# Image Encryption Scheme with Key Sequences based on Chaotic Functions

Shruthi K. M.
Department of E&CE
JNNCE
Shimoga India
Email: shruthikmtth@gmail.com

Sheela S.
Department of E&CE
JNNCE
Shimoga India
Email: sheela.cit@gmail.com

Dr. S. V. Sathyanarayana
Department of E&CE
JNNCE
Shimoga India
Email: svs.tce@gmail.com

***Abstract*—The current information age demands enormous opportunities, where, the sensitive data and information is being exchanged, analyzed and made use of. It has led to several concerns and challenges, mainly in the areas of information privacy, authentication and integrity. This concern, attracted cryptographers to device more effective methodologies and algorithms to ensure better protection to sensitive information. In this context, the application of chaotic based systems is considered to design a pseudorandom sequence generator, which is used as a key stream generator in the additive Stream Cipher system. Chaotic map is a mathematic function that generates highly nonlinear and random real sequence which is very sensitive to initial conditions. In this view, this work focusses on the study of Logistic map, considered from a bunch of various Chaotic functions available [1], [2]. Chaotic real sequence is binarized using a new binarization algorithm using Linear Feedback Shift Register (LFSR), which is designed in such a way that the randomness of Chaotic real sequence is not affected as far as possible. Using Logistic map, about 50 sequences are generated each of length $\geq 10^6$. To ensure the randomness of binary sequences, NIST(National Institute of Standards and Technology) test is used. It is observed that, all the sequences have strictly passed most of the NIST tests with an average passing proportion $\geq 0.87$. These sequences are used as key sequences in image encryption and decryption. It is interesting to observe that, encrypted image does not contain any residual information. This result is cross verified by plotting the Histogram, computing the Correlation coefficient and Entropy of the output images. It is observed that, Histograms are almost flat indicating the equiprobable distribution of pixels. Also, Entropy of the encrypted image is close to 8 and Correlation coefficient value is very negligible indicating that neighboring pixels are heavily uncorrelated. As the key sequence based on Chaotic functions is sensitive to initial conditions, the sequence generated will be highly nonlinear and random which encourages one to use in cryptographic applications.**

***Keywords*—Additive Stream Ciphers, Linear Feedback Shift Register, NIST, chaotic functions**

## I. Introduction

THE fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. To meet this challenge, a variety of encryption schemes have been proposed. Among them, Chaos based algorithms have shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power and computational overhead, etc [3]. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms such as DES, IDEA and RSA are not suitable for practical image encryption, especially under the scenario of on-line communications [3]. The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse data by traditional means of cryptology. In this respect, Chaos-based algorithms have shown their superior performance [4]. In many aspects Chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms. For instance, classical encryption algorithms are sensitive to keys, while chaotic maps are sensitive to initial conditions and parameters [4]. Cryptographic algorithms shuffle and diffuse data by rounds of encryption, while Chaotic maps spread the initial region over the entire phase space via iterations. The main difference between conventional encryption algorithms and chaos-based algorithms is that encryption operations are defined on finite sets, while chaos in a strict mathematical sense is defined on real numbers [3]. The Chaotic real sequences need to be converted to binary before using them in Encryption. Mahalinga V. Mandi et al. [1] have proposed a model to generate large set of chaotic binary sequences using six chaotic map equations such as Logistic map, Tent Map, Cubic Map, Quadratic Map and Bernoulli Map. It is found that these sequences have good cross correlation values and large linear complexity and hence can be used as spreading sequences in CDMA applications. Ali Kanso et al. [5] have proposed two pseudorandom binary sequence generators, based on logistic chaotic maps intended for Stream Cipher applications. The first is based on a single one-dimensional logistic map which exhibits random, noise-like properties at given certain parameter values, and the second is based on a combination of two logistic maps. The encryption step proposed in both algorithms consists of a simple bitwise XOR operation of the plaintext binary sequence with the keystream binary sequence to produce the ciphertext binary sequence. A threshold function is applied to convert the floating-point iterates into binary form. In [6], a simple threshold function is used to binarize the chaotic sequence and the performance of chaotic code generators implemented in spread spectrum communication system is analyzed and compared to those using conventional pseudo random code generators. Huang-Pei Xiao et al. [7] have proposed an image encryption scheme based on two chaotic systems. One of the chaotic systems is

978-1-4799-6629-5/14/$31.00 

used to generate a Chaotic sequence which is binarized by a threshold function. The binary sequence obtained in this approach do not pass many of the randomness tests.

In this paper, a novel approach has been proposed for the generation of key sequence using chaotic functions. Chaotic real sequence is binarized using threshold function [7]. Further, the generated binary sequence is used as initial condition of Linear Feedback Shift Register (LFSR). Output of LFSR is used as the key sequence for image encryption and the results are analyzed.

## II. Proposed Sequence Generator

### A. Chaos Basics

Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions, an effect which is popularly referred to as the butterfly effect. It is the qualitative study of unstable aperiodic behavior in deterministic nonlinear dynamical systems [8]. With this definition, several conclusions about the characteristics of chaos is done. First, that the system is dynamical, means that it changes over time. Second, that the behavior of the system is aperiodic and unstable means that it does not repeat itself. Third, because the system is nonlinear, it is sensitive to initial conditions. Fourth, because the system is deterministic, chaotic behavior is not random even though its aperiodicity and unpredictability may make it appears to be so. The natures of chaotic signals can be very helpful in enhancing the security in Cryptographic applications. The different chaotic maps available are Logistic Map, Tent Map, Sinusoidal Map, Gaussian Map, Lozi Map [2], Cubic Map, Quadratic Map and Bernoulli Map [1]. The most widely used one dimensional chaotic map is Logistic map [2] and is given in equation 1.

$$x_{n+1} = r * x_n * (1 - x_n) \tag{1}$$

where $x_n \in (0, 1)$, r is the bifurcation parameter or control parameter and $r \in (0, 4), n = 0, 1, \ldots$ The sensitivity of chaotic functions is based on bifurcation parameter and initial condition. Bifurcation is a period doubling, a change from an N-point attractor to a 2N-point attractor, which occurs when the control parameter is changed. Consider r = 0.25, 0.5 and 0.75 with initial value $x_0$ = 0.5 and for 10 iterations a plot of number of iterations versus magnitude (x) is plotted in Figure 1(a). Consider r = 1.25, 2 and 2.75 with initial value $x_0$ = 0.5 and for 25 iterations, a plot of number of iterations versus magnitude (x) is plotted in Figure 1(b). When r = 3.2 $(r > 3)$, the system is called a two-point attractor as it settles down between two points shown in Figure 1(c). When r = 3.54, the system settles down between four points and hence called a four-point attractor shown in Figure 1(d). When r = 3.99, it results in an N-point attractor and is shown in Figure 1(e).

Sensitivity of logistic map to initial conditions is shown in the Figure 2, that is, a small change in initial conditions yield dramatically different results over time.

As seen from the Figure 2, upto 33 iterations, both the initial conditions result in same values. Hence the first 100 points of the chaotic iteration curve are abnegated in order to avoid the harmful effect of transitional procedure [9].

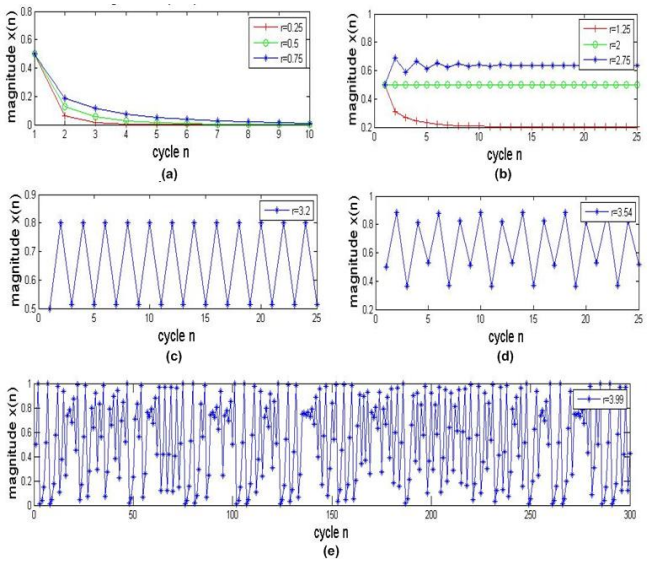


Fig. 1. Logistic Map Analysis for $x_0$ = 0.5 (a) r = 0.25, 0.5 and 0.75 (b) r = 1.25, 2 and 2.75 (c) r = 3.2 (d) r = 3.54 (e) r = 3.99

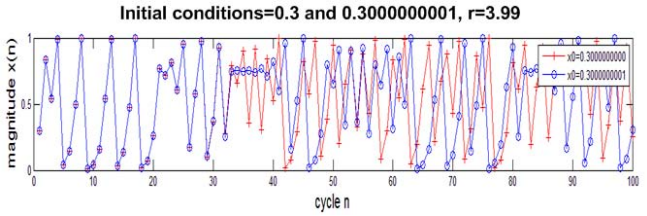


Fig. 2. Sensitivity of Logistic Map to Initial Conditions

### B. Linear Feedback Shift Registers (LFSRs)

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. 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 [10],[11] and hence more secure.

An n-stage shift register is a circuit consisting of n consecutive storage units. Shift register is converted into a code generator by including a feedback loop, which computes a new term for the left-most stage, based on the n previous terms. To obtain a new value for stage n, we compute using a function of all the present terms in the shift register and use this in stage n. If the feedback function is a linear function, then the output sequence is called a Linear Feedback Shift Register (LFSR) sequence. Otherwise, it is called a Nonlinear Feedback Shift Register (NLFSR) sequence. The general schematic of LFSR is shown in the Figure 3.

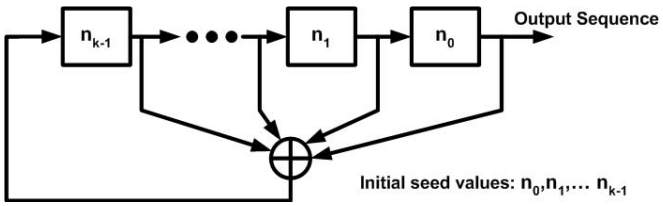


Fig. 3. General Schematic of k-stage LFSR

### C. Proposed Approach

The model to obtain Chaotic binary sequence using LFSR is shown in the Figure 4. The steps are as follows:

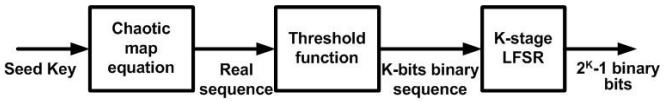


Fig. 4. Scheme of Generating Chaotic Binary Sequence using LFSR

1) Generate a chaotic real sequence using the sub-key k(r and $x_0$) as the initial conditions of the Logistic Map.
2) Transform the chaotic sequence into a binary stream by a threshold function. The threshold function T [7] is defined in the equation 2 as values of x are in between 0 and $1(0 < x < 1)$.

$$T(x) = \begin{cases} 00\cdots00 & 0 \le x < \frac{1}{2^k} \\ 00\cdots01 & \frac{1}{2^k} \le x < \frac{2}{2^k} \\ \vdots & \vdots \\ 11\cdots11 & \frac{2^k-1}{2^k} \le x < 1 \end{cases} \quad (2)$$

3) To avoid the transition effect, first 100 Chaotic real values are discarded. The next chaotic real sequence is represented in k binary bits using threshold function defined in the equation 2. These k binary bits drive LFSR to generate binary sequence of length $2^k - 1$.

## III. Encryption Algorithm Using Chaotic Key Sequence

Block Ciphers and Stream Ciphers are the two techniques of Cryptography. Information is transformed to ciphertext using a fixed key for all the blocks in case of Block Ciphers, where as in case of Stream Ciphers, for each information byte a different key is used. So, generation of random sequence is an important task in Stream Ciphers. Here a synchronous additive Stream Cipher system is designed where the key sequence is derived from logistic map. The same key sequence is used for both encryption and decryption process and is shown in the Figure 5.

Plaintext is represented as sequence of image pixels, $p_i$. The key sequence is represented as $k_i$, the ciphertext is denoted by $c_i$. The length of the message is taken as $'d'$ bytes.

**Enciphering Algorithm:**

$$c_i = p_i \oplus k_i \ \forall \ i = 0, 1, \ldots, d-1$$

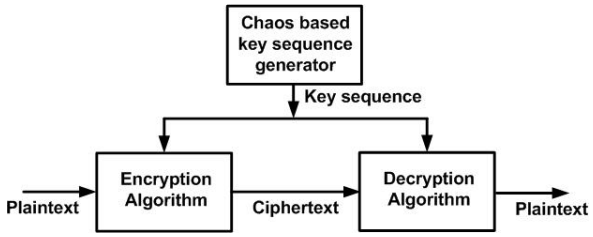


Fig. 5. Chaos based additive Stream Cipher system

**Deciphering Algorithm:**

$$p_i = c_i \oplus k_i \ \forall \ i = 0, 1, \ldots, d-1$$

**Implementation Details:**
These Algorithms are programmed using MATLAB 7.10 on windows based computer environment with core Intel i3(R) 2.2GHz processor.

### A. Performance Evaluation

The performance of the encryption algorithm discussed is measured by computing Entropy and correlation coefficient of the encrypted images and then comparing Entropy and Correlation coefficient of the input image.

**(i) Entropy**
Entropy is a measure of uncertainty. Higher the value of entropy of encrypted image, better the security. The Entropy $E_n$ of the input image and the encrypted image is calculated as:

$$E_n = \sum_{i=0}^{255} \left( p(i) * \log_2 \left( {}^1\!/_{p(i)} \right) \right) \quad (3)$$

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

**(ii) 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 two formulae given in equation 4 and equation 5 [12]:

$$Cov(x, y) = E(x - E(x))(y - E(y)) \quad (4)$$

$$r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x) D(y)}} \quad (5)$$

where x and y are the values of two adjacent pixels in the image. In numerical computations, the discrete formulas given in equations 6, 7 and 8 are used:

$$E(x) = \frac{1}{R} \sum_{i=1}^{R} x_i \quad (6)$$

$$D(x) = \frac{1}{R} \sum_{i=1}^{R} (x_i - E(x))^2 \quad (7)$$

$$cov\,(x,y) = \frac{1}{R}\sum_{i=1}^{R}\left(x_i - E\,(x)\right)\left(y_i - E\,(y)\right) \qquad (8)$$

## IV. Results and Discussion

The binary sequences generated using the proposed approach is analyzed to test the randomness properties using NIST tests [13]. It is expected to have similar level of randomness and nonlinearity of chaotic real sequence. Using Chaotic function, 50 Chaotic binary sequences are generated considering various initial conditions and bifurcation parameter. The randomness of these sequences are analyzed using NIST test suite. These sequences are used as key sequences in additive Stream Cipher system and the performance analysis is done using histogram, correlation coefficient and entropy. Compared to existing method [7], the proposed method gives better results.

### A. Statistical Analysis

Due to the difficulty of proving the unpredictability in a theoretical way, sequences generated using Chaotic systems are subjected to statistical tests. Statistical tests determine whether the sequences possess certain attributes that truly random sequences would be likely to exhibit [5]. Hence, any random number generator which is proposed for use in cryptographic applications, must be subjected to statistical tests. The Statistical analysis of the generated Chaotic binary sequence is performed using NIST (National Institute of Standards and Technology) Statistical Test Suite (sts-2.1). It is recommended that this suite should be invoked with a sequence of length of 1,000,000 bits (i.e., $n \geq 10^6$) . A file finalAnalysisReport.txt is generated when statistical testing is completed, which indicates the proportion of passing a test of the input sequence. Using Logistic Map, 50 Chaotic binary sequences are generated considering various initial conditions $x_0(0 < x < 1)$ and bifurcation parameter r $(3.57 < r < 4)$. According to this test suite, the minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.947786 for a sample size = 50 binary sequences and the minimum pass rate for the random excursion (variant) test is approximately 0.840752 for a sample size = 4 binary sequences [13]. The NIST randomness test results of the existing and the proposed approach are tabulated in the Table I.

TABLE I
Results of NIST Randomness Tests (Prp-proportion of passing a test)

| Sl.No | Tests | Existing algorithm [7] | | Proposed algorithm | |
|---|---|---|---|---|---|
| | | Prp | Status | Prp | Status |
| 1 | Frequency | 0.0600 | Fail | 1.0000 | **Pass** |
| 2 | Block Frequency | 0.2800 | Fail | 1.0000 | **Pass** |
| 3 | Cumulative Sums | 0.1000 | Fail | 1.0000 | **Pass** |
| 4 | Runs | 0.0000 | Fail | 1.0000 | **Pass** |
| 5 | Longest Run | 0.1400 | Fail | 1.0000 | **Pass** |
| 6 | Rank | 0.9800 | **Pass** | 0.0000 | Fail |
| 7 | FFT | 0.2600 | Fail | 0.0000 | Fail |
| 8 | Overlapping Template | 0.4200 | Fail | 1.0000 | **Pass** |
| 9 | Universal | 0.4600 | Fail | 1.0000 | **Pass** |
| 10 | Approximate Entropy | 0.0000 | Fail | 1.0000 | **Pass** |
| 11 | Serial | 0.0000 | Fail | 1.0000 | **Pass** |
| 12 | Linear Complexity | 1.0000 | **Pass** | 1.0000 | **Pass** |

**13. Non overlapping Template Test**: In this test multiple values will be computed depending on the number of templates i.e., one value will be computed for each template and for sequence of length 1,000,000 bits 148 values will be computed. For the existing algorithm none of the values satisfy the passing proportion. For the proposed algorithm, 144 values satisfy the passing proportion.

**14. Random Excursions Test**: This test is actually a series of eight tests: -4, -3, -2, -1 and +1, +2, +3, +4. For a given state x, a measure of how well the observed number of state visits within a cycle match the expected number of state visits within a cycle, under an assumption of randomness. For the existing algorithm, 4 states pass the test. For the proposed algorithm, all 8 states pass the test.

**15. Random Excursions Variant Test**: This test is actually a series of eighteen tests: -9, -8, . . ., -1 and +1, +2, . . ., +9. For a given state x, a measure of how well the observed number of state visits within a cycle match the expected number of state visits within a cycle, under an assumption of randomness. For both algorithms, all 18 states pass the test.

Observing the above results, we can infer that, existing algorithm passes only 4 tests whereas proposed algorithm passes 13 tests exhibiting better randomness properties compared to existing algorithm.

### B. Results of Image Encryption and Decryption

In this subsection the results of Encryption performed using chaotic binary sequences generated from Logistic map for both existing and proposed algorithms have been presented. The system is tested for a medical image (CT scanned brain image) which is a gray scale image of size 30.3 KB. The input medical image and encrypted images are shown in the Figure 6. The corresponding Histograms are shown in the Figure 7.

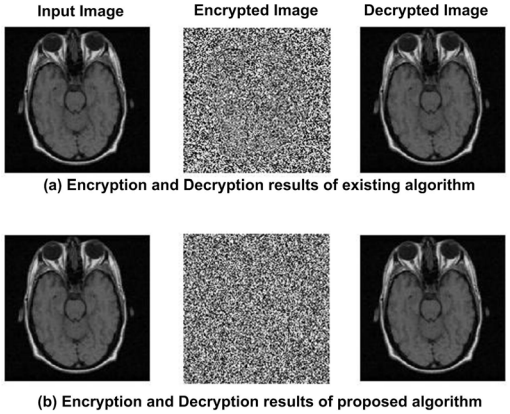


Fig. 6. Input, Encrypted and Decrypted Images of Medical Image

The Histograms are compared based on the difference between maximum and minimum values of Histogram. Smaller values of difference implies flatter histogram. To observe this minute difference among the algorithms, width of the Histogram band is measured which is the difference between

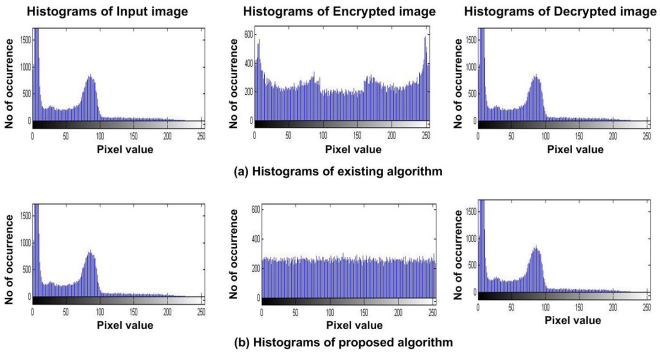


Fig. 7. Histograms of Input, Encrypted and Decrypted Images of Medical Image

the maximum value of occurrence of a pixel and the minimum value of the occurrence. The Correlation coefficients, Entropy and Histogram band are shown in the Table II. Proposed Algorithm exhibits flat Histogram which indicates that all the pixels occur with equal probability. The input entropy for the input medical image is 6.2065. It can be seen from the table that the Entropy of the encrypted image is very close to eight for the proposed algorithms. The two adjacent pixels in the input image are highly correlated as the vertical, horizontal and diagonal Correlation coefficient of the input image is 0.9671, 0.9804 and 0.9514 respectively. The vertical, horizontal and diagonal Correlation coefficients are shown in the Table II. It is clear from the values that there is negligible correlation between the two adjacent pixels in the encrypted image, which indicates that from any portion of the image, the attacker cannot reproduce the input image.

TABLE II
THE CORRELATION COEFFICIENTS, ENTROPY AND HISTOGRAM BAND OF EXISTING AND PROPOSED ALGORITHMS

| | Correlation coefficients | | | Entropy | Histogram band |
|---|---|---|---|---|---|
| | Vertical | Horizontal | Diagonal | | |
| Existing algorithm [7] | -0.0055 | -0.0036 | 0.0047 | 7.9517 | 424 |
| Proposed algorithm | -0.0020 | 0.0027 | 0.0024 | 7.9973 | 88 |

## V. CONCLUSION

The present day communication networks such as wireless networks and internet are public media, that are not suitable for raw transmission of confidential information. Sensitive information like medical and legal records, business transactions, drawings specific to military and defense applications are generally exchanged through internet. In this background, this paper focussed on the application of theory of Chaotic systems in the design of additive Stream Cipher system. Chaotic system is essentially governed by a mathematical function, which is used to generate sequence of real numbers. This is interesting to observe that these sequences are highly nonlinear, random and very sensitive to initial conditions. These characteristics of Chaotic sequences tempted the researchers towards their use in the area of key sequence generators for Stream Cipher system. In this direction, this project focussed on the design of a suitable and efficient key sequence generator based on Chaotic functions. Logistic map is the Chaotic function considered for study and implementation. Chaotic real sequences are generated using Logistic map. The proposed binarization algorithm shows good randomness properties compared to existing algorithm. The sequences have been used as a key sequence in additive Stream Cipher system to encrypt image. The encrypted images have been analyzed based on visual observation, Histogram, Correlation coefficient and Entropy. Visually no portion of encrypted image gives any information about input image. Histograms of encrypted image is flat and is justified using Histogram band. Correlation coefficient value is highly negligible and the Entropy is almost very close to 8. In summary, it was concluded that, pseudorandom key sequences generated using the proposed algorithm can be comfortably and confidently used as key sequences in additive Stream Cipher systems. The key sequences are generated and stored offline in advance. Hence this system is best suitable for real time tactical applications. The sequences can be tried in an affine Stream Cipher system, to obtain better security level. Because of the time constraint, security analysis could not be performed on the algorithms developed. This can be taken as a further work of investigation.

## REFERENCES


[1] M. V. Mandi, K. N. Hari Bhat, and R. Murali, "Generation of large set of binary sequences derived from chaotic functions with large linear complexity and good cross correlation properties," in *Proc. IEEE International Workshop on Microelectromechanical Systems (MEMS97)*.

[2] M. Bucolo, R. Caponetto, L. Fortuna, M. Frasca, and A. Rizzo, "Does chaos work better than noise?" *Circuits and Systems Magazine, IEEE*, vol. 2, no. 3, pp. 4–19, 2002.

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

[4] L. Kocarev, "Chaos-based cryptography: a brief overview," *Circuits and Systems Magazine, IEEE*, vol. 1, no. 3, pp. 6–21, 2001.

[5] A. Kanso and N. Smaoui, "Logistic chaotic maps for binary numbers generations," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2557–2568, 2009.

[6] M. Youssef, M. Zahara, A. Emam, and M. A. ElGhany, "Chaotic sequences implementations on residue number spread spectrum system," *International Journal of Communications*, vol. 2, pp. 143–154, 2008.

[7] H.-P. Xiao and G.-J. Zhang, "An image encryption scheme based on chaotic systems," in *Machine Learning and Cybernetics, 2006 International Conference on*. IEEE, 2006, pp. 2707–2711.

[8] S. H. Kellert, *In the wake of chaos: Unpredictable order in dynamical systems*. University of Chicago press, 1994.

[9] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[10] M. J. Robshaw, "Stream ciphers," *RSA Laboratories, a division of RSA Data Security, Inc*, 1995.

[11] S. V. Sathyanarayana, M. Aswatha Kumar, and K. N. Hari Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points." *IJ Network Security*, vol. 12, no. 3, pp. 137–150, 2011.

[12] H. E.-d. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "An efficient chaos-based feedback stream cipher (ecbfsc) for image encryption and decryption," *Informatica (Slovenia)*, vol. 31, no. 1, pp. 121–129, 2007.

[13] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, S. Vo *et al.*, "Statistical test suite for random and pseudorandom number generators for cryptographic applications, nist special publication," 2010.