations

Group operation denoted with the addition symbol "+", which means that two given points P and Q coordinates are P =(x_1, y_1) and Q =(x_2, y_2), to compute third point R is such that

R = P+Q

(8)

(x_3, y_3)=(x_1, y_1)+(x_2, y_2)

(9)

Proposed Medical Image Cryptography

Nowadays, sharing medical images via insecure open systems has made cryptography techniques crucial for protecting information. The failure to meet user expectations for information protection and the inability to stop all privacy issues makes conventional methods more challenging. New and robust security mechanisms must be created to increase the confidentiality of medical images. Thus, a novel encryption technique based on ECC over finite field key generation is introduced in this research. The workflow of the proposed methodology is presented in Figure 1.

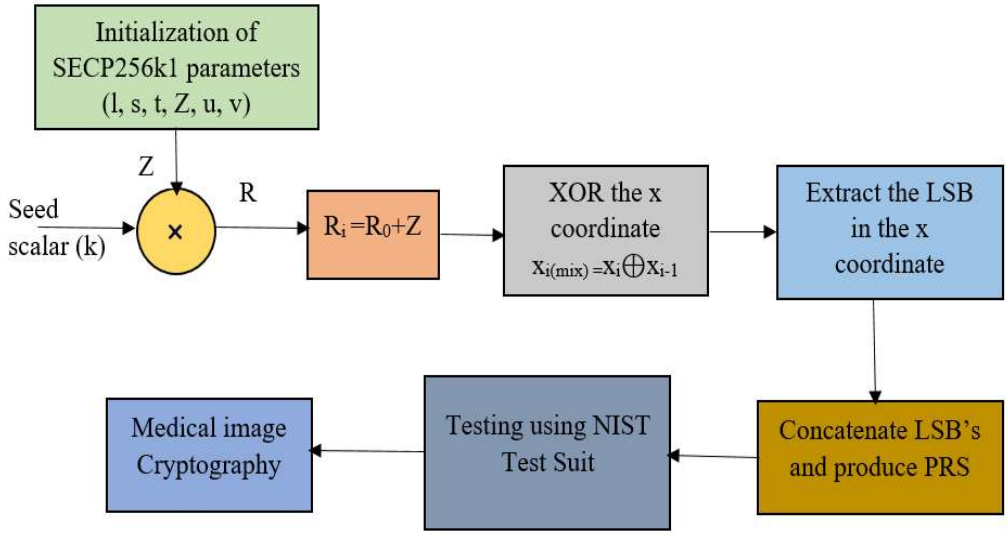


Figure 1. Block diagram of the proposed EC based pseudo-random sequence generator (PRSG) used for medical image cryptography.

The process begins with the initialization of SECP256k1 parameters (l, s, t, Z, u, v) and a seed scalar k. Point multiplication generates R, followed by point addition to obtain R_i. The x-coordinate values are mixed using XOR operations, and the least significant bits (LSBs) are extracted and concatenated to generate the pseudo-random sequence (PRS). The generated sequence is validated using the NIST statistical test suite before being applied for medical image cryptography.

Initially, the Pseudo Random Sequence (PRS) over Elliptic Curve Group defined over Prime Fields using secp256k1. The EC based PRSG proposed here is based on the secp256k1 elliptic curve. It proposes the hardness of Elliptic curve discrete logarithm problem (ECDLP). In this parameters (l, s, t ,Z, u, v) are specified. This scheme consists of three phases: First the initialization of secp256k1 parameters and random seed scalar k. Second computing points on elliptic curve. Third XOR technique is used for x coordinates. Last extracting LSB of XORed x-coordinate, which serves as pseudorandom sequences, these bits are evaluated by NIST test suite, then these PRS can be utilized for the medical image cryptography using the image taken from publically available medical image dataset.

Pseudo-Random Sequence Generation

The pseudo-random sequence generation process is performed using the following steps.

Step 1: **Initialization of secp256k1 parameters:** In this step all the specified parameters are initialized i,e. (l, s, t, Z, u, v) and also seed scalar k is generated such that k € (1, n-1). R_0 is computed using scalar multiplication.

$R_0=k^* Z(x_g, y_g)$ (10)

Step 2: Computing points on elliptic curve: In each iteration i, the next point in the sequence is computed by adding the base point G to the current state is given by

$R_i = R_{i-1} + Z$ (11)

This elliptic curve point computed by iterative addition.

Step 3: XOR transformation: To make unpredictable sequence, here we have complex technique called XOR transformation. In which elliptic curve point R_i has x coordinate x_i, and mixed sequence is computed by

$x_{i(mix)} = xi \oplus x_{i-1}$ (12)

where, $\oplus$ is XOR operation, x_{i-1} is initialized as constant seed, for i=0.

Step 4: Extracting LSBs from XORed x-coordinate: To provide high entropy and resist back tracking attacks, here we have 32 bit LSB extraction and it is concatenated to obtain pseudorandom sequences is given by the equation

$B=LSB(x_{i(mix(0))}) \| LSB(x_{i(mix(1))}) \| \ldots \| LSB(x_{i(mix(m))})$ (13)

Randomness Test Using NIST, Auto-Correlation, and Entropy

The randomness of the generated pseudo-random sequence is evaluated using three statistical techniques, namely the NIST statistical test suite, correlation analysis, and entropy analysis.

NIST Statistical Test Suite

The NIST statistical test suite is widely used to evaluate the randomness of binary sequences. The tests assume a null hypothesis that the generated sequences are ideally random and mutually independent. To validate the randomness properties of the proposed pseudo-random generator, fifteen different statistical tests from the NIST suite are applied. These tests are described as follows.

The NIST test suite is used to evaluate a set of sequences for randomness. The test assumes, as a null hypothesis, that the sequences are ideally random and mutually independent. For the analysis of the randomness 15 various tests are assessed. The fifteen various test evaluated using the NIST are:

Frequency (Monobit) Test: It checks whether the number of 0s and 1s in a sequence are approximately equal, as expected for a truly random sequence.

Frequency Test within a Block: It divides the sequence into blocks and then tests whether the number of 0's and 1's within each block is approximately equal. This helps detect if certain regions of the sequence are more biased than others.

Runs Test: It examine the total number of runs (consecutive sequences of the same bit) in the sequence and checks whether the number and lengths of these runs are as expected in a random sequence.

Test for the Longest Run of Ones in a Block: It divides the sequence into blocks and checks the length of the longest run of 1's in each block. It then compares these lengths to the expected distribution for a random sequence.

Binary Matrix Rank Test: It assesses the rank of matrices created from the sequence. The rank of a binary matrix is the number of linearly independent rows. The test checks if the sequence has the expected rank distribution for random matrices.

Discrete Fourier Transform (Spectral) Test: It identifies periodic features in the sequence that would indicate a deviation from randomness. It analyzes the peak heights in the DFT of the sequence.

Non-overlapping Template Matching Test: It searches for occurrences of a specified template (a short binary pattern) in the sequence. It counts how many times the template appears in non-overlapping blocks of the sequence.

Overlapping Template Matching Test: It searches for a specified template but allows overlapping matches. It helps detect periodicities and repetitive patterns that overlap within the sequence.

Maurer's "Universal Statistical" Test: It measures the sequence's compressibility, which is related to its randomness. A truly random sequence should be difficult to compress. The test analyzes how much the sequence can be compressed by comparing it to an expected theoretical result.

Linear Complexity Test: It evaluates the linear complexity of the sequence, which is the length of the shortest linear feedback shift register (LFSR) that can produce the sequence. A random sequence should have a high linear complexity.

Serial Test: It checks for patterns of consecutive bits by examining all possible overlapping m-bit patterns within the sequence. It then compares the frequency of these patterns to the expected distribution for a random sequence.

Approximate Entropy Test: assesses the frequency of all possible overlapping m-bit patterns in the sequence and compares these frequencies to those of (m+1)-bit patterns. It measures the randomness of the sequence by examining the entropy, or unpredictability, of the patterns.

Cumulative Sums Test (Forward and Backward): It calculates the cumulative sum of the bits (where 0 is -1 and 1 is +1) and checks whether this sum remains close to zero. It is performed in both the forward and backward directions to detect deviations from randomness throughout the sequence.

Random Excursions Test: It examines the number of times the cumulative sum of the sequence hits specific states (such as +1 or -1) and returns to zero. It checks for deviations from the expected number of state transitions.

Random Excursions Variant Test: It looks at the number of times each state is visited. It provides additional checks

on the randomness of the sequence by analyzing the frequency of visits to specific states.

Correlation Analysis

The correlation analysis is employed to assess how sensitive the PRNG is to small changes in the initial conditions. By calculating the correlation coefficients between the original sequence and the sequences generated with slightly altered initial condition, the sensitivity of the key is identified. If the generated sequence produces significantly different sequences (low correlation) with minor changes in initial keys that indicates the high sensitivity of the generated key. If the generated sequence is similar to the original sequence (high correlation), it indicates low sensitivity to the changes in the initial key. Let, the correlation between two sequences is indicated as:

$$CA(K_1,K_2)=\frac{\sum_{a=1}^{W}(c_a-\bar{c})(d_a-\bar{d})}{\sqrt{\sum_{a=1}^{W}(c_a-\bar{c})^2}\sqrt{\sum_{a=1}^{W}(d_a-\bar{d})^2}} \quad (14)$$

where, the correlation between the two sequences $K_1=[c_1,c_2,....c_W]$ and $K_2=[d_1,d_2,....d_W]$ is signified as $CA(K_1,K_2)$. $\bar{c}$ and $\bar{d}$ are the mean values of the sequences K_1 and K_2 respectively. The CA close to 1 indicates a strong correlation between the two sequences and 0 indicates little to no correlation between the sequences.

Information Entropy

Shannon introduced entropy, which is one of the most significant ideas in information theory to measure the uncertainty. An information system's uncertainty and unpredictability are reflected in its entropy. It evaluates the randomness with which a sequence is generated by the ECC over finite rings. It is expressed as:

$$G(K)=-\sum_{a=1}^{W}p(b_a)\log_2\left(\frac{1}{p(b_a)}\right) \quad (7)$$

where, the entropy for the sequence $K=[c_1,c_2,....c_w]$ is signified as $G(K)$. b_a is a unique value in the sequence and $p(b_a)$ is the probability b_a occurring in the sequence K.

Thus, the generated pseudo-random sequence that passes the three tests is utilized for the medical image encryption.

Encryption of Image

The input medical image is acquired from Diabetic Retinopathy (DR) dataset [26] and is encrypted using the key generated by the ECC over large secp256k1 finite fields. In the proposed method, the encryption is employed based on the following steps:

Step 1: The three color channels (Red, Green, and Blue) of the plain image P are progressively read row by row in order to create a one-dimensional (1D) array.

Step 2: Block 0, Block 1,..., Block 255 are the 256 blocks that make up the image P. Block 0 through Block 255 are the first blocks from which pixels are read in order.

Step 3: An index number, which is unique to each block directs the reading of the pixels inside that block.

Step 4: Then, the encryption is employed between the image and the ECC over finite fields of large prime secp256 k1 sequence. It is formulated as:

$M_x=A_x \oplus B_x$ (8)

where, the XOR operation is signified with the symbol, the sequence generated by the ECC is denoted as B_x. The encrypted image is denoted as M_x, and the current pixel is defined as A_x.

Thus, using the above mentioned steps the encryption is employed for the secure medical image sharing.

Decryption

The decryption is employed in the reverse process and it begins from the last block. The steps for the decryption are:

Step 1: The blocks will be referred to as Block 0, Block 1... Block 255. The first step in decryption is to access Block 255.

Step 3: Each block's decryption is done pixel by pixel. It advances towards the first pixel from the final pixel in the block.

Step 4: Then, the decryption is employed using:

$A_x = M_x \oplus B_x$ (9)

Step 6: where, the XOR operation is signified with the symbol, the sequence generated by the ECC is denoted as Bx. The decrypted image is denoted as A_x, and the current pixel is defined as M_x.

Thus, the decrypted image is accomplished and further processed for disease diagnosis.

5. Result and Discussion

The proposed cryptography of the medical image using the EC secp256k1over finite fields is implemented in PYTHON and is assessed based on various measures.

5.1 Experimental Outcome of the proposed scheme

The proposed PRSG generates random sequences, these sequences are evaluated by NIST test. Later these sequences are used as medical image cryptography, various evaluations methods are used for the performance measurement is discussed in this section.

The cryptography of the medical image using the sequence generated by the EC secp256k1 over finite is portrayed in this section.

5.1.1 Analysis of ECC-Based PRSG Using NIST Test Suite

The randomness performance of the proposed pseudo-random sequence generator (PRSG) is evaluated using the NIST statistical test suite. Table 1 presents the results of the core benchmark tests applied to the proposed PRSG and compares them with the existing PRB generator [32] and a fast multiple color image encryption [33].

The consistency of the obtained results indicates that the XOR transformation successfully removes structural regularities that typically occur in raw elliptic curve sequences.

Table 1. NIST test analysis of the proposed PRSG with the existing PRB generator.

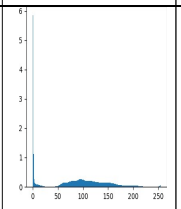
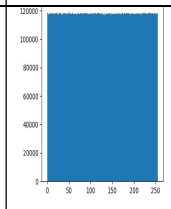
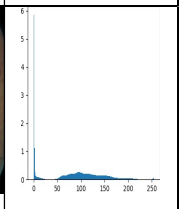
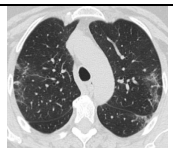
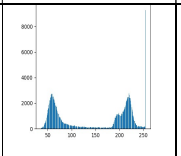
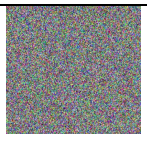
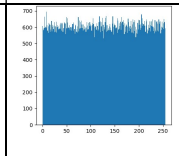
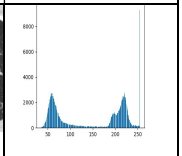
Test	P-value of Proposed PRSG	Ref. [32]	Ref. [33]	Result
1	0.8171	0.046169	0.804768	Pass
2	0.1781	0.681211	0.716425	Pass
3	0.2308	0.878529	0.290353	Pass
4	0.7089	0.674391	0.916169	Pass
5	0.4940	0.128851	0.322396	Pass
6	0.8833	0.149590	0.980152	Pass
7	0.2590	0.638151	0.303546	Pass
8	0.4882	1.000000	0.221742	Pass
9	0.0929	0.120402	0.340125	Pass
10	0.1062	0.197506	0.832177	Pass
11	0.6171	0.681211	0.171312	Pass
12	0.1781	0.051599	0.724727	Pass
13	0.2308	0.050388	0.5449	Pass
14	0.7089	0.499889	0.4591	Pass
15	0.4940	0.703017	0.5747	Pass

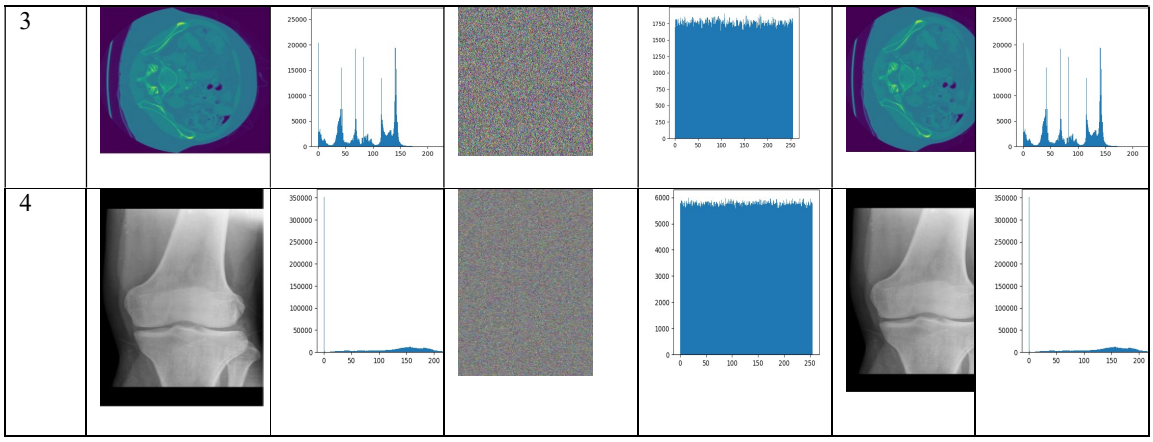
5.1.2 Analysis of ECC-Based PRSG Using Histogram

The medical image cryptography using ECC over prime fields is illustrated in Table 2. The table presents the histogram analysis of the original, encrypted, and decrypted images. Analyzing the histogram of the original image helps to understand the initial distribution of pixel values. It is crucial for comparing the changes after encryption and decryption. Any significant differences between the histograms of the original and decrypted images may indicate flaws in the encryption or decryption process, which could lead to image degradation or loss of information.

In the proposed approach, the similarity between the histograms of the original and decrypted images signifies that the encryption scheme achieves lossless information recovery while maintaining enhanced security.

Table 2. Histogram analysis of the proposed PRSG.

Sl.no	Original Image	Histogram	Encrypted Image	Histogram of encrypted image	Decrypted Image	Histogram of decrypted image
1						
2						



5.1.3 Correlation Coefficients

The correlation coefficient analysis of both the proposed PRSG and the existing ECPRBG [31] with vertical, horizontal, and diagonal directions is presented in Table 3. A minimal correlation coefficient is desirable because it indicates that the encrypted data is effectively randomized and does not reveal patterns related to the original data, thereby improving security.

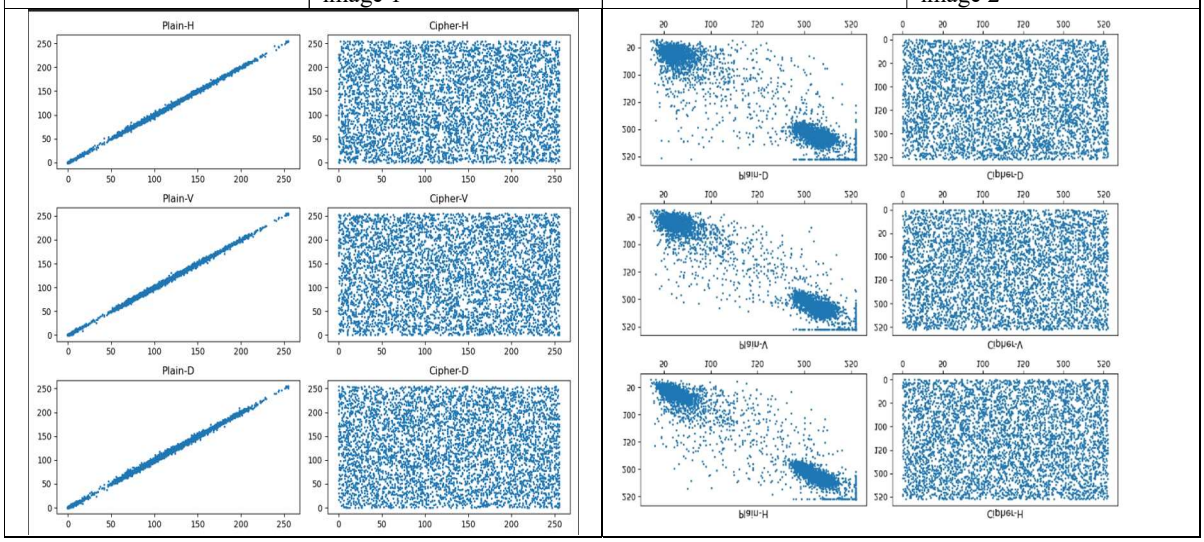
The medical image cryptography using the proposed PRSG achieves lower correlation values compared to EC-PRBG [32] and fast multiple color image encryption [33]. Hence, the proposed PRSG combined with ECC provides enhanced security. The obtained results show that there is negligible correlation between two adjacent pixels in the encrypted image, even though adjacent pixels in the plain image are highly correlated, as shown in Table 3.

Table 3. Vertical, horizontal, and diagonal correlation analysis of the proposed PRSG.

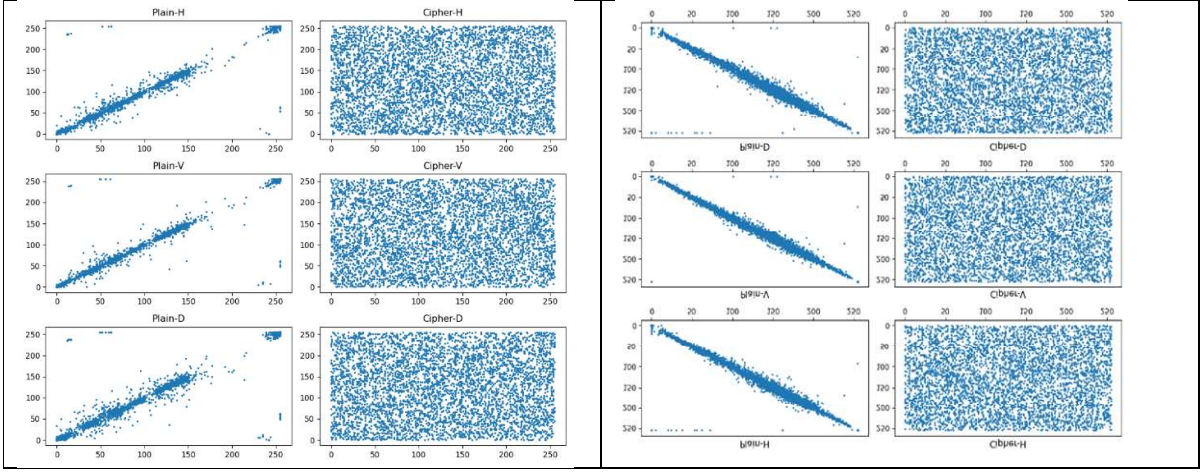
Scheme	Original image			Encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
1	0.99968	0.99962	0.99943	0.02675	-0.01102	0.00135
2	0.96866	0.96889	0.95223	-0.00211	-0.01005	0.00691
3	0.96702	0.97100	0.93831	0.01938	0.02289	0.01202
3	0.98398	0.98947	0.97583	-0.01857	0.00628	-0.01655
REF[32]	0.93915	0.96890	0.91686	-0.00287	0.03450	0.00196
REF [33]	0.9244	0.9166	0.8888	0.00231	0.00087	0.00094

Table 4. Vertical, horizontal, and diagonal correlation analysis of the proposed PRSG.

Correlation of image 1	Correlation encrypted image 1	Correlation of image 2	Correlation encrypted image 2



Correlation of image 3	Correlation encrypted image 3	Correlation of image 4	Correlation encrypted image 4



5.1.4 Sensitivity Analysis

NPCR (Number of Pixels Change Rate) measures the percentage of pixels that change when an image is encrypted and evaluates the diffusion property of an encryption algorithm. UACI (Unified Average Changing Intensity) measures the average intensity difference between the plain and encrypted images and evaluates the confusion property of encryption. Due to this property, known-plaintext attacks become impractical [27].

To evaluate this requirement, Table 5 presents the NPCR and UACI values for four medical test images using the proposed scheme and compares them with the existing method. The proposed method achieves NPCR values greater than 99.6% and UACI values around 33%, which indicates strong resistance against differential attacks. These results demonstrate that the proposed PRSG is highly suitable for secure medical image encryption.

Table 5. Sensitivity analysis of the proposed PRSG with existing method.

Scheme	NPCR	UACI
Test image-1	99.61%	33.88%
Test image-2	99.61%	34.68%
Test image-3	99.60%	33.09%
Test image-4	99.60%	34.64%
REF[32]	99.47%	30.48%
REF [33]	99.62%	33.31%

5.1.5 Experimental Analysis for Entropy, PSNR, MAE, and MSE

The experimental outcomes of the information entropy, PSNR, MAE, and MSE analysis for the proposed PRSG are presented in Table 6. The results obtained for four different medical images using the proposed PRSG are compared with the existing EC-PRBG method [32] and fast multiple color image encryption [33]. The comparison shows that the proposed PRSG achieves better performance in terms of entropy and error metrics, demonstrating its effectiveness for secure medical image encryption.

Table 6. Analysis of entropy, NPCR, MAE, and MSE of the proposed PRSG with existing method.

Scheme	Entropy	PSNR	MAE	MSE
1	8.0000	10.8408	86.41	5358.02
2	7.9985	10.7832	88.53	5429.49
3	7.9995	10.9796	84.56	5189.40
4	7.9999	10.8932	88.32	5293.75
Ref[32]	7.9971	8.5631	79.52	9305.32
Ref [33]	7.9990	8.0683	82.82	10281.1

Conclusions

This study presented a secure encryption for medical images, which is constructed from the elliptic curve secp256k1 over large finite fields. This introduces a novel approach for ECC-based pseudorandom sequence generator (PRSG). The generated sequences is strengthened by extraction of least significant bit (LSB) and XOR mixing process to produce highly unpredictable sequences. The proposed system achieves a high level of security by relying on the mathematical difficulty of the elliptic curve discrete logarithm problem (ECDLP) and remaining

computationally efficient for healthcare network environments. The standard randomness requirements confirmed by examining the sequences using the NIST statistical test suite. The applied XOR based refinement reduces detectable patterns in the raw elliptic curve outputs, thereby improving unpredictability and minimizing the risk of statistical attacks. Experimental findings demonstrate that the encryption process performs effectively across multiple security metrics. The histograms of encrypted images show a uniform distribution of pixel intensities, indicating that statistical features of the original image are concealed. Correlation analysis confirms that relationships between neighboring pixels are almost completely removed after encryption. In addition, the method shows strong resistance to differential attacks, with NPCR values above 99.60% and UACI values greater than 33%, reflecting effective diffusion and confusion properties. The entropy values of the encrypted images approach 8 bits per pixel, further confirming a high level of randomness. For medical applications, preserving image quality after decryption is essential. The proposed method ensures exact reconstruction of the original image without information loss. Improved PSNR values along with reduced MAE and MSE indicate that diagnostic clarity is maintained. This combination of strong security and reliable image recovery addresses common shortcomings found in several existing chaos-based, EC based, and hybrid encryption approaches. In summary, the developed EC based PRSG encryption scheme provides reliable security, strong statistical characteristics, computational practicality, and complete loss-less recovery. These features make it well suited for protecting sensitive medical images transmitted through telemedicine platforms, wireless healthcare systems, and cloud-supported medical networks.

REFERENCE

1. Zhou, J.; Cao, Z.; Dong, X. Security and privacy for cloud-based medical data sharing. IEEE Trans. Inf. Forensics Secur. 2019, 14, 317–330. https://doi.org/10.1109/TIFS.2018.2851286

2. Kumar, R.; Jung, K.H. A systematic survey on medical image encryption. J. Inf. Secur. Appl. 2020, 51, 102424. https://doi.org/10.1016/j.jisa.2019.102424

3. Schneier, B. Applied Cryptography, 2nd ed.; Wiley: New York, NY, USA, 1996.Wang, X.; Feng, L. Image encryption algorithm based on AES and chaotic systems. Signal Process. 2018, 142, 101–110. https://doi.org/10.1016/j.sigpro.2017.07.012

5. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt. Commun. 2011, 284, 3895–3903. https://doi.org/10.1016/j.optcom.2011.04.043

6. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004, 21, 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

7. Kocarev, L. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. 2001, 1, 6–21. https://doi.org/10.1109/7384.963463

8. Li, S.; Li, C.; Chen, G. Cryptanalysis of chaos-based image encryption. IEEE Trans. Circuits Syst. Video Technol. 2017, 27, 207–219. https://doi.org/10.1109/TCSVT.2016.2601627

9. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos 2006, 16, 2129–2151. https://doi.org/10.1142/S0218127406015970

10. Miller, V. Use of elliptic curves in cryptography. In Advances in Cryptology—CRYPTO ’85; Springer: Berlin, Germany, 1986; pp. 417–426. https://doi.org/10.1007/3-540-39799-X

11. Koblitz, N. Elliptic curve cryptosystems. Math. Comput. 1987, 48, 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

12. Mahalanobis, A.; Annamalai, K. Elliptic curve cryptography over rings. Des. Codes Cryptogr. 2016, 78, 277–296. https://doi.org/10.1007/s10623-014-9982-0

13. Joye, M.; Yen, S.M. The Montgomery powering ladder. In Cryptographic Hardware and Embedded Systems (CHES); Springer: Berlin, Germany, 2002; pp. 291–302. https://doi.org/10.1007/3-540- 36400

14. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; NIST SP 800-22; NIST: Gaithersburg, MD, USA,2010.

15. Çavu¸so ˘glu, Ü.; Kaçar, S.; Pehlivan, I. Secure image encryption using ECC and chaotic maps. Nonlinear Dyn. 2019, 95, 3179–3191. https://doi.org/10.1007/s11071-018-4677-4

16. Zhang, Y.; Xiao, D. An image encryption scheme based on elliptic curve and chaotic system. IEEE Access 2018, 6, 34603–34617. https://doi.org/10.1109/ACCESS.2018.2846595

17. Wang, X.; Liu, L. ECC-based image encryption algorithm for medical images. Multimed. Tools Appl. 2020, 79, 18343–18361. https://doi.org/10.1007/s11042-019-08366-8

18. Rukhin, A. NIST Statistical Test Suite; NIST: Gaithersburg, MD, USA, 2010.

19. Gonzalez, R.C.; Woods, R.E. Digital Image Processing, 4th ed.; Pearson: New York, NY, USA, 2018.

20. Wu, Y.; Zhou, Y.; Bao, L. Image encryption using NPCR and UACI analysis. Inf. Sci. 2014, 278,434–447. https://doi.org/10.1016/j.ins.2014.03.025

21. Wang, Z.; Bovik, A.C. Modern image quality assessment. IEEE Signal Process. Mag. 2006, 23, 98–117. https://doi.org/10.1109/MSP.2006.1597056
22. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcat. Chaos 1998, 8, 1259–1284. https://doi.org/10.1142/S021812749800098X
23. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004, 21, 749–761. https://doi.org/10.1016/j.chaos.2003.12.022
24. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos 2006, 16, 2129–2151. https://doi.org/10.1142/S0218127406015970
25. Li, S.; Chen, G.; Mou, X. On the security of a class of image encryption schemes. IEEE Trans. Circuits Syst. Video Technol. 2005, 15, 1001–1006. https://doi.org/10.1109/TCSVT.2005.853405
26. National Institute of Standards and Technology. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (SP 800-22 Rev.1a); NIST: Gaithersburg, MD, USA, 2010.
27. Koblitz, N. Elliptic curve cryptosystems. Math. Comput. 1987, 48, 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
28. Liao, X.; Lai, S.; Zhou, Q. A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process. 2011, 90, 2714–2722. https://doi.org/10.1016/j.sigpro.2010.12.004
https://doi.org/10.3390/1010000Version April 13, 2026 submitted to Journal Not Specified 15 of 15
29. Zhang, Y.; Wang, X. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf. Sci. 2015, 273, 329–351. https://doi.org/10.1016/j.ins.2014.03.102
30. Patel, V.; Gupta, R. Randomness evaluation of elliptic curve cryptographic pseudo-random generators. Int. J. Netw. Secur. 2018, 20, 102–110.
31. Belazi, A.; Khan, M.; El-Latif, A.A.A.; Belghith, S. Efficient cryptosystem approaches based on chaotic maps and elliptic curve cryptography. Multimed. Tools Appl. 2019, 78, 20733–20757. https://doi.org/10.1007/s11042-019-7264-3
32. AlOmar Reyad.; Mohamed Karar.; Kadry Hamed. Random bit generator mechanism based on elliptic curves and secure hash function. In Proceedings of the IEEE International Conference on Computing, Communication and Security (ICCCS), Rome, Italy, 23–25 October 2019; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
33. Zhang, Y.; Liu, H.; Wang, X. Secure medical image encryption using chaotic systems. Clust. Comput. 2024, 27, 12345–12360. https://doi.org/10.1007/s10586-024-04919-0.