Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points

S. V. Sathyanarayana[1], M. Aswatha Kumar[2] and K. N. Hari Bhat[3]
(Corresponding author: S. V. Sathyanarayana)
Department of Electronics & Communication Engineering, JNNCE, Shimoga-577 204, Karnataka, India[1]
Department of Information Science & Engineering, MSRIT, Bangalore, Karnataka, India[2]
Department of Electronics & Communication Engineering, NCET, Bangalore, Karnataka, India[3]
(Email: svs.tce@gmail.com)
(Received July 30, 2009; revised and accepted Mar. 4, 2010)

Abstract

In this paper, cyclic elliptic curves of the form $y^2 + xy = x^3 + ax^2 + b, a, b \in GF(2^m)$ with order M is considered in the design of a Symmetric Key Image Encryption Scheme with Key Sequence derived from random sequence of cyclic elliptic Curve points. P with co-ordinates (x_P, y_P) which satisfy the elliptic curve equation is called a point on elliptic curve. The order M is the total number of points (x,y) along with $x = \infty, y = \infty$ which satisfy the elliptic curve equation. Least integer N for which NP is equal to point at infinity O is called order of point P. Then P, 2P, ... (N-1)P are distinct points on elliptic curve. In case of cyclic elliptic Curve there exists a point P having the same order N as elliptic curve order M. A finite field $GF(p)$ (p$\geq$ N) is considered. Random sequence $\{k_i\}$ of integers is generated using Linear Feedback Shift Register (LFSR) over $GF(p)$ for maximum period. Such sequences are called maximal length sequences and their properties are well established. Every element in sequence $\{k_i\}$ is mapped to k_iP which is a point on cyclic elliptic Curve with co-ordinates say (x_i, y_i). The sequence $\{k_iP\}$ is a random sequence of elliptic curve points. From the sequence (x_i, y_i) several binary and non-binary sequences are derived. These sequences find applications in Stream Cipher Systems. Two encryption algorithms - Additive Cipher and Affine Cipher are considered. Results of Image Encryption for a medical image is discussed in this paper. Here, cyclic elliptic Curve over $GF(2^8)$ is chosen for analysis.

Keywords: Additive cipher, affine cipher, cyclic elliptic curve, image encryption, stream cipher system

1 Introduction

Security is of utmost importance in present day communications. But the communication networks such as mobile networks and Internet are public media and are not suitable for direct transmission of confidential information. Sensitive information like medical and legal records, credit ratings, Business transactions, Voice mail, images like a protected geographical area of military importance or drawings which correspond to critical components of the system, defence information are routinely exchanged through Internet.

Cryptography is a practical means for protecting these private information. Cryptosystems are divided between those that are secret key or symmetric and those that are public key or asymmetric. There is a further division of symmetric cryptosystems into block and stream ciphers. Block ciphers operate with a fixed transformation on large blocks of plaintext data; Stream ciphers operate with a time varying transformation on individual plaintext digits. Stream ciphers are fast and simple compared to block ciphers. The main challenge in Stream Cipher Cryptography is the generation of a long unpredictable key sequence from a short and random seed key. For a sequence to be random the period of the sequence must be large and various patterns of a given length must be uniformly distributed over the sequence.

The sequence may be generated in various ways, but nearly all of these methods employ feed back shift registers. One of the main reasons for this is that they are easily obtainable [1, 23, 33]. The key stream generators designed using Linear Feedback Shift Register are easily analyzed using algebraic techniques. If the feedback

is non-linear for a given number of stages of shift register, the resulting key sequence will be of higher linear complexity [1, 23] and hence more secure. The key sequence generator discussed in this paper is a variation of the above basic scheme, where, the key sequence elements are random sequence of elliptic curve points. Considerable research has been made in the design and analysis of pseudo random generators over the last decade. Some of them are reported in [9, 13, 23]. The key sequence derived from sequence of cyclic elliptic curve points are discussed in [29]. It is shown that such sequence satisfy FIPS-140 and NIST tests. Hence, they are suitable for cryptographic applications. The random bit generators based on chaotic maps are discussed in [22], where, the properties of chaotic systems are used to design a random bit generator, called CCCBG, in which two chaotic systems are cross-coupled with each other. The CCCBG can be used in many applications requiring random binary sequences and also in the design of secure cryptosystems.

Images are routinely used in diverse areas such as medical, military, science, engineering, art, entertainment, advertising, education as well as training. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Recently many chaos-based image encryption schemes were proposed [4] - [27]. Essentially, these schemes can be classified as one class and they are composed of two parts: Position permutation and Diffusion of pixel value with the same cipher-text feedback function. The operations involved in the two basic parts are determined by a random sequence generated by iterating a chaotic dynamic system.

Towards this direction, [6] presents an efficient chaos based feedback stream cipher (ECBFSC) for image cryptosystems. Mazleena Salleh et al. [27] discuss an alternative symmetric-key encryption algorithm for securing images, namely Secure Image Encryption (SIP) that is based on chaos. [11] introduced a chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. The external secret key is used to derive the initial conditions for the chaotic maps, and is employed with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the pixels are encrypted using an iterative cipher module based feedback and data-dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information.

To make the cipher more robust against any attack, the secret key is modified after encryption of each pixel of the plain image. In [20] a new image encryption approach using combinational permutation technique is proposed. The main idea behind the work is that image can be viewed as an arrangement of bits, pixels and blocks. Zeghid et al. [35] proposes new encryption schemes as a modification of AES algorithm. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES image encryption algorithm in order to increase the image security and in turn the encryption performance.

In this paper, cyclic elliptic curves of the form $y^2+xy = x^3 + ax^2 + b$, $a, b \in GF(2^m), b \neq 0$ is considered. elliptic curve is essentially a cubic equation in two variables, x and y, with coefficients from a field satisfying certain conditions. In cryptographic applications the coefficients are chosen from finite fields of the form $GF(2^m)$ [2, 5, 15, 24]. Each pair of (x, y) which satisfies the cubic equation is called a point on the elliptic curve. The set of all points on the elliptic curve along with the point at infinity O constitutes an additive Abelian group where the addition operation is based on the geometrical properties of elliptic curve. The total number of points on the elliptic curve along with the point at infinity O is called order of the elliptic curve denoted by M.

The order N of a point P on an elliptic curve is defined as the smallest integer N such that NP = O (point at infinity) N $\leq$ M [12, 17, 18]. For certain choice of a and b it is possible to choose a base point P of highest order N = M which is square free. That is, square root of M is not an integer [7]. Further, P, 2P, 3P... MP are the M points of elliptic curve, where MP is the point at infinity. Such an elliptic curve is called as **c**yclic elliptic Curve. In general, there are $\phi(M)$ points of order M, where ϕ is Euler's Totient Function [12]. A Linear Feedback Shift Register (LFSR) is used for generating sequence of integers $\{k_i\}$ modulo p, a prime, where p $\geq$ M. The properties of such sequences are well established [1, 25]. Every element in sequence $\{k_i\}$ is mapped to k_iP which is a point on cyclic elliptic curve with co-ordinates say (x_i, y_i).

The sequence $\{k_iP\}$ is a random sequence of elliptic curve points. From the sequence (x_i, y_i) several binary and non-binary sequences are derived and their randomness properties are investigated in [29]. Choosing a linear feedback with connection polynomial primitive over GF(p), can generate periodic sequence with maximum period [10]. For any choice of n-stages > 1, an appropriate feedback connection can be obtained using an n^{th} degree primitive polynomial over GF (p). It can be shown under this condition; the sequence $\{k_i\}$ is periodic (with all initial values $k_{n-1}, k_{n-2} \ldots k_1, k_0$ not zero) and is of period $p^n - 1$. If the cyclic elliptic Curve is chosen, the random sequence $\{k_iP\}$ covers all points in elliptic curve and can be used for encryption and decryption. It can be noted that the sequence is a sequence of elliptic curve points with (M-1) elements excluding point at infinity and has inherent non-linearity. Such sequences find applications in Stream Cipher Systems [30, 31, 32].

To investigate the random properties of sequences derived from $\{k_iP\}$ sequence, cyclic elliptic curve, $y^2+xy = x^3 + ax^2 + b$, $a, b \in GF(2^8)$ is considered [29]. In this paper, an application of pseudo random sequences based on the properties of random numbers and cyclic elliptic curves in image encryption is presented.

2 The Proposed Random Sequence Generator

As mentioned earlier, the random sequence of elliptic curve points is generated in two separate stages. In the first stage, a random sequence $\{k_i\}$ of integers over $GF(p)$ is generated using Linear Feedback Shift Register (LFSR) over GF(p). In the second stage, random sequence of elliptic curve points is generated using the sequence $\{k_i\}$. That is, each element k_i of sequence $\{k_i\}$ is mapped to k_iP to get elliptic curve point (x_i, y_i). The sequence $\{k_iP\} = \{(x_i, y_i)\}$ is a random sequence of elliptic curve points. Random integer sequence can be generated using linear recurrence relation defined over finite field $GF(p)$ where $p \geq N$. Such a recurrence relation can be implemented using LFSR. In general, with n–stages and appropriate feedback connection, periodic sequence with period $p^n - 1$ can be generated. The sequence $\{k_i\}$ is random sequence of elements from 0 to p-1. This sequence is referred as Basic Sequence in this work. The basic sequence is used to generate the random sequence of elliptic curve points over $GF(2^m)$ as shown in Figure 1.

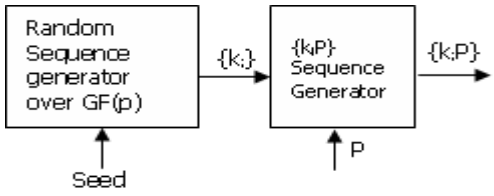

Figure 1: Block diagram of the proposed elliptic curve based pseudo random generator

2.1 Algorithm for Generating Random Sequence of Cyclic Elliptic Curve Points

In the proposed scheme, the random sequence of cyclic elliptic curve points is generated as per the step by step procedure given below [29]:

1) Construct cyclic elliptic curve $y^2 + xy = x^3 + ax^2 + b$ by choosing the appropriate constants a and b (b not equal to zero) over $GF(2^m)$ based on the irreducible polynomial of degree m over $GF(2)$ [12]. The following algorithm is used to construct cyclic elliptic curves [21].

```
Procedure construct( )
  repeat
  choose E (i.e. a and b) at random
  compute M
  until M is square free
end
```

2) Using exhaustive search, find the order of each point denoted by N and choose base point P having largest order N equal to order of the elliptic curve M.

3) Choose a prime integer p greater than the order of base point P.

4) For LFSR, choose a primitive connection polynomial over GF (p) of degree n so that maximal length sequence can be obtained of period $p^n - 1$ [10].

5) For each number k_i generated, obtain k_iP from pre-computed and stored points P, 2P, 3P, ... (M-1)P.

6) The key sequence is sequence of points $k_iP = (x_i, y_i)$ on elliptic curve.

The following example illustrates the above algorithm for generating the random sequence of cyclic elliptic curve points over $GF(2^8)$.

Example 1. *An elliptic Curve $y^2 + x^y = x^3 + g^4x^2 + g^2$ is constructed over $GF(2^8)$ based on primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$ over $GF(2)$ (where g is a primitive element in $GF(2^8)$). Using exhaustive search, the total number of elliptic curve points is found to be M=240 including O (point at infinity). Also, the order of each point is found using doubling and addition equations [12], [34]. The maximum order is found to be N=240. For example, $P = (g^{11}, g^{119})$ is chosen as the base point, which has the order 240. It can be seen that $N = M = 240$ is square free. Hence the given elliptic curve group is cyclic. Further, $P, 2P, \cdots, 240P$ generates all the elements of elliptic curve over $GF(2^8)$. The random sequence of cyclic elliptic curve points discussed is generated as follows.*

1) A prime integer $p = 241$ greater than the order of base point $P = (g^{11}, g^{119})$, $N = 240$ is chosen.

2) For LFSR, a primitive connection polynomial over $GF(241)$ of degree 4, $f(x) = x^4 + 240x + 228$ is chosen [10]. $x^4 + 240x + 228 = 0$ gives us the characteristic equation of recurrence relation $k_i = -240k_{i-3} - 228$ mod 241, that is, $k_i = k_{i-3} + 13$, i greater than or equal to 4. The feedback coefficients are 0, 0, 1and 13. The scheme is shown in Figure 2.

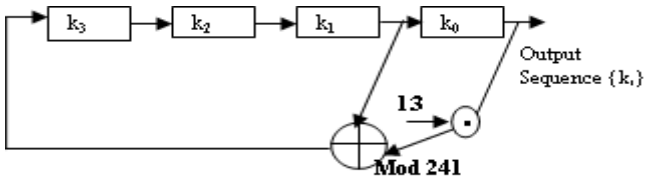

Figure 2: A LFSR over GF(241)

3) For each number k_i generated, k_iP is obtained from pre-computed and stored points $P, 2P, 3P, \cdots (N-1)P$. While computing $P, 2P, 3P, \cdots (N-1)P$ adding and doubling rule [12, 17] is used.

4) The key sequence is sequence of points (x_i, y_i) on cyclic elliptic curve.

It is to be noted that, if N is order of any point, then there are $\phi(N)$ points of same order. The output sequence k_i generated is a random sequence over $GF(241)$. As 240P is the point at infinity, if the output sequence $\{k_i\}$ contains 240 or zero, (x_i, y_i) becomes indeterminate. To avoid this, whenever k_i is 240 or zero, k_i is replaced by integer, say 5 or 3 respectively.

3 Encryption Algorithms Using Random Key Sequence of Cyclic Elliptic Curve Points

Generally elliptic curve is used in public key systems. The security is based on discrete log problem and has advantages over RSA scheme [17]. In this paper, the usage of elliptic curves in Private Key Cryptosystems is discussed. A Stream cipher, which is much faster, compared to Block cipher, has been developed with key sequences derived from random cyclic elliptic curve points. Schemes of generation of random sequence of elliptic curve points are discussed in Section 2. Its application in Stream Cipher System for encrypting images is presented here. Eight schemes of image encryption using sequence $\{k_iP\}$ are designed and comparison of encrypted image is done using Histogram, Entropy, Correlation Coefficient and Encryption Time. The algorithms are applicable to other forms of data like speech samples, text and video apart from images.

3.1 Additive Stream Cipher System

Here a synchronous additive stream cipher system encrypting images is designed where the key sequence derived from a random sequence of elliptic curve points. The block diagram is as shown in Figure 3. The same key sequence $\{k_iP\}$ is used for both encryption and decryption process.

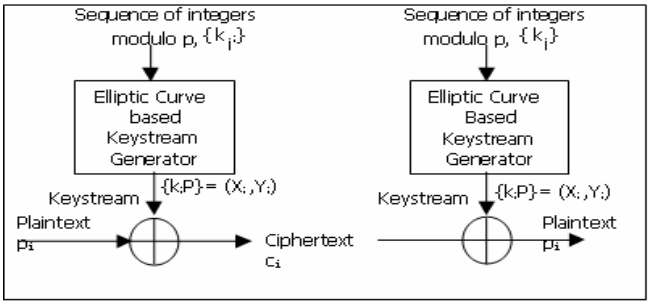

Figure 3: Elliptic curve based additive stream cipher system

Various Encryption and Decryption algorithms are discussed. Any type of files like text, document or image can be Encrypted and Decrypted byte by byte. In this paper, image encryption is considered as an example. The key sequence is in the form of x and y coordinates of randomly generated elliptic curve points, $x, y \in GF(2^8)$. Here, plaintext is represented as sequence of image pixels, p_i. The key sequence is represented as $\{k_iP\}$, where P is a base point in the chosen elliptic curve. Let (x_i, y_i) be coordinates of $k_iP, x_i, y_i \in GF(2^8)$. The ciphertext is denoted by c_i. The length of the message is taken as 'd' bytes. Here, six different types of Encryption/Decryption Algorithms are considered and they are given below.

In what follows elements $c_i, p_i, x_i, y_i, Lx_i, Ly_i$ *and* Lz_i are elements of $GF(2^8)$ and $\oplus$ is addition operation in $GF(2^8)$.

Scheme-1: Using only x-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{x_i\}$]. Here, only x-coordinates of sequence $\{k_iP\}$ are considered for encryption/decryption process.

Enciphering algorithm:

$$c_i = p_i \oplus x_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus x_i, \forall i = 0, 1, \cdots, d-1.$$

Scheme-2: Using only y-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{y_i\}$]. Here, only y-coordinates of $\{k_iP\}$ sequence are considered for Encryption/decryption process.

Enciphering algorithm:

$$c_i = p_i \oplus y_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus y_i, \forall i = 0, 1, \cdots, d-1.$$

Scheme-3: Using x or y coordinates depending on the output of another random binary sequence b_i generated using any of the well known techniques [25]. Let z_i be the i^{th} key element, then $z_i = x_i$ if $b_i = 0, z_i = y_i$ if $b_i = 1$.

Enciphering algorithm:

$$c_i = p_i \oplus z_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus z_i, \forall i = 0, 1, \cdots, d-1.$$

Scheme-4: Using only least significant bit (LSB) of x-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{Lx_i\}$]. Here, LSB of x-coordinates of eight consecutive random elliptic curve points in the sequence $\{k_iP\}$ are extracted and formed as a key byte, let it

be Lx_i. Then it is used for encryption/decryption process as per the algorithm given below.

Enciphering algorithm:

$$c_i = p_i \oplus Lx_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus Lx_i, \forall i = 0, 1, \cdots, d-1.$$

Scheme-5: Using only LSB of y-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{Ly_i\}$]. Here, LSB of y-coordinates of eight consecutive random elliptic curve points in the sequence $\{k_iP\}$ are extracted and formed as a key byte, let it be Ly_i. Then it is used for encryption/decryption process as per the algorithm given below.

Enciphering algorithm:

$$c_i = p_i \oplus Ly_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus Ly_i, \forall i = 0, 1, \cdots, d-1.$$

Scheme-6: Selecting LSB of the sequences generated in Scheme-4: [Sequence $\{Lz_i\}$]. Here, x and y coordinates are selected randomly depending on the output of another random binary sequence b_i generated using any of the well known techniques [25]. Let z_i be the i^{th} key element, then $z_i = x_i$ if $b_i = 0, z_i = y_i$ if $b_i = 1$. Extract the LSB of eight such points (z_i's), and form as a key byte, let it be Lz_i. Then it is used for encryption/decryption process as per the algorithm given below.

Enciphering algorithm:

$$c_i = p_i \oplus Lz_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = c_i \oplus Lz_i, \forall i = 0, 1, \cdots, d-1.$$

3.2 Affine Systems

Generally, affine system is one where addition and multiplication schemes are used in sequence. In this paper, an elliptic curve based affine stream cipher system is designed. As mentioned earlier, a random sequence of elliptic curve points, called $\{k_iP\}$ sequence, is generated. Both x and y coordinates of random elliptic curve points are used as keys in two different encryption stages, one in an additive stage and another in a multiplication stage as explained in Scheme-7 and Scheme-8. Arithmetic is in $GF(2^m)$. So, this method is a super encryption scheme. This has an added advantage of increased security level [33].

Scheme-7: This scheme uses x-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{x_i\}$] in additive stage and y -coordinates of $\{k_iP\}$ as key sequence [Sequence $\{y_i\}$] in multiplicative stage of affine encryption/decryption algorithm. When y_i is zero use any non-zero element as key sequence in multiplicative stage.

Enciphering algorithm:

$$c_i = (p_i.y_i) \oplus x_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = (c_i \oplus x_i).y_i^{-1},$$

where y_i^{-1} is multiplicative inverse of $y_i, \forall i = 0, 1, \cdots, d-1$.

Scheme-8: This scheme uses y-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{y_i\}$] in additive stage and x-coordinates of $\{k_iP\}$ as key sequence [Sequence $\{x_i\}$] in multiplicative stage of affine encryption/decryption algorithm. When x_i is zero use any non-zero element as key sequence in multiplicative stage.

Enciphering algorithm:

$$c_i = (p_i.x_i) \oplus y_i, \forall i = 0, 1, \cdots, d-1.$$

Deciphering algorithm:

$$p_i = (c_i \oplus y_i).x_i^{-1},$$

where x_i^{-1} is multiplicative inverse of $x_i, \forall i = 0, 1, \cdots, d-1$.

3.3 Computing Entropy and Correlation Coefficient

The performance of the encryption algorithms discussed so far are measured by computing Entropy and correlation coefficient of the encrypted images and then comparing Entropy and Correlation Coefficient of the input image.

1) Entropy. Entropy is a measure of uncertainty. Higher the value of entropy of encrypted image, better the security. The Entropy En of the input image and the encrypted image is calculated as:

$$E_n = \sum_{i=0}^{255} (\mathrm{p(i)} \ * \ \log_2(\ 1/\mathrm{p(i)}). \qquad (1)$$

p(i) = Number of occurrence of a pixel/Total number of pixel in the image.

2) Correlation Coefficient. The correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plainimage/encrypted image respectively is analyzed. The

procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulae [6]. In the following, x and y refer to values of adjacent pixels in the image.

$$\begin{aligned} Cov(x,y) &= E(x-E(x))(y-E(y)). \\ r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)D(y)}}. \end{aligned}$$

In numerical computations, the following discrete formulas are used with R = 1000:

$$E(x) = \frac{1}{R}\sum_{i=1}^{R} x_i \quad (2)$$

$$D(x) = \frac{1}{R}\sum_{i=1}^{R}(x_i - E(x))^2 \quad (3)$$

$$cov(x,y) = \frac{1}{R}\sum_{i=1}^{R}(x_i - E(x))(y_i - E(y)) \quad (4)$$

4 Results of Image Encryption

Eight encryption algorithms using random sequence of elliptic curve points as key sequence are discussed above. These algorithms are used in encrypting various images and results are discussed [28].In this paper, Example 2 given below gives the encrypted images of an input medical image. The algorithms are compared based on the histogram, entropy and correlation coefficient.

Example 2. *The system is tested for a medical image (CT scanned brain image) which is a gray scale image of size 55.4 KB. As mentioned earlier, Medical imaging systems, where the diagnostic images and videos of all patients are required to be stored in lossless forms, the only choice is to use lossless compression or to leave the images/videos uncompressed [14]. The schemes designed in this paper are suitable for such cases. The input brain image and respective encrypted images are shown in Figure 4. The corresponding histograms are shown in Figure 5.*

Table 1 gives the variation of the histogram which indicates that the Scheme-4 to Scheme-8 are flatter compared to the histograms of the Scheme-1 to Scheme-3 indicating that the Scheme-4 to Scheme-8 are superior compared to Scheme-1 to Scheme-3. Table 2 lists the values of entropy computed for input and the encrypted images as per the formula given in Equation 1. The input entropy for the input medical image is 1.951202. It can be seen from the table that the entropy of the encrypted image is very close to eight which is the ideal value indicating that every pixel in the encrypted image occurs with equal probability. In this example, among Scheme-4 to Scheme-8, the performance of Scheme-7 is superior as the value of histogram variation indicated in Table 1 is 75 which is less compared to other schemes and the entropy value of Scheme-7 given in Table 2 is 7.9971 which is highest compared to all other schemes.

The horizontal, vertical and diagonal correlation coefficient of the input BMP image is 0.8356, 0.8217 and 0.7699 respectively. Results of horizontal, diagonal and vertical directions are obtained as shown in Table 3 through Table 5. It is clear from the table, the correlation coefficient values are small which implies that there is negligible correlation between the two adjacent pixels in the encrypted image. However, the two adjacent pixels in the plainimage are highly correlated. Table 6 indicates the encryption time consumed by various algorithms. It can be observed that except the affine stream cipher schemes (Scheme-7 and Scheme-8) other algorithms can run very fast with less than 0.28 second indicating that it can be effectively used in medical image transmission applications.

5 Security Aspects of the Proposed System

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, security aspects of the present elliptic curve based image encryption algorithm will be discussed. It is seen that the present cryptosystem is secure against the Statistical, Brute force and cryptanalytic attacks [23, 25, 33]. What follows are the security aspects of the proposed system using the available techniques of analysis.

5.1 Key Space

For a secure cryptosystem, the key space should be large enough to make the brute force attack infeasible. The present elliptic curve pseudorandom key sequence generator has a flexible, moderately large key space, which is estimated as follows:

The key space comprises of - number of stages in shift register over GF(p), initial contents of shift registers, feedback coefficients, possible elliptic curves and base point. Then the size of key space KS can be estimated as below:

Let the number of stages of LFSR over $GF(p)$ be n.

The number of possible initial values of LFSR is $(p^n - 1)$.

The number of possible feedback coefficients is $\Phi(p^n - 1)/n$.

The number of distinct elliptic curves over $GF(2^m)$ is $2(2^m - 1)$.

The number of base points in cyclic elliptic curve having largest order M is $\Phi(M)$.

Then the total number of possible keys is the size of key space KS and is equal to the product of the above,

$$KS = n * (p^n - 1) * (\Phi(p^n - 1)/n * 2(2^m - 1) * \Phi(M).$$

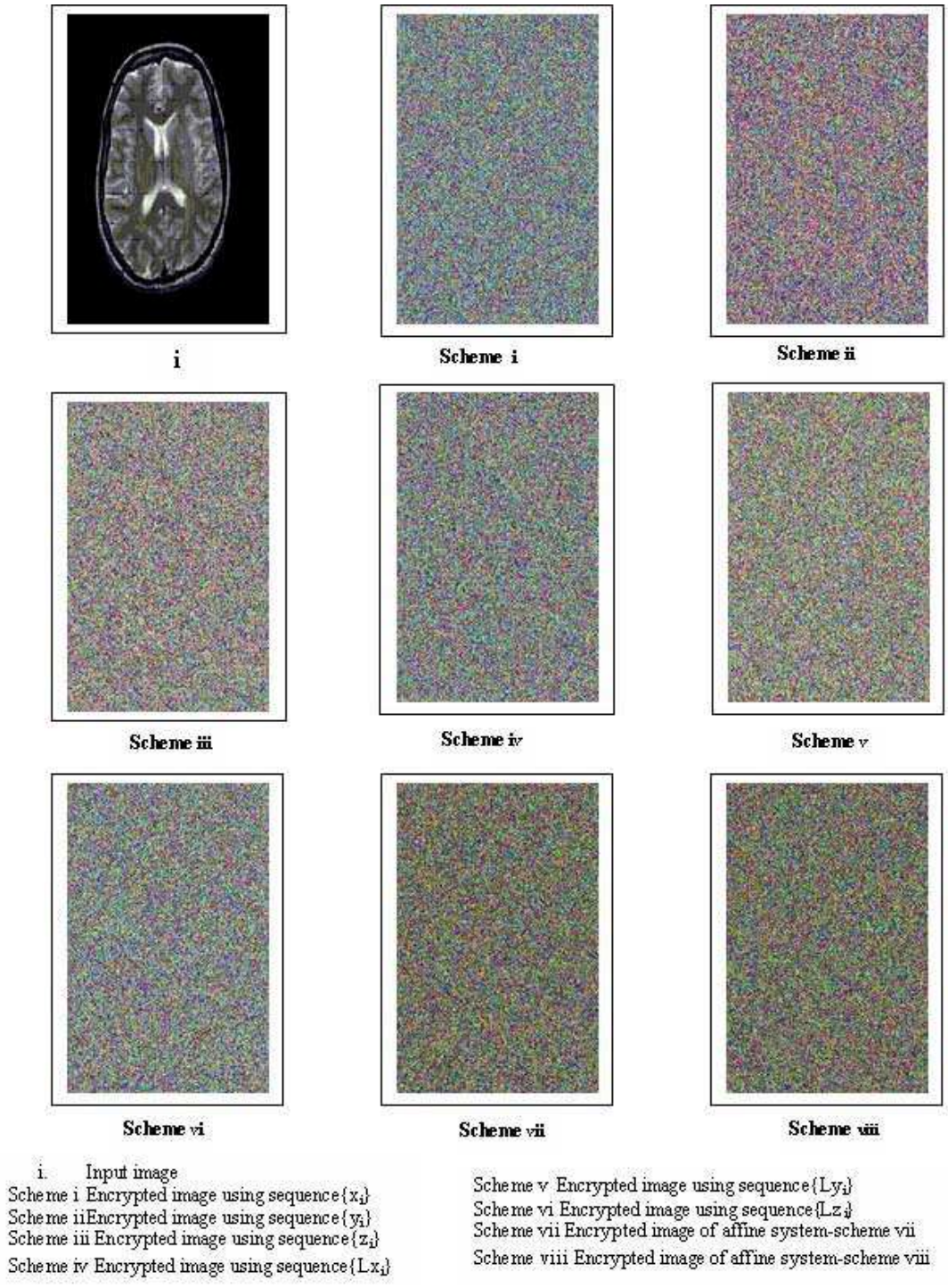

Figure 4: Input and encrypted images of brain image

Table 1: Difference between maximum and minimum values of histograms of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Variations	528	678	501	100	215	103	75	85

Table 2: Entropies of the encrypted images of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Entropy	7.61	7.665	7.807	7.994	7.978	7.994	7.997	7.996

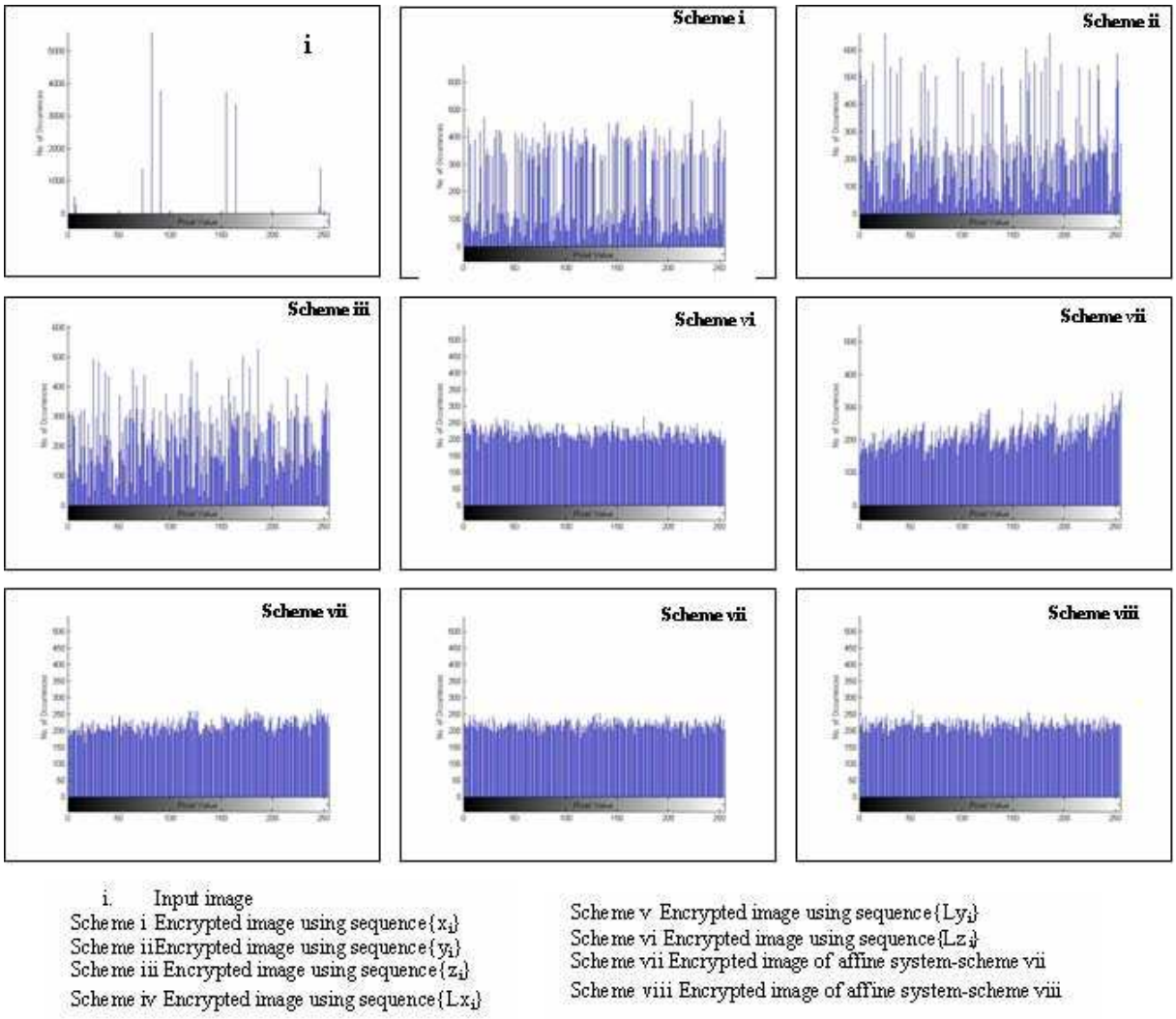

Figure 5: Histograms of input and encrypted images of brain image

Table 3: Horizontal correlation coefficient of the encrypted images of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Corr. Coef.	0.002	0.001	-7.0e-004	-0.003	0.006	0.004	-0.001	3.70e-004

Table 4: Vertical correlation coefficient of the encrypted images of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Corr. Coef.	0.0013	-0.0019	0.0023	0.0101	-0.0047	-0.0021	0.0053	1.40e-004

Table 5: Diagonal correlation coefficient of the encrypted images of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Corr. Coef.	0.0073	-2.9e-004	4.7e-004	-0.0058	0.0058	0.0043	-3.2e-004	-5.2e-005

Table 6: Encryption time of the various schemes of encryption of brain image

	Scheme-1	Scheme-2	Scheme-3	Scheme-4	Scheme-5	Scheme-6	Scheme-7	Scheme-8
Time in secs	0.165	0.165	0.165	0.219	0.219	0.274	1.373	1.373

For a given cyclic elliptic curve,

$$KS = n * (p^n - 1) * (\Phi(p^n - 1)/n * \Phi(M),$$

where M is order of the cyclic elliptic curve and Φ is the Euler's Totient Function.

It is to be noted that unless all the above elements of the key space are known to the attacker, decryption using Brute force attack is difficult.

Consider the Example 1, where the elliptic curve group chosen is $y^2 + xy = x^3 + g^4x^2 + g^2$ over $GF(2^8)$ whose order M=240 and the nearest prime is 241. The key size in terms of the total number of bits required can be computed as follows:

1) The number of bits for expressing each initial value is 8. If the number of stages of shift register for generating k_i is 'n', the number of bits required for 'n' initial values: 8n bits.
2) The number of bits for expressing 'n' feedback coefficients: 8n bits.
3) The number of bits for expressing constants 'a' and 'b' in elliptic curve over $GF(2^8)$: 16 bits.
4) The number of bits for expressing elliptic curve base points (x_p, y_p) : 16 bits.

So, the size of the secret key is the sum of all the above (1) to (4) and is equal to (32 + 16n) bits.

In general, for the example considered the key size depends on the number of shift register stages 'n' used for generating k_i as shown below:

For n=2, key size is 32+(16)*(2) = 64 bits.

For n=4, key size is 32+(16)*(4) = 96 bits.

For n=6, key size is 32+(16)*(6) = 128 bits.

For n=8, key size is 32+(16)*(8) = 160 bits.

For n=10, key size is 32+(16)*(10) = 192bits.

So, desired key size can be obtained by proper choice of 'n' depending on the level of security required. Thus, the algorithms can be implemented with variable key size which makes it flexible. If the key is so chosen that the length of the key sequence is greater than the size of the image, then the system approaches one time pad.

5.2 Security Against Statistical Attack

It is possible to make use of apriori probability of occurrence of certain patterns in the image or encrypted image in breaking the cipher. This concept is termed as statistical attack. It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. The following aspects related to statistical attack are considered in this paper:

1) Histograms;
2) Computing and comparing the entropy of the plain and encrypted image;
3) Testing the generated sequence using various FIPS and NIST randomness tests.

Based on these aspects it is seen that the currently-designed algorithms are immune against statistical attack. The following are the details of the various aspects listed above.

5.2.1 Histograms

To prevent the leakage of information to an opponent, it is also advantageous if the encrypted image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each intensity level. In this work, the histograms are plotted for several encrypted images as well as original images that have widely different color levels and content.

The plots are shown for eight different schemes in Section 4. It can be seen that the histogram of the plain image contains large spikes. These spikes correspond to color values that appear more often in the plain image. Whereas, the histogram of the cipher image is almost flat and uniform, indicating almost equal probability of occurrence of each element. They are significantly different from that of the original image and bear no statistical resemblance to the plain image. Hence, this does not provide any clue to employ any statistical attack on the designed image encryption procedure. However, histograms of the encrypted images, using Scheme-1 to Scheme-5 in Figure 5 are not very flat. The improvement in Scheme-4, Scheme-5, and Scheme-6 is due to the use of eight key elements to encrypt one pixel element, thus employing a larger key space. Table 1 gives the difference between maximum and minimum values of histogram of the encrypted images of Scheme-1 through Scheme-8 of medical image. A smaller value of difference indicates flatter histogram. It can be observed that the variation in Scheme-4, Scheme-5, and Scheme-6 is small compared to the other additive stream cipher schemes. Also, the affine Scheme-7 and Scheme-8 are best compared to the additive stream cipher schemes as the difference is very small. This implies that all pixels in encrypted image occur with almost equal probability, which provides security against ciphertext only attack by statistical analysis. The plots indicate the significant improvement in affine schemes compared to the additive schemes and the histograms are flat.

5.2.2 Computing and Comparing the Entropy of the Plain and Encrypted Image

As mentioned earlier, Entropy is a measure of uncertainty. Higher the value of entropy of encrypted image, better the security. The entropy of the input Medical image is

1.951202. Table 2 indicates the various values of the entropies for encrypted images. It can be noted that the entropy of the encrypted images are very near to 8 indicating that in the encrypted images all the pixels occur with almost equal probability. Especially in the Scheme-7 and Scheme-8 the entropy is very close to 8, indicating the superiority of the two schemes compared with the remaining.

5.2.3 Testing the Generated Sequence Using Various FIPS and NIST Randomness Tests

To verify the randomness property of the sequence of elliptic Curve points k_iP [29], the tests given by FIPS [19] and NIST [26] are used. It is seen that all the sequences pass all NIST tests. These results imply that statistical attacks are difficult to perform.

5.3 Sensitivity Aspect

An ideal image encryption procedure should be sensitive with respect to both the secret key and plainimage. The change of a single bit in either the secret key or plainimage should produce a completely different encrypted image. To prove the robustness of the present system, sensitivity analysis is performed with respect to key.

For testing the key sensitivity of the proposed image encryption procedure, the following steps have been taken:

1) An original image in Figure 6(a) is encrypted by using the secret key that is the initial content of 4-byte LFSR as 11, 23, 7, 17 and the resultant image is referred as encrypted image A as shown in Figure 6(b).

2) Initial values (11, 23, 7, 17) is changed to (11, 23, 7, 16)[the LSB of 17 is changed] and the resultant image is referred as encrypted image B as shown in Figure 6(c).

3) Initial values (11, 23, 7, 17) is changed to (11, 23, 7, 97) [the MSB of 17 is changed] and the resultant image is referred as encrypted image C as shown in Figure 6(d).

4) Finally, the three encrypted images A, B and C are compared.

In Figure 6 the original image as well as the three encrypted images produced in the aforesaid steps is shown. It is not easy to compare the encrypted images by simply observing these images. So for comparison, correlation between the corresponding pixels of the three encrypted images is calculated. For this calculation, the same formula as given in Equations 2 to 4 is used, except that in this case x and y are the values of corresponding pixels in the two encrypted images to be compared. In Table 7, the results of the correlation coefficients between the corresponding pixels of the three encrypted images A, B and C using Scheme-1 are given. It is clear from the table that no correlation exists among three encrypted images even though these have been produced by using slightly different secret keys. Similar exercise is conducted for the other schemes also and it is verified that there is no correlation exists among encrypted images corresponding to small change in the key.

5.4 Security Against Correlation Attack

In addition to the histogram, computation has also been done for the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plainimage/encrypted image respectively. Results of horizontal, diagonal and vertical directions are obtained as shown in Table 3 through Table 5. It is clear from the tables that there is negligible correlation between the two adjacent pixels in the encrypted image, even when the two adjacent pixels in the plainimage are highly correlated.

5.5 Security Against Algebraic Attack

If the Key sequence elements are linearly related even if the period is large, by knowing a small segment of key sequence, it may be possible to construct set of linear simultaneous equations and solve for the entire key sequence. In the case of random sequence of elliptic curve points, $\{k_iP\}$, the sequence elements are non-linearly related. Then it may not be possible to construct finite number of proper equations whose solution finally leads to knowledge of complete sequence. Further, the running key makes the cipher polyalphabetic. Thus, the nonlinear key sequence makes the relation between cipher text and plain text non-linear and provides immunity against Algebraic type attack [3].

6 Comparison of Proposed Image Encryption Scheme with some of the Existing Schemes

With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. One of the solution is to encrypt image data, e.g., using DES (Data Encryption Standard). DES, however, is very complicated and involves large computations. A software DES implementation is not fast enough to process the vast amount of data generated by multimedia applications and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers. In order to tackle these problems systems based on advanced encryption standard (AES) were proposed [8]. The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption. However, a central consideration for

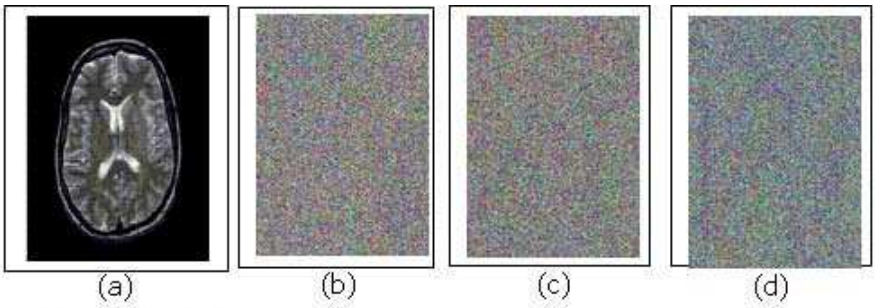

Fig. 6(a) Original Medical BMP image

Fig. 6(b) Image A: Encrypted image with the initial content of 4-byte LFSR as 11, 23, 7, 17

Fig. 6(c) Image B: Encrypted image with the initial content of 4-byte LFSR as 11, 23, 7, 16

Fig. 6(d) Image C: Encrypted image with the initial content of 4-byte LFSR as 11, 23, 7, 87

Figure 6: Key sensitivity analysis of present image encryption algorithm

Table 7: Results of the correlation coefficients between the corresponding pixels of the three encrypted images A, B And C using Scheme-1

Image 1	Image 2	Correlation Coefficient
Encrypted Image A of Figure 5(b)	Encrypted Image B of Figure 5(c)	0.0037
Encrypted Image B of Figure 5(c)	Encrypted Image C of Figure 5(d)	0.0042
Encrypted Image C of Figure 5(d)	Encrypted Image A of Figure 5(b)	0.0035

any cryptographic system is its susceptibility to possible attacks against the encryption algorithm such as statistical attack, differential attack, and various brute attacks. Zeghid et al. [35] proposes new encryption schemes as a modification of AES algorithm. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES image encryption algorithm in order to increase the image security and in turn the encryption performance. But, block cipher algorithms proves limited in an image encryption due to the processing time. Whereas the proposed stream cipher scheme finds its importance in real time tactical and strategic applications where lot of image transmissions are involved.

By studying the strengths of the confusion and diffusion properties of AES, and its security against statistical attack, AES ensures a high security for ciphered image. But the security of the scheme is based on the complexity of AES and the image proprieties. In fact, if the image contains homogeneous zones, all the blocks remain the same after ciphering. In this case encrypted image will also contain textured zones or residual information and the entropy of the image is not maximal. The author Zeghid et al. [35] claims that the modified AES which is done by adding a key stream generator, such as (A5/1, W7), could remove the textual zones of the encrypted image. Like wise, in the proposed scheme also, as the key sequence is time varying one and random, there is no residual information or textual zones observed in the encrypted images obtained using all the eight schemes.

A number of different objective measures can be utilized for quantitative comparison of the performance of the different algorithms. These criteria provide some measure of closeness between two digital images by exploiting the differences in the statistical distributions of the pixel values. In this study computations of horizontal, vertical correlation coefficients and entropy values are used for comparing the performance of proposed algorithms with those reported in [6] and [35] where LENA image is used for encryption. The Table 8 shows the comparison of results in terms of Correlation and Entropy for a LENA Image for the schemes AES, AES + A5/1, AES + W7, and the proposed scheme. From the Entropy and correlation coefficient values indicated in tables it can be seen that the proposed Scheme-1 to Scheme-8 perform better compared to the other schemes mentioned.

The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. Towards this direction, Ahmed et al. [6] presents an efficient chaos-based feedback stream cipher (ECBFSC) for image cryptosystems. This stream cipher is based on the use of a chaotic logistic map and an external secret key of 256-bit. The initial conditions for the chaotic logistic map are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. The results of several experimental, key space analysis, statistical analysis, and key sensitivity tests are presented in this literature. These results are compared with the proposed schemes.

Table 8 shows the results of correlation coefficients ob-

Table 8: Comparison of results in terms of correlation and entropy for a Lena image

Schemes	Entropy	Horizontal Correlation Coefficient	Vertical Correlation Coefficient	Diagonal Correlation Coefficient
AES	7.91	0.046	0.066	0.056
AES + W7	˜8	0.02	0.03	0.025
AES + A5/1	7.96	0.056	0.077	0.067
Chaos based	7.92	0.0308	0.0304	0.0317
Proposed Scheme-1	7.9331	-0.0037	0.0032	0.0055
Proposed Scheme-2	7.9520	0.0013	0.0044	0.0080
Proposed Scheme-3	7.9718	0.0031	0.0029	7.59e-005
Proposed Scheme-4	7.9966	7.6340e-004	0.0045	-4.24e-005
Proposed Scheme-5	7.9915	4.9460e-005	-7.20e-004	-0.0011
Proposed Scheme-6	7.9964	-7.98e-004	-0.0013	-0.0046
Proposed Scheme-7	7.9997	0.0030	0.0030	0.0027
Proposed Scheme-8	7.9996	-0.0027	-0.0028	0.0026

tained for the encrypted LENA image using the chaos system proposed by [6]. It can be seen from the tables that in the proposed schemes the results of horizontal, vertical and correlation coefficients are better compare to the chaos system proposed by [6]. That is, the correlation between the adjacent pixels of encrypted image is very less as indicated in the tables.

The flexibility in the choice of key size makes the proposed scheme suitable for both tactical and strategic applications. The histogram, entropy and correlation aspects of encrypted images show that the proposed scheme perform better compared to the three schemes given in [6] and [35] used for image encryption. In the example considered,for a given elliptic curve (a, b known) and fixed feed back connection of k_i generator, the seed value has only 32 bits which is the Key size. But, in case of A5/1 scheme and AES [35], the key size is 64 bits and 128 bits respectively. So, the proposed scheme works better with lesser key size compared to these two schemes. The schemes in general can be used for encrypting byte by byte binary data other than images also.

7 Conclusion

This paper focuses on the application of properties of Finite Fields and elliptic curves in the design of a stream cipher system. Additive and Affine encryption schemes using six schemes of key sequences obtained from random elliptic curve points are designed and investigated. The system is tested for image sample of a brain image of size 55.4KB. The encrypted images obtained for this input image and the corresponding histograms are discussed. It is seen that encrypted image does not have residual information and the corresponding histograms are almost flat offering good security for images. The Entropy and the correlation coefficient of the input and encrypted images are computed and analyzed. The encryption time required for all the eight algorithms implementing all these schemes are estimated using a state-of-the-art machine while encrypting the brain image. It can be observed that except the affine stream cipher schemes (Scheme-7 and Scheme-8), other schemes can run very fast indicating their suitability in real time applications. Security aspects of the proposed elliptic curve based image encryption algorithm are discussed. Here the security aspects like Key Space, Statistical, correlation, algebraic and Sensitivity with respect to key, are discussed with examples. It is seen that the present cryptosystem is secure against the Statistical, Brute force and Cryptanalytic attacks.

References

[1] H. Beker, and F. Piper, *Cipher Systems: The Protection of Communications*, Northwood Books, London, 1992.

[2] G. Berkhoff, S. M. Lane, *A Survey of Modern Algebra*, AKP Classics, USA, 2008.

[3] A. Biryukov, "Block ciphers and stream ciphers: The state of the art", *Technical report*, Belgium, 2006. (http://www.esat.kuleuven.ac.be)

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric encryption scheme based on 3D chaotic cat maps", *Chaos, Solutions & Fractals*, vol. 21, no. 3, pp. 749-761, 2004.

[5] J. R. Durbin, *Modern Algebra: An Introduction 5e*, John Wiley and Sons Inc., 2005.

[6] H. El-din, H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption"', *Informatica*, vol. 31, pp. 121-129, 2007.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information theory*, vol. IT-31, pp. 469-472, 1985.

[8] Federal Information Processing Standards Publications (FIPS 197), *Advanced Encryption Standard (AES)*, Nov. 2001.

[9] G. Gong, T. A. Berson, D. R. Stinson, "Elliptic curve pseudorandom sequence generators", *Proceedings of*

the 6th Annual International Workshop on Selected Areas in Cryptography, LNCS 1758, pp 34-48, 1999.

[10] T. Hansen, G. L. Mullen, "Primitive polynomials over finite fields", *Mathematics of Computation*, vol. 59, no. 200, pp. 639-643, Oct. 1992.

[11] I. A. Ismail, M. Amin, and H. Diab,"A digital image encryption algorithm based a composition of two chaotic logistic maps", *International Journal of Network Security*, vol. 11, no. 1, pp. 1-10, July 2010.

[12] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, New York, 1984.

[13] L. P. Lee, K. W. Wong, "A random number generator based elliptic curve operations", *Computers and Mathematics with Applications*, vol. 47, pp. 217-226, 2004.

[14] S. Li, G. Chen and X. Zheng, *Chaos-based Encryption for Digital Images and Videos*, Chapter 4 in Multimedia Security Handbook, Feb. 2004.

[15] S. Lin, *An Introduction to Error Correcting Codes*, Prentice Hall Englewood Cliffs, 1970.

[16] Y. Mao, G. Chen and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps", *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613-3624, 2004.

[17] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[18] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology (Crypto'85)*, LNCS 218, Springer Verlag, pp. 417-426, 1986.

[19] R. Mita, G. Paumba, S. Pennisi, M. Poli, "A novel pseudo random bit generator for cryptography applications", *9th International Conference on Electronic Circuits & Systems*, vol. 2, pp. 489-492, 2002.

[20] A. Mitra, Y. V. S. Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques", *International Journal of Computer Science*, vol. 1, no. 1, pp. 127-131, 2006.

[21] F. Morain, "Building cyclic elliptic curves modulo large primes", LNCS 547, pp. 328-336, 1990.

[22] N. K. Pareek, V. Patidar, and K. K. Sud, "A random bit generator using chaotic maps", *International Journal of Network Security*, vol. 10, no. 1, PP. 32-38, Jan. 2010.

[23] M. J. B. Robshaw, "Stream ciphers", *RSA Lab. Technical Report*, TR-701, Version 2.0, 1995.

[24] J. J. Rofman, *Advanced Modern Algebra*, PHI Publisher, 2007.

[25] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[26] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications", *NIST Special Publication*, 800-22, May 15, 2001.

[27] M. Salleh, S. Ibrahim, and I. F. Isnin, "Image encryption algorithm based on chaotic mapping", *Journal Teknologi*, vol. 39(D), pp. 1–12, 2003.

[28] S. V. Sathyanarayana, "Key sequences of elliptic curve points over finite fields, their properties and application in image encryption and decryption", *Ph.D Thesis*, Manipal University, 2010.

[29] S. V. Sathyanarayana, M. A. Kumar, K. N. Haribhat, "Design of pseudo random sequence generator based on properties of cyclic elliptic curves over finite fields", *Accepted for publication in International Journal of Information Security: Global Perspective*, Taylor & Francis, Online ISSN:1939-3547.

[30] S. V. Sathyanarayana, M. A. Kumar, K. N. Haribhat, "Some studies on elliptic curve based stream cipher systems", *National Conference at Goa College of Engineering Goa*, PONDA, Jan. 2004.

[31] S. V. Sathyanarayana, M. A. Kumar, K. N. Haribhat, "Generation of pseudorandom sequence over cyclic elliptic curve group and their properties", *International Conference on Advances in Information and Communication (ICICOT'07)*, MIT Manipal, pp. 28-30, Dec. 2007.

[32] S. V. Sathyanarayana, M. A. Kumar, K. N. Haribhat, "Generation of pseudorandom sequence over elliptic curve group and their properties", *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 10, no. 6, pp. 731-747, 2007.

[33] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition*, John Wiley and Sons, Inc., 1996.

[34] Z. J. Shi and H. Yan, "Software implementations of elliptic curve cryptography", *International Journal of Network Security*, vol. 7, no. 1, pp. 141-150, July 2008.

[35] M. Zehid, M. Machhout, L. Khrijji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption", *Proceedings of World Academy of Science, Engineering and Technology*, vol. 21, pp. 206-211, May 2007.

S. V. Sathyanarayana received the B.E. degree in Electronics & Communication from Mysore University in 1993, M.E. in Electronics from Bangalore University in 1999 and Ph.D. from Manipal University in the area of Cryptography in 2010 under the guidance of K. N. Hari Bhat and M. Aswatha Kumar. He has total teaching experience of 16 years. He is presently working as Professor in the department of Electronics & Communication, JNN College of Engg., Shimoga. He is a member of the Cryptography Research Society of India (CRSI), Kolkatta, I.S.T.E and Fellow of the I.E.T.E. He has co-authored a text book on Introduction to Computer Security and authored two study materials for distance education courses. His areas of interest are Information Theory & Coding and Cryptography.

M. Aswatha Kumar received his B.E. degree from the University of Mysore, M.E. from the Indian Institute of Science Bangalore and Ph.D. from the Indian Institute of Technology, Kharagpur, India. He served as lecturer and selection grade lecturer at the University BDT

College Engineering, Davangere, Karnataka Polytechnic Mangalore, DRR Polytechnic, Davangere, Professor & Head, Department of Computer Science & Eng, JNN College of Engineering, Shimoga, India. Currently he is Professor & Head, Department of Information Science & Eng, M.S. Ramaiah Institute of Technology, Bangalore, India. He is a member of the I.E.E.E, I.S.T.E and Fellow of the I.E.T.E. He has published papers extensively at both international conferences and journals. His research interests include digital geometry, computer vision, image processing, graphics, evolutionary computing and Knowledge Management.

K. N. Hari Bhat received the B.E degree with honours from Mysore University in 1966, M.Tech and Ph.D degrees in Electronics & Communication Engineering from Indian Institute of Technology Kanpur in 1973 and 1986 respectively. He was with the Karnataka Regional Engineering College Suratkal (now Known as National Institute of Technology) for more than 30years upto 2001. He is presently the Head of the Department of Electronics & Communication Engg , Nagarjuna College of Engineering & Technology, Bangalore. He has co-authored two books in Communication Engg. His areas of interest are Digital Communication and Cryptography.