Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HYBRID CHAOTIC KEYSTREAM GENERATION (HCKG) FOR SYMMETRIC IMAGE ENCRYPTION

[1]ALI H. KASHMAR, [2]AHMED K. HASSN, E. S. ISMAIL[3]
[1]University of Baghdad, College of Science, Baghdad, Iraq
[2]University of Baghdad, College of Science, Baghdad, Iraq
[3]School of Mathematical Sciences, Faculty of Science and Technology
Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
E-mail: [1]kashmar992000@yahoo.dk,[2]ahmedalesamy@yahoo.com

ABSTRACT

Today, data security is the main objective to protected personal data from unauthorized access users, because of the high-speed development of unsecured networks. The aim of apply symmetric-key algorithms is to produce a good encrypt data in order to safety transmitted information through unsecure networks; such goal is achieve by design efficient keystream generator mechanism. However, there are many properties should be taken in consideration to design a good ciphers including; implement strong and high-speed keystream generation, utilize a complex invertible round functions, as well as time execution and security level. This paper suggested a new technique for design efficient keystream generator mechanism called Hybrid Chaotic Keystream Generator (HCKG) that is suitable for symmetric image encryption. HCKG generator passes through four stages; firstly, choose the chaotic maps, including, Chebyshev, Tent, Gaussian, Henon, and Duffing maps. The secondly stage, exponential function [exp(x)] and the next stage is machine words multiplexer to find the floating-point representation group of random numbers. The final stage, random matrix table as a dynamic substitution box (S-box) depend on random key, shifting, logistic maps for (1D, 2D, 3D), and particle swarm algorithm. Visual Studio was employed as a programming language to implement the algorithms of proposal system. The output of HCKG is testing in several measurements represent including complexity, time execution and avalanche criterion balance; the numerical results show that the keystream generation successfully passed through NIST (statistical package tests for randomness). Finally, image encryption for the corresponding algorithm was done; preliminary results show that HCKG algorithm has good cryptographic strength and resistant against security attacks.

Keywords: *Cryptography, Symmetric key, Chaotic Maps, Image encryption, NIST*

1. INTRODUCTION

The detailed investigation and analysis of nonlinear dynamical system based on the developing of chaotic functions has been much interesting in a period of past ten years. Chaotic functions become larger for different applications such as information technology, digital communications and cryptography either theory or practice. The fundamental truth of sensitively dependence on its initial condition is the most significant feature of the chaotic system; Prof Lorenz is the first researcher who illustrated this properly. In the course of a search, he discovered that a bit changed the initial conditions in the system of differential equations could completely change the resulting after short period [1], such particular feature of chaos has been supported by many researchers [2][3].

Uncorrelated number, Random-looking sequences and reproducible singles can be generating based on the principle of the sensitive dependence of chaotic systems on their initial conditions. Due to the deterministically and disguising modulation property, chaotic dynamical system can be easily made as noise based on its random-like behavior [4]. Many advantages have been provide by the application of chaotic sequence over conventional binary sequences, particularly Pseudorandom Number Generators (PRNGs) sequences that frequently employed in cryptography and digital communications [5]. The consideration of conventional systems is not a good choice of transmitting message with efficient way,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

thus employing chaotic maps become necessary in the design of a secure cryptosystem. Diffusion and confusion, the two basic structure of symmetric key encryption can be modeled well by chaos theory [6], moreover the coupled between chaos theory and DNA, offered efficient method to encrypt information [7].

The focus of the paper is heavy built upon the theory of chaos. The application of the theory of chaos to cryptography is the main objective of this research.

The eligible chaotic PRNG was create, based on the equations derived from nonlinear dynamical system capable of exhibiting chaos,

$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

For each use, a different initial condition was assigning, stars the chaotic map with the initial condition of the intended receiver and repeatedly generated points of the orbit. Sensitively depending on its initial values x_0, for these values of r, the orbit will be great numbers which are noise-like, random-like and reproducible. Therefore, cipher system based on chaotic PRNG resistance against security attack [8].

This paper outlines the work of the author's investigation into the generation of new keystream dependent on hybrid chaotic maps. Many crypto systems dependent chaotic maps have been proposed in the past [9], [10], [11], [12], [13]. However, the effecting of these researches made rather marginal on modern cryptography for many reasons; chaos-based cryptographic algorithms in general employ a dynamical system defined on a set of real numbers so that it is hard for application, implement slow and weak keystream generation and do not provide security.

A new method to generate keystream as a function of the secret key based on Hybrid Chaotic Keystream Generation (HCKG) for symmetrical algorithms will be presented. In the next section, the chaotic map in cryptography was briefly introduced. A central part of the paper describes the construction of new (HCKG). In the following two sections, the paper gives the significant properties of propose algorithm as well as results and discussions. Finally, the paper contributes some conclusions.

2. RELATED WORKS

Shannon in his classic 1949 first mathematical paper on cryptography proposed chaotic maps as models - mechanisms for symmetric key encryption, before the development of Chaos Theory [14]. Hopf based this remarkable intuition on the use of the Baker's map in 1934 as a simple deterministic mixing model with statistical regularity [15].

Over the past twenty years, nonlinear chaotic systems have been used in the design of digital data encryption and transmission systems. The similarities between the chaotic maps and the cryptographic systems are the main motivation for the design of chaos based cryptographic algorithms. Hundreds cryptosystems designed based on chaos and nonlinear dynamic systems including, PRNGs, block and stream ciphers, hash functions, public-key ciphers, image encryptions, steganography and watermarking [16]. They emerged as a new promising candidate for cryptography because many chaos fundamental characteristics such as a broadband spectrum, periodicity and high sensitivity to initial conditions are directly connection as well as two basic properties of good ciphers, confusion and diffusion [17].

Generally, the low costs and speed make chaotic system more efficient than traditional methods for image encryption [18]. In this section, the briefly consideration of some significant improvements on image encryption methods using chaotic system will be provided. First, Matthew [19] introduced a new encryption algorithm based on a logistic map, then, Fridrich [20] followed him, proposed a new architecture for image encryption with two stages permutation and diffusion utilized 1D and 2D chaotic maps. Additionally, Guan et al.[21] has been used both of permutation /diffusion for the image encrypting applied 3D Arnolad's catmap and Chen chaos system. After that, Pareeka et al.[22] suggested 8 various kinds of operations utilized with 80-bit key to accomplish the encryption process based on two logistic map. In [23] a new method was introduced depending on the use multi-chaotic functions with Rossler attractor to generate the key for permutation all image pixels. [24] introduces two general tent chaotic maps to increase the degrees of freedom and produce a versatile response that can fit many cipher applications. [25] propose a novel image encryption algorithm based on two pseudorandom bit generators; Chebyshev map for permutation and rotation equation for substitution operations. [26] an image encryption algorithm based on Ikeda and Henon chaotic maps is presented. [27] propose a novel image encryption scheme based on the chaotic tent map, to generate

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

key stream by a 1D chaotic tent map, that is more suitable for image encryption. Finally, [28] discusses and presents an image encryption and decryption approach using Gauss iterated map.

3. THE PROPOSED SYSTEM CONSTRUCTION

The structure design of propose algorithm, as illustrated in Figure 1 below, show that, it was modern technique based on different chaotic maps.

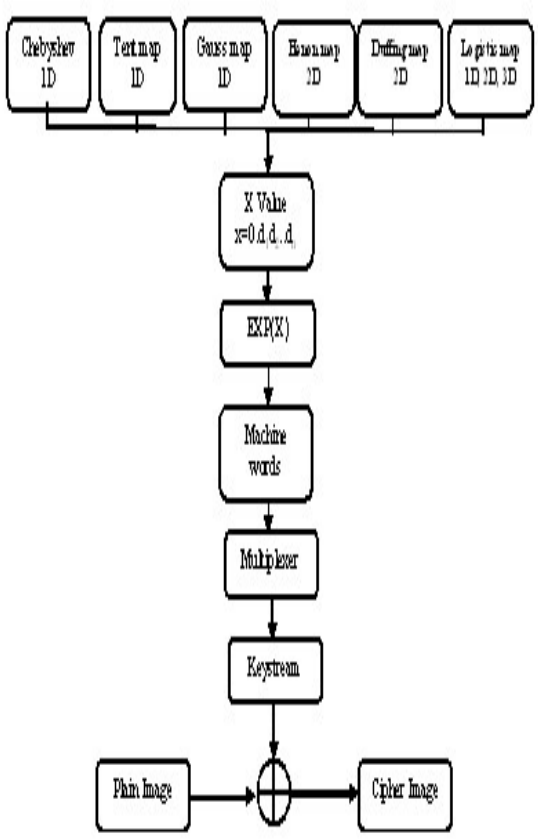

Figure 1: shows the structure of the design of propose algorithm

As demonstrated in Figure 1, the HCKG generator passes through four stages; firstly, choose the chaotic maps, including, Chebyshev, Tent, Gaussian, Henon, and Duffing maps. The secondly stage, exponential function [exp(x)] and the next stage is machine words multiplexer to find the floating-point representation group of random numbers. The final stage, random matrix table as a dynamic substitution box (S-box) depend on random key, shifting, logistic maps for (1D, 2D, 3D), and particle swarm algorithm, as shown in the following steps:

Step 1: Choose the chaotic maps.

-Chebyshev:

$$f(x_{n+1}) = cos(karccos(x_n)).$$

Where, $-1 \le x_n \le 1, n = 1, 2, 3,$

- One Dimensional Logistic map:

$$x_{n+1} = \lambda x_n(1 - x_n).$$

Where $\lambda = 4$

- One Dimensional Tent map:

$$(\mu = 0.62)$$

$$x_{n+1} = \begin{cases} \frac{x_n}{\mu} & 0 \le x_n \le \mu \\ \frac{1-x_n}{\mu} & \mu \le x_n \le 1 \end{cases}$$

Where, $\mu \in (0.1),\ \mu \neq 0 \cdot 5$

- One Dimensional Gaussian map:

$$x_{n+1} = e^{-\alpha x_n^2} + \beta.$$

Where, $\alpha = 6 \cdot 2,\ \beta = -0 \cdot 5$

- Two Dimensional Henon map:

$$x_{n+1} = 1 - ax_n^{\ 2} + y_n$$
$$y_{n+1} = bx_n$$

Where, $a = 0 \cdot 80,\ b = 0 \cdot 05$

- Two Dimensional Duffing map:

$$x_{n+1} = y_n$$
$$y_{n+1} = -bx_n + ay_n - y_n^{\ 3}.$$

Where, $a = 2 \cdot 75,\ b = 0 \cdot 2$

- Two Dimensional Logistic map:

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \delta_1 y_n^{\ 2}$$
$$y_{n+1} = \mu_2 y_n(1 - y_n) + \delta_2(x_n^{\ 2} + x_n y_n)$$

Where:

$2 \cdot 75 < \mu_1 < 3 \cdot 4$,
$2 \cdot 7 < \mu_2 < 3 \cdot 45$,
$0 \cdot 13 < \delta_1 < 0 \cdot 21$ and
$0 \cdot 13 < \delta_2 < 0 \cdot 15$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Three Dimensional Logistic map:

$$x_{n+1} = \lambda x_n(1-x_n) + \beta y_n{}^2 x_n + \alpha z_n{}^3$$
$$y_{n+1} = \lambda y_n(1-y_n) + \beta z_n{}^2 y_n + \alpha x_n{}^3$$
$$z_{n+1} = \lambda z_n(1-z_n) + \beta x_n{}^2 z_n + \alpha y_n{}^3$$

Where:

$3 \cdot 53 < \lambda < 3 \cdot 81$,
$0 < \beta < 0 \cdot 022$, and
$0 < \alpha < 0 \cdot 015$

Step 2: Enter the initial parameters values.

Step 3: Apply the selected chaotic map to generate a sequence of new values of x, which are real numbers between 0 and 1.

Step 4: Find the Exponential to generate the extended values Exp(x).

Step 5: Find the Floating-Point Representation group of random numbers as in Algorithm1:

Goal	*Key generation*
Input	*FloData[] floating* *no : number generation*
Output	*Xbit Machine Code Representation*

Step1	Init matrix
	For all (i=0, j=1; k<=9, j <=6; i++,j++)
	matrix[i,j]=k;
	k +=1
	End For

Step2	xColumn = 1
	BxRows = false
	xRows = 1
	Forall(xi=0;k<=9; xi++)
	Xvalue= FloData [xi]
	For each char c in Xvalue
	Select(c)
	case 'A': case 'B': case 'C': case 'D': case 'E': case 'F':
	for (j=1;k<=6;j++)
	if (c = matrix[0,j]) xColumn = j
	end for
	default:
	xRows = acii(c)
	BxRows = true;
	End case
	if (BxRows)
	BxRows = false
	XLocat++
	xn1= matrix[xRows + 1,xColumn],
	matrix[xRows + 1,xColumn]= k;
	xbit += DToB(xn1)
	for(shi=1;shi<= 5;shi++)
	temp = matrix [shi,xColumn]
	matrix[shi,xColumn] = matrix[xvalue-shi+ 1,xColumn]
	matrix[xvalue- shi + 1,xColumn]= temp;

Figure 2: Shows Floating-Point Representation groups of random numbers (Algorithm 1)

Step 6: Find the Random Keystream based on the random Matrix Table as in Algorithm 2:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

goal	Generation the Random Key based on the random Matrix
Input	x1: Machine Code Representation
Output	deToWord

Step1	For all (i=0, j=1;i<=9, j <= 6; i++,j++)
	matrix[i,j]=k;
	k +=1
	End For

Step2	value = Math.Exp(x1);
	delimiters = new char[] { '.' };
	parts = value.Split(delimiters, StringSplitOptions.RemoveEmptyEntries);
	s = OctToBin(DecimalToOct(parts[0])).Remove(1)
	n = (OctToBin(DecimalToOct(parts[0]))).Length - 1
	BiEx = OctToBin(DecimalToOct(parts[0])).Substring(1)+
	OctToBin(DecimalToOct(parts[1])
	c = n + 1023;
	s1 = OctToBin (DecimalToOct(c)).Remove(1)
	if(s1=="0") then
	BiEx1= OctToBin(DecimalToOct(c)).Substring(1)
	else
	BiEx1= OctToBin(DecimalToOct(c)
	Endif
	SingBit = s+ " " + BiEx1 + "" + BiEx
	if (SingBit.Length mod 4 <> 0) then
	xbit = null
	for (cc = 1; cc <= (SingBit.Length mod 4); cc++)
	xbit += "0";
	SingBit += xbit;
	endif
	newsbit = null, hexq = null, str11 = null
	for (i = 0;i <= SingBit.Length - 1; i++)
	if ((i + 1) % 4 == 0) then
	newsbit += SingBit[i] + " ";
	hexq += SingBit[i];
	deToWord += DtoHex(hexq)

Figure 3: Shows Generated Random Keystream based on the Random Matrix (Algorithm 2)

Step 7: Utilize the key for the encryption and decryption processes as in Algorithm3:

goal	Encryption and Decryption process
Input	Machine Code Random Numbers
Output	Encrypted Image

```
Offset ← 1
Countk ← 0
For all X , Y Do {where Offset to Wid – Offset , Offset To Hgt- Offset }
    For all I Do { Where Offset To Offset -1}
        For all J Do { Where Offset To Offset -1}
            ReGrBl ←Convert To Bin(GetPixel(j + fi, i + fj) ))
            xbin ←""
            For all K Do { Where 1 To 24}
                If Countk = Length Bits Key THEN
                   Countk ← 0
                End If
                Countk+ ← + 1
                xbin += Key[Countk]
            End For
            xReGrBl←ReGrBl Xor Bin2Dec(xbin)
            Put ReGrBl (x,y)
        End For
    End For
Exit For
```

Figure 4: Shows Utilized the key for encryption and decryption processes (Algorithm 3)

4. THE TEST VECTORS FOR EXECUTING PROPOSE SYSTEM

This section is dedicating for the design and implementation of the proposed digital image encryption system. Generally, the proposed system encrypted a colure squared digital image using the advantage of chaotic maps properties to make the encryption more secure and robust against security attacks. In the following subsections, test vectors show the results of implementing propose algorithm for the key generation steps and encryption/decryption processes.

4.1 Key Generation Steps

As shown in Figure 3.1, the key generation is presenting by the following steps:

1. Number of chaotic generators have been applied by selected one of the following maps; Chebyshev (1D), logistic map (1D, 2D, 3D) Tent map (1D), Gauss map, Henon map (2D) and Duffing map (2D), as shown in Figure 5.

Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

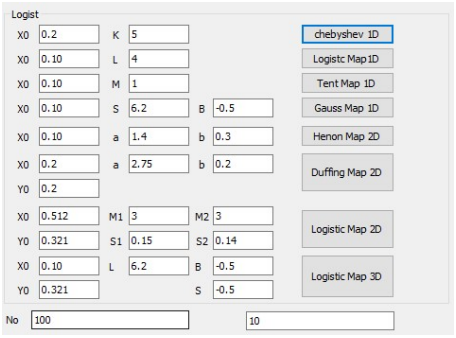

Figure 5: Shows the selection chaotic maps step

2. The output of each selected maps is passing through the exponential function [exp(x)] to get wide range of input as shown in Figure 6.
3. Then the result of step 2 is mapping into words to fit the required domain of the used multiplexed (as illustrated in algorithm 1).

No	X	Exp(x)	Machine Words
0	0.378286738313747	1.4597814581445	401485D0635B18
1	0.604907566120297	1.83108294696228	40152E58A1887490
2	0.942699401149351	2.56690117050383	4018CE3CC928003C
3	0.446447899221967	1.56275126487814	4014CCBA4BB22C18
4	0.71332552526167	2.04076660751219	401BB52BEA7B73
5	0.999042637777578	2.71568069343945	4019045CF566EB24
6	0.143701165915936	1.15453904135163	4015C1C48EEC7F
7	0.332850639597567	1.39493893426892	40148FAD8DF43B30
8	0.5372317106248	1.71126302780316	401502C1880BAE70
9	0.855583954498669	2.35274787721323	4018805434C441AC

Figure 6: Shows the Exp(x) and machine words steps

4. The next stage is passing the dictionary words into the multiplexer to produce the secret keystream. The multiplexer stage works to find the random keystream based on the random Matrix Table(10×6), as shown in Figure 7 , generation such keystream represented as a main goal of the propose algorithm such that the input machine words to get the random keystream (as demonstrated in algorithm 2).

	A	B	C	D	E	F
0	1093	1073	1047	1126	1027	844
1	1096	1021	1138	1130	1115	1069
2	1144	827	1108	887	1132	1064
3	1006	993	1140	1111	1031	667
4	1089	1019	1135	1131	1113	1067
5	1145	879	1074	1128	1143	1070
6	1081	952	1041	944	1112	1141
7	1084	942	1050	1133	905	1142
8	1085	826	1063	1129	1028	866
9	1094	1020	1139	1134	1117	1068

Figure 7: Shows the Random Matrix Table

4.2 Encryption Process

In previous subsection, we show how we generating the output pseudo random key, this keystream is unique for any size image. Suppose we have two stations, the sender is in station 1, and wants to send an image to the receiver in station 2, so he has to encrypt the plain image by using the represented keystream, that used to encrypt the plain image and decrypt the cipher image. The output of stream generator is xor'ed sequentially item to item with plain image to produce the cipher image (as explained in algorithm 3). The plaint image, as shown in Figure 8, which wants to be encrypted, is read from a text file, suppose we have the following image.

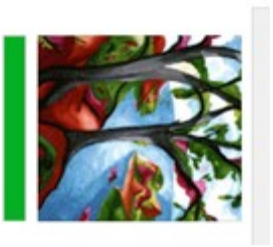

Figure 8: Shows the plain image

The cipher image after applied encryption process shown in Figure 9.

Figure 9: Shows the cipher image after encryption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.3 Decryption Process

For decryption process, as shown in Figure 10, the receiver employs the output of stream generator is xor'ed sequentially item to item with cipher image to produce the plain image.

Figure 10: Shows the plain image after decryption

4. SIGNIFICANT PROPERTIES OF CHAOTIC MAPS

Hence, the following discussions address some of the advantages of using chaotic maps in the design of the proposed system in this paper.

1. As chaotic functions, Logistic, Tent, Chebyshev, Henon, Gaussian and Duffing chaotic maps describe extremely good properties for encryption such as confusion and diffusion, that is why these functions are widely used to design various cryptographic schemes.
2. To design efficient and secure cryptosystem the encryption process should be achieve the confidentiality property. However, the schemes of traditional public key cryptography are not desirable to achieve it since the management of encryption key in these schemes produces heavy computational burden. Inspired by the excellent semi-group property, the extended Chebyshev chaotic map over the finite field has been used to develop our design since the discrete logarithm problem and Diffie-Hellman problem are assumed intractable within polynomial time [29].
3. In spite of the fact that Tent chaotic map form is simple linear equation, for certain parameter values, this system can display highly complex behavior and even chaotic phenomena.
4. Although the output of the conventional Tent chaotic map is a special case and shows different responses, it has only one control parameter that limits its behaviour and applications. Many Tent maps have been introduces to show the characteristics of each generalization such as fixed points, bifurcation diagrams, and Lyapunov exponents, which can be applied on simple image encryptions. Moreover, statistical and sensitivity analysis are presented to demonstrate the benefits of the generalized maps [30].
5. Subsequently Gaussian chaotic map employs more control parameters that improve the data security and takes lesser time for the encryption and decryption, many image encryption techniques using Gaussian chaotic map as iteration function [31].
6. Since the non-integer dimension of the attractor and associated with chaotic systems, the Hénon attractor is a strange attractor, which can be used to present an image encryption algorithm based on Hénon chaotic map [32] [33].
7. Finally, since the implementation of Duffing chaotic map is easy, suitable to acquire shuffled pixels and reflectivity in nature, it used in image block shuffling [34].

Given the previous advantages, the Chaotic Maps are using to construct mutual authentication with strong anonymity in this paper.

6. POSITIVE PROPERTIES OF PROPOSED ALGORITHM

The positive properties of the newly devised cipher as well as some of the major advantages of the proposed cipher along with a limited degree of analysis are presented in this section.

1. The utilization of random matrix table (10×6) dependent on secret key ensured great difficulties relative to attackers. Because the random matrix table was unrecognizable for the attacker, the number of probabilities faces the attacker would increase.
2. A strong diffusion can be produce from the selection of chaotic maps because there is a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

dependency between the output value and the input value of the random matrix table.

3. Unique random matrix table (weak collision resistant): no two different keys have the same random matrix table elements. In the mathematical steps, the functions make a unique value for each input value. This means that the new random matrix table resistant against differential cryptanalysis, which require that the random matrix table be known.
4. Efficiency: calculating of chaotic map value, x-value, exp(x), random matrix table and encryption process are easy to used and simple implementation according to comparing results of different algorithms.
5. Strict Avalanche Criterion (SAC): when change one value of input, the random matrix table value should be change more than half values [14]. In mathematical steps of random matrix table, the previous byte of new block will be changing all the next bytes.
6. Pseudo randomness: in the proposed random matrix table, the keys is difficult to cryptanalysis attacks (randomness) according to:
   a) Key values generated from strong PRNG and used only once (as one time pad).
   b) random matrix table has the same frequency for each key.
7. As a final point, the size of the key block has a great effect on the algorithm, the key size should be minimal size with maximum period, the block size of the propose algorithm is 128-bits.

7. RESULTS AND DISCUSSIONS

There are four main aspects of results to introduce the efficiency and robust of the propose design. These aspects are fast, complexity, secure and random.

1. Fast: the execution time of proposed algorithm is a criterion to check the design efficiency. The execution time computed by calculating the arrange time of multi execution time for the similar algorithms. The execution time based on the complexity of algorithm and size of dataset. Table 1 shows the compression between the execution time for a propose design and some identical algorithm. Comparing the propose algorithm based on fastens aspect shows without any doubt that, the execution time results for the propose design is faster than identical algorithms.

Table 1: compression between HCKG and some identical algorithms

Type of Algorithms	Key Size (Bytes)	Number of Rounds	Encryption Execution Time M/s	Decryption Execution Time M/s	Standard Deviation (S.D)
AES	128	10	3.8	5.7	32.77
3DES	64	48	20.3	20.75	10.75
DES	56	16	10.13	10.31	0.64
HCKG	128	10	8.3	8.9	1.30

2. Less Complexity: the less complexity of the propose algorithm come from:
   a) Generated x-value, exp(x) and machine words based on secure value.
   b) Substitution steps of the propose algorithm are based on chaotic maps.
3. Secure and random: the security result is one of the important matric that should be providing in the design of any cipher. There are many parameters used to demonstrate the security of the propose system:
   a) Construction random matrix table based on secure key. The random matrix table is comparing with security parameters such as balanced output, SAC and hamming distance, the results show that any change in the input will change the output and the ciphertext has fiat frequency distribution as shown in Figure 11 below.

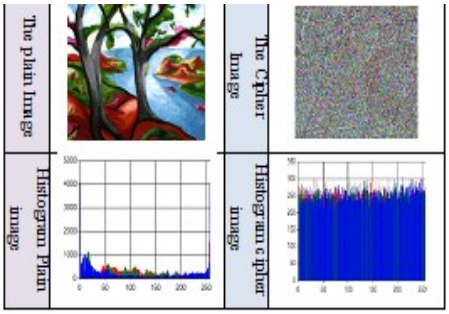

Figure 11: Shows the Histogram for the Plain Image and Cipher Image.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

b) Generated secure, random and robust machine words and multiplexer for producing keystream based on strong and efficient chaotic maps.

c) Furthermore, the generated keystreams successfully pass all NIST statistical tests for randomness, which are usually apply to measure the efficiency of generated keystreams for block ciphers and stream ciphers as shown in Table 2.

Table 2: The Results of NIST Statistical Suite Tests for HCKG

Statistical Tests	*P*-Values	Result
Frequency	0.511369	SUCCESS
Block Frequency (128)	0.515017	SUCCESS
Runs	0.544917	SUCCESS
Long Runs of Ones (10000)	1.000000	SUCCESS
Rank	0.000000	SUCCESS
Spectral DFT	0.381350	SUCCESS
Non-Overlapping Templates (9)	1.000000	SUCCESS
Overlapping Templates (9)	1.000000	SUCCESS
Universal (7)	0.600640	SUCCESS
Linear Complexity (500)	1.000000	SUCCESS
Serial1 (16)	0.498961	SUCCESS
Serial2 (16)	0.498531	SUCCESS
Approximate Entropy (10)	1.000000	SUCCESS
Cumulative – sums Fwd	0.528055	SUCCESS
Cumulative – sums Rev	0.536731	SUCCESS
Random Excursions	0.941084	SUCCESS
Random Excursions Variant	0.983947	SUCCESS

As a results, the propose system was fast, random and resistant against some security attacks such as frequency analysis, known plaintext attack, linear, differential and statistical attacks.

8. CONCLUSION

In this paper, a new approach has been suggested for design efficient keystream mechanism called Hybrid Chaotic Keystream Generator (HCKG), which was suitable for encrypted symmetric images. HCKG mechanism has been applied many kinds of chaotic functions as well as dynamic S- box, which based on the input pseudorandom key, shift operation, triple logistic maps (1D, 2D, 3D), and particle swarm algorithm.

Several measurements applied for testing the output of HCKG, including time execution, avalanche criterion balance and complexity; the results show that, the generated keystream has been successfully passed through NIST. Finally, the application of image encryption for the corresponding algorithm has been done, the result show that HCKG mechanism was absolute efficient with good cryptographic properties as well as resistant against security analysis attacks.

REFERENCES:

[1] Lorenz, Edward N. "Deterministic Nonperiodic Flow",. *Journal of the Atmospheric Sciences.* Vol. 20, No. 2, 1963.pp. 130–141.

[2] Lighthill, J., "The recently recognized failure of predictability in Newtonian dynamics", 1986. Proc. Roy. Soc. London A407, 35-50.

[3] Devaney, R., "A First Course in Chaotic Dynamical Systems", 1992. Perseus Books.

[4] Vinod Patidar and Sud, K. K.," A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", *Informatica Journal*, Vol. 33, 2009 pp:441–452.

[5] Piyush Kumar Shukla , Ankur Khare , Murtaza Abbas Rizvi , Shalini Stalin and Sanjay Kumar, "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing", *Journal Entropy*, Vol. 17, 2015, , pp:1387-1410.

[6] Wang, Xingyuan and Zhao, Jianfeng. "An improved key agreement protocol based on chaos". *Commun. Nonlinear Sci. Numer. Simul.* Vol. 15, No. 12. 2012: pp:4052–4057.

[7] Babaei, Majid. "A novel text and image encryption method based on chaos theory and DNA computing". *Natural Computing. an International Journal*. Vol.12, No. 1. 2013. pp.101–107.

[8] George Makris , G. and Ioannis Antoniou, L." Cryptography with Chaos", *Proceedings, 5th Chaotic Modeling and Simulation International Conference,* 12 – 15 June 2012, Athens Greece, pp: 309-318.

[9] Jakimoski, G. and Kocarev, L. 2001." Chaos and cryptography: block encryption ciphers based on chaotic maps, Circuits and Systems I: Fundamental Theory and Applications", *IEEE Transactions* on Vol. 48 (2), No. 309, 2001, pp. 163–169.

[10] Alvarez, G., Li, S. "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems". *International Journal of Bifurcation and Chaos, World Scientific*, Vol. 16, 2006. pp 2129-2151.

[11] Bogdan, C., Chargé, P., and Fournier-Purnaret, D. "Behavior of Chaotic Sequences Under a Finite Representation and its

Cryptographic Applications", *IEEE Workshop on Nonlinear Maps and Applications (NOMA),* Toulouse, 2007.

[12] Amigó, J.M. "Chaos-Based Cryptography. In: Intelligent Computing Based on Chaos", *Springer,* ISBN 978-3-540-95971-7, 2009. pp. 291-313, Berlin.

[13] Alvarez, G., Amigó, J.M., Arroyo, D., Li, S. "Lessons Learnt from Cryptoanalysis of Chaos-based Ciphers, in Chaos-Based Cryptography. Theory, Algorithms and Applications". *Studies in Computational Intelligence*, Vol. 354, ISBN 978-3-642-20542- 2, 2011, Berlin, pp. 257-295.

[14] Shannon, C., "Communication Theory of Secrecy Systems". *Bell System Technical Journal*, Vol. 28, Issue 4, 1949, pp 656–715.

[15] Hopf E. "On Causality, Statistics and Probability", *J. Math. and Phys*. Vol. 13, No.51, 1934, pp.102-107

[16] Akhavan, A.; Samsudin, A. and Akhshani, A. "A symmetric image encryption scheme based on combination of nonlinear chaotic maps". *Journal of the Franklin Institute.* Vol. 348, No. 8, 2011. pp: 1797–1813.

[17] Behnia, S.; Akhshani. A.; Mahmodi, H. and Akhavan, A... "A novel algorithm for image encryption based on mixture of chaotic maps". *Chaos, Solitons & Fractals*. Vol. 35, No. 2, 2008. pp:408–419.

[18] Wang, X., L. Teng, and X. Qin,." A novel colour image encryption algorithm based on chaos". *Signal Processing*, Vol.92 No.4, 2012. pp. 1101-1108.

[19] Matthews, R. "On the derivation of a "chaotic" *encryption algorithm. Cryptologia*, Vol. 13, No.1, 1989, pp. 29-42.

[20] Fridrich, J.."Symmetric ciphers based on two-dimensional chaotic maps". *International Journal of Bifurcation and chaos*, Vol. 8, No.06, 1998, pp. 1259-1284.

[21] Guan, Z.-H., F. Huang, and W. Guan,. "Chaos-based image encryption algorithm". *Physics Letters A,* Vol. 346, No.1, 2005. pp. 153-157.

[22] Pareek, N.K., Patidar, V. and Sud, K.K. "Image encryption using chaotic logistic map". *Image and vision computing*, Vol. 24, No.9, 2006. pp. 926-934.

[23] Alsafasfeh, Q.H. and A.A. Arfoa,. "Image encryption based on the general approach for multiple chaotic systems". *J. Signal and Information Processing*, Vol. 2, No.3, 2011, pp. 238-244.

[24] Salwa K. Abd-El-Hafiz, Ahmed G. Radwan∗ and Sherif H. AbdEl-Haleem, "Encryption Applications of a Generalized Chaotic Map", *Appl. Math. Inf. Sci*.Vol. 9, No. 6,2015, pp.3215-3233.

[25] Borislav Stoyanov and Krasimir Kordov. "Image Encryption Using Chebyshev Map and Rotation Equation", *Journal Entropy* Vol. 17, 2015, pp.2117-2139.

[26] Şekertekin, Y. and Atan, Ö. , "An image encryption algorithm using Ikeda and Henon chaotic maps" , *24th Telecommunications Forum (TELFOR).* 2016, Belgrade, Serbia.

[27] Chunhu Li, Guangchun Luo, Ke Qin and Chunbao Li., "An image encryption scheme based on chaotic tent map" *Nonlinear Dynamics Journal*, Vol. 87, No. 1,2016, pp.127-133.

[28] Sharma, M. C. and Sharma, P.,"Image Encryption based on Random Scrambling and Chaotic Gauss Iterative Map" *International Journal of Computer Applications,* Vol. 157 , No 3,2017, pp. 18-23.

[29] Tan, Z.. "A chaotic maps-based authenticated key agreement protocol with strong anonymity," *Nonlinear Dynamics*, vol. 72, No. 1-2,2013, pp. 311–320.

[30] Radwan, A. G, and Abd-El-Hafiz, S. K, . "Image encryption using generalized tent map ". IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS). 2013. Abu Dhabi, United Arab Emirates.

[31] Robert C. Hilborn,." Chaos and nonlinear dynamics: an introduction for scientists and engineers", 2nd Ed., Oxford, Univ. Press, New York, 2004.

[32] Sahay, A. and Pradhan, C "Multidimensional Comparative Analysis of Image Encryption using Gauss Iterated and Logistic Maps*", IEEE International Conference on Communication and Signal Processing (ICCSP*), 6-8 Apr 2017, Melmaruvathur, India.

[33] Hilborn, R.C.." Chaos and Nonlinear Dynamics: An introduction for Scientists and Engineers". UK. Oxford University Press.2000.

[34] Srinivasu, P.N. and S. Rao, A." Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel". *International Journal of Computer Applications,* Vol. 120, No.4, 2015.