COMPREHENSIVE PERFORMANCE ANALYSIS OF CHAOTIC COLOUR IMAGE ENCRYPTION ALGORITHMS BASED ON ITS CRYPTOGRAPHIC REQUIREMENTS

K S Tamilkodi[1] and Dr. (Mrs) N Rama[2]

[1]Assistant Prof in Computer Science, Presidency College, Chennai
tamil_vizhi@hotmail.com
[2]Associate Prof in Computer Science, Presidency College, Chennai
n_ramabalu@yahoo.com

"The state of being free from danger or threat." - *Security*

ABSTRACT

As we live and revel in a digital age, the day to day transmission of multimedia data over the internet is beyond our imaginations. Consequently, the increased risk of losing or altering the data during transit is more. Protection of this multimedia data (audio/speech, image, and video) becomes one of the major security concerns, because millions of Internet users worldwide, are infringing digital rights daily, by downloading multimedia content illegally from the Internet. The image protection is very important, as the image transmission covers the highest percentage of the multimedia data. Image encryption is one of the ways out to achieve this. Our world, built upon the concept of progression and advancement, has entered a new scientific realm known as Chaos theory. Chaotic encryption is one of the best alternative ways to ensure security. Many image encryption schemes using chaotic maps have been proposed, because of its extreme sensitivity to initial conditions, unpredictability and random like behaviors. Each one of them has its own strength and weakness. In this paper, some existing chaos based colour image encryption schemes are classified and analyzed with respect to various parameters like implementation, key management, security analysis and channel issues to fulfill some basic cryptographic requirements for chaos based image encryption algorithms from the year 2010 to 2014.

KEYWORDS

Chaotic algorithms, Cryptography and Chaotic maps.

1. INTRODUCTION

We live in a connected world and the internet play a major role in keeping us connected to share every last details of our life with others. In the realm of high-end internet technology, where size of a file and speed is not consideration, the greatest driving force in the transmission of multimedia data (audio, image and video) is the push towards making it more secure. When compared to audio and video in the multimedia transmission, the percentages of images are high. Image security is of more concern because of its widespread applications in Tele-medicine,

Sundarapandian et al. (Eds) : ITCCMA, FUZZY, SIGEM, DMDBS, NATL - 2015
pp. 07–19, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.50502

E-Learning, Electronic publishing, Electronic financial transactions, Confidential video conferences, Entertainments, Economics, Politics, Personal communication, Military communications. In order to protect these multimedia contents cryptography appears to be an appropriate tool.

Cryptography is the art and science of protecting information by converting text in intelligible form into an unintelligible form in the presence of adversaries [**22**]. It can use either a private key (single key) or public key (double key) to encrypt the secret message. In private key cryptography single key is used for both encryption and decryption. Key management is difficult and the computational speed of private key encryption is tolerable. In public key cryptography two keys are used, one for encryption and the other for decryption. Both the keys are mathematically related and it is infeasible to deduce one key from the other. But it is not suitable for real world applications where the encryption speed is of concern.

Image encryption has become an important way to protect an image against illegal copying and distribution and also become extremely vital especially, while transmitting it on the internet, intranets and extranets. Image encryption is nothing but converting an original image into cipher image that is difficult to understand for an unintended users.Color image encryption is generally implemented by extracting and encrypting each channel (Red, Green, & Blue) independently and then combining these to get the encrypted image. Decryption is to get back the original image from the cipher image. No one can view the content of an image without knowing a decryption key.

The classical ciphers like DES (Data Encryption Standard), AES (Advanced Encryption Standard) and RSA (Rivest, Shamir and Adleman) are most suited for text and binary encryption but not ideal for multimedia applications because of the following reasons[23]

1. Multimedia data such as audio, video and image are very large-sized and bulky.

2. In digital images, adjacent pixels often have similar grey-scale values and strong correlations or image blocks have similar patterns, while for video data, consecutive frames are similar and only few pixels would differ from frame to frame.

3. For many real-life multimedia applications like video pay-per-view system, it is important that very light encryption should be made to preserve some perceptual information.

An encryption level can be enhanced by combining chaos theory and the cryptography. Chaotic systems and cryptographic algorithms have similarities like ergodicity, sensitive to initial conditions and parameters.

Hence, chaos based image encryption techniques are considered to be good for practical applications. Sufficiently large numbers of Chaos based image encryption algorithms have been proposed by many researchers for secure image transmission over insecure channel **[**6, 19]. However many of the proposed schemes failed to explain or do not possess a number of features that are fundamentally important to all kind of cryptosystems.

A good chaos based image encryption algorithm must specify the some of the basic cryptographic requirements such as implementation, key management, security analysis and channel issues in order to evaluate their security and performance. New chaos based image encryption techniques are developed day after day by ignoring these simple requirements. An attempt is made to study the performance of some colour image encryption techniques proposed from the year 2010 to 2014.

Like rain in monsoon, new image encryption techniques are evolving and so we have selected 15 colour image encryptions schemes using different chaotic maps like Cat Map, Chebyshev, Henon, Logistic, standard and sine map in this article. All these schemes are good in their own regard. Each one is unique in their respective implementation, key management and security issues. Finding a single encryption technique that can satisfy all the cryptographic requirements [1] is an impossible task.

The rest of the paper is organized as follows: in section 2 we introduced the concepts of Chaos Theory and its relationship with cryptography. Existing colour image encryption schemes are explored in section 3. Descriptions about some chaotic maps are given in section 4. In section 5 the rules to optimize the performance of chaos based cryptosystems are itemized and conclusions are given in section 6.

2. CHAOS AND CRYPTOGRAPHY

Chaotic dynamical systems are ubiquitous in nature (such as tornado, stock market, population growth in ecology, turbulence and weather) and laboratory (electrical circuits, lasers, chemical reactions, fluid dynamics and mechanical systems). Chaotic behavior has also found numerous applications in electrical and communication engineering, information and communication technologies, biology and medicine. Poincare is believed to be the one who studied chaos first in 19th century. The "Butterfly Effect" was revealed by the father of chaos Edward Lorenz in 1963. In 1975, Li and Yorke published the paper "Period three implies chaos". Since then a lot of important concepts like Lyapunov exponents, dimensions and attractors have been introduced. [20, 24]

In a world of digital image encryption algorithms, there are umpteen number of applications developed with each have advantages / drawbacks over the others. Both cryptography and chaos theory dominate different parts of information security in remarkably different ways. But their similarities cannot be ignored, since both are best known for information protection against possible attacks. Chaos theory deserves credit for its bundle of unique properties.

In common usage, chaos means a state of disorder. Since there is no universally accepted mathematical definition of chaos, a commonly used definition is that, for a dynamical system to be said as chaotic, it must have the following properties:

1) It must be sensitive to initial conditions

2) Its periodic orbit must be dense

3) It must be topologically mixing

Dynamical systems are the study of how things change over time. Examples include the growth of populations, the change in the weather, radioactive decay, mixing of liquids such as the ocean currents, motion of the planets, the interest in a bank account. Some of these dynamical systems are well behaved and predictable, if we know how much money we have in the bank today, it should be possible to calculate how much we will have next month. However, some dynamical systems are inherently unpredictable and so are called chaotic. An example of this is weather forecasting, which is generally unreliable beyond predicting weather for the next three or four days. To quote Edward Lorenz, who was the first to realize that deterministic chaos is present in weather forecasting: Chaos is "when the present determines the future, but the approximate present does not approximately determine the future". In theory, if we could measure exactly the weather at some instant in time at every point in the earth's atmosphere, we could predict how it will behave in the future. But because we can only approximately measure the weather (temperature, wind speed and direction), the future weather is unpredictable.

Many fundamental concepts in chaos theory, such as mixing and sensitivity to initial conditions and parameters, coincide with those in cryptography. The similarities and differences between the two are given [9] in Table 1. Chaos based algorithms provide a good combination of speed, complexity, high security, reasonable computational overheads and computational power.

Table1. Similarities and differences between chaos and cryptography

Chaotic systems	**Cryptographic algorithms**
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	Rounds
Parameters	Key
Sensitivity to initial conditions /control parameters	Diffusion with a small change in the Plain Text / Key
Mixing	Diffusion with a small change in one PT-block of the whole PT
Ergodicity	Confusion
Deterministic dynamics	Deterministic pseudo-randomness
Structure Complexity	Algorithm (attack) complexity
Analytic methods	Algebraic methods

3. EXPLORATION OF EXISTING COLOUR IMAGE ENCRYPTION SCHEMES

In order to communicate an image over an insecure communication channel, it is necessary to develop an efficient chaos based image encryption algorithms. To meet this requirement, number of chaotic crypto systems has been proposed by researchers. Here is a list of fifteen such chaos-based cryptosystems.

3.1. "A Novel Image Encryption Algorithm based on Logistic Maps"

Dongming Chen et al [2] has proposed a block encryption algorithm using CBC (Cipher Block Chain) mode, two logistic maps and a secret key of 80-bits. Correlation analysis of two adjacent pixels, Histogram analysis, NPCR and UACI analysis as well as key sensitivity analysis are carried out by the authors to prove the security of their algorithm. The hardware implementation and an encryption time of this algorithm are stated by the authors.

3.2. "A Novel Color Image Encryption Algorithm Based on Chaotic Maps"

HuibinLu et al [5] has recommended an algorithm based on Chen and Lorenz systems to encrypt color images implemented in MATLAB 7.0 with the key space of about $\mathbf{10^{120}}$. In this algorithm, first image information is integrated into the Lorenz map, and then it is mixed into the Chen map via the Lorenz map. Correlation analysis of two adjacent pixels, Histogram and Entropy analysis, NPCR, UACI as well as key space and sensitivity analysis are carried out by the authors to prove the security of the algorithm. The infeasibility of Brute-Force attacks and Resistance attack has been verified by the authors.

3.3. "A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map"

Jianjiang CU Iet al [6] suggested a chaotic color image encryption method using Arnold-Cat and Chebyshev Maps with a key space of $\mathbf{2}^{\mathbf{153}}$. Correlation analysis of two adjacent pixels, Histogram and Entropy analysis, as well as key space and sensitivity analysis are carried out by the authors to prove the security of the algorithm. The infeasibility of brute-force attacks has been verified by the authors. The hardware implementation, digital arithmetic and an encryption time of this algorithm are documented by the authors.

3.4. "Improved Image Encryption Algorithm Using Chaotic Map", International Journal of Computer Applications"

Joshi Rohit A et al [7] introduced an improved image encryption scheme based on Henon Map. To resist plain text attacks, both parts of the keys are generated using plain image. Statistical analysis, Correlation analysis, Histogram analysis, Key sensitivity analysis and Differential analysis, NPCR and UACI are carried out by the authors to prove the security of the algorithm.

3.5. "A New Chaotic Algorithms for Image Encryption and Decryption of Digital Color Images"

K. Sakthidasan et al [19] designed an image encryption scheme, which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels and another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain image to resist attacks.Correlation analysis, Histogram analysis and Key sensitivity analysis are carried out by the authors to prove the efficiency of their algorithm.

3.6. "New Approach for Fast Color Image Encryption Using Chaotic Map"

Kamlesh Gupta et al [8] devised a technique which utilizes 3D Standard and 3D Cat Map with the key size of 148 Bits to provide better encryption. Correlation analysis, Histogram and Entropy analysis, as well as key space and sensitivity analysis, Differential analysis, NPCR, UACI, FIPS TEST and MAE are carried out by the authors to prove the security of the algorithm. The infeasibility of brute-force and differential attacks has been verified by the authors. The hardware and software implementation (MATLAB 7.0) are documented by the authors.

3.7. "An Inter-Component Pixels Permutation Based Color Image Encryption Using Hyper-chaos "

Musheer Ahmad et al [12] proposed an algorithm based on the concept of inter-component shuffling of image pixels using Arnold Cat Map and 2D hyper-chaotic system with the key space of about $\mathbf{10}^{\mathbf{-14}}$. To encrypt all pixels, XOR operation and CBC mode is used. Correlation analysis of two adjacent pixels (H, V & D), Chi-Square Test, Histogram and Entropy analysis, as well as NPCR are carried out by the authors.

3.8. "A New Chaos-Based Image Encryption Scheme for RGB Components of Color Image"

Nashwan A. Al-Romema et al [13] introduced an image encryption algorithm based on chaotic logistic map implemented in MATLAB. They used another image as a key, that should be larger or of the same size of the plain image. Correlation analysis of two adjacent pixels (R, G & B), Histogram analysis and MSE, as well as key sensitivity analysis are carried out by the authors to prove the security of the algorithm. The infeasibility of Brute-Force attacks has been verified by the authors.

3.9. "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map"

Ni G. A. P. Harry Saptarini et al [4] has suggested a color image encryption method implemented in C# (2005) based on RC4 stream cipher and chaotic logistic map with the key size of 256 Bytes. Experimental results such as Histogram and Entropy analysis, Key Sensitivity Test as well as NPCR and UACI are carried out by the authors.

3.10. "A Proposed Permutation Scheme Based On 3-D Chaotic System For Encrypting The Colored Images"

Osama M. Abu Zaid et al [14] proposed a color image encryption algorithm implemented in MATLAB 7.0 based on Chen's chaotic system. The experimental results and analysis like Correlation analysis of two adjacent pixels, Histogram analysis, NPCR and UACI analysis as well as key sensitivity analysis and Signal / Noise Ratio are carried out by the authors to prove the security of the algorithm. The hardware implementation details are specified by the authors.

3.11. "High Security Nested PWLCM Chaotic Map Bit-Level Permutation Based Image Encryption"

An image encryption scheme based on Nested Piece Wise Linear Chaotic Map with 96 Bits key size is proposed by QassimNasir et al [15]. The system is stream cipher architecture. The experimental results such as Correlation analysis of two adjacent pixels (H, V & D), Histogram and Entropy analysis, NPCR and UACI are carried out by the authors to prove the security of the algorithm.

3.12. "Enhancement and Analysis of Chaotic Image Encryption Algorithms"

An encryption algorithm implemented in MATLAB based on combining the Logistic and Henon maps to expand the parameters is proposed by R. Raja Kumar et al [16]. The pixel values of an image are changed by the XOR operation with chaos sequences generated by Logistic and Henon maps, and cyclic shift in binary. The experimental results such as Histogram Entropy analysis, NPCR and UACI are carried out by the authors. Key parameters and its ranges are also specified in this paper.

3.13. "An Improved Image Encryption Scheme Using Chaotic Logistic Maps"

Ravindra K. Purwar et al [17] presented an image encryption algorithm based on 2 chaotic logistic maps with 80-bit secret key to derive an initial condition. The initial conditions for the second logistic map are determined by the outcome of first logistic map and the secret key. Depending upon the outcome of the second logistic map, algorithm performs any of eight different types of operations on image pixels. The secret key is modified after encrypting a block of 16-pixels. Along with the hardware implementation details, experiment results like Correlation analysis, Histogram and Encryption Time analysis as well as key sensitivity analysis are carried out by the authors.

3.14. "New Algorithm For Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation"

Rui Liu et al [18] proposed a SBLP and chaotic map to encrypt color image with the key space of about $\mathbf{10^{68}}$. Logistic chaotic sequence is used to shuffle the positions of image pixels and another Logistic map is used to rearrange the positions of the image pixels. The security analysis and experimental results such as Correlation analysis Correlation analysis, Histogram analysis, NPCR and UACI as well as key sensitivity analysis are carried out by the authors.

3.15. "Image Encryption and Decryption Using Chaotic Maps and Modular Arithmetic"

Shyamsunder et al [20] proposed encryption and decryption of an image using three different chaotic maps and modular arithmetic with the key space of about $\mathbf{2^{128}}$. Out of the three different maps, they suggested that the logistic mapis the fastest of all. Security analysis which includes Statistical analysis, Correlation analysis, Histogram analysis, Key sensitivity analysis, Chosen / Known Plain Text attacks, Encryption time and DMF (Deviation Measuring Factor) are carried out by the authors to prove the security of the algorithm.

4. CHAOTIC MAPS

Some of the chaotic maps used in the above reviewed papers are presented in this section.

4.1. MAPS

Systems can change at discrete times. A discrete time dynamical system is also called as Map. The dynamics is then given by a list of numbers. For example x_0=125, x_1=250, x_2=500, x_3=100, ...x_n represents the state variable x at the nth time instant. A map is then given by $\mathbf{x_{n+1} = F\ (x_n)}$ where $F(x_n)$ is the mathematical rule (function) governing the evolution of the system.

Chaotic maps are with a long history in nonlinear dynamical studies. Chaos can be produced by both discrete and continuous equations mathematically. The discrete systems such as Logistic map, Henon map, Standard map and Circular map can be expressed as [23] $\mathbf{x_{n+1} = F\ (x_n)}$.

The continuous systems are known as flows, which can be expressed as $\mathbf{dx(t) / dt = F(x(t))}$.

The Lorenz equation, Rossler equation, Duffing's equation and Chua's circuit are some of the chaotic flows. The discrete maps and continuous flows have close relationship with one another.

4.2. LOGISTIC MAP

A system with sensitive dependence on initial conditions is the logistic equation [25]

$$X_{n+1} = R\ X_n\ (1 - X_n)$$

where R is a parameter, and X_n is the variable at the n^{th} iteration with value between 1 and 0, and n can be considered as the running variable. It is a recursive equation, which generates a new value from the previous value. It can be used as a simple model for species population with no predators, but limited food supply. In this case, the population is a number between 0 and 1, where 1 represents the maximum possible population and 0 represents extinction. R is the growth rate, and n-generation number. Logistic equation was proposed by Pierre Verhulst in 1845 [20].

4.3. ARNOLD CAT MAP

In mathematics, **Arnold's cat map** is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, hence the name.

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \text{MOD N}$$

where N is the width / height of the image.

4.4. STANDARD MAP 3D

The **standard map** (also known as the **Chirikov–Taylor map** or as the **Chirikov standard map**) is an area-preserving chaotic map from a square with side 2π onto itself [25]. It is constructed by a Poincaré's surface of section of the kicked rotator, and is defined by:

$$P_{n+1} = P_n + K \sin(\theta_n)$$

$\theta_{n+1} = \theta_n + P_{n+1}$ where P_n and θ_n are taken modulo 2π.

The properties of chaos of the standard map were established by Boris Chirikov in 1969.

4.5. LORENZ SYSTEM

In 1963, Edward Lorenz developed a simplified mathematical model for atmospheric convection. The model is a system of three ordinary differential equations now known as the Lorenz equations [25]

$$x^{\cdot} = a(y - x)$$

$$y^{\cdot} = cx - xz - y$$

$$z^{\cdot} = xy - bz$$

which is chaotic when $a = 10$, $b = 8/3$, $c = 28$.Here x, y and z make up the system state and a, b, c are the system parameters. The Lorenz equations also arise in simplified models for lasers, dynamos, brushless DC motors, electric circuits,chemical reactionsand forward osmosis. The Lorenz system is nonlinear, three-dimensional and deterministic.

4.6. CHEN SYSTEM

In 1999, Chen found chaotic attractor, also in a simple three-dimensional autonomous system, which nevertheless is not topologically equivalent to the Lorenz's equations [25]

$$x = a(y_0 - x_0)$$

$$y = (c - a)x_0 - x_0 z_0 + c y_0$$

$$z = x_0 y_0 - b z_0$$

is chaotic when a = 35, b = 3, c = [20, 28]

4.7. SINE MAP

Sine map is defined as [25]

$$X_{n+1} = a\ x_n^2 \sin(\pi\ x_n)$$

when $x_0 = 0.7$ and a=2.3, equation 2 has the simplified form. For the interval (0, 1) it generates chaotic sequence.

4.8. HENON MAP

The map was introduced by Michel Henon as a simplified model of the Poincare section of the Lorenz model [25]. The Henon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Henon map takes a point (x_n, y_n) in the plane and maps it to a new point

$$X_{n+1} = 1 - a\,X_n^2 + Y_n$$

$$Y_{n+1} = b\ Xn$$

The map depends on two parameters, *a* and *b*, where a = 1.4 and *b* = 0.3. For the classical values the Henon map is chaotic.

5. RULES TO OPTIMIZE THE PERFORMANCE OF CHAOS BASED CRYPTOSYSTEMS

The internet has numerous chaotic image encryption algorithms floating around and it is very difficult to evaluate which one of them is actually worth in terms of security and performance. Evaluating an algorithm is quite a finicky process. All the algorithms need to be calibrated to some sort of baseline and the tools used must be up to the task. Gonzalo Alvarez and Shujun Li suggested the following rules that researchers need to keep in mind while designing chaotic image encryption algorithms in order to eliminate the difficulties faced by the cryptanalysts.

Rule 1 A thorough description of the implementation of the chaotic systems involved should be provided.

Rule 2 For chaotic systems implemented in digital form, the negative effects of dynamical degradation should be taken into consideration with careful evaluation.

Rule 3 Without loss of security, the cryptosystem should be easy to implement with acceptable cost and speed.

Rule 4 The key should be precisely defined.

Rule 5 The key space K, from which valid keys are to be chosen, should be precisely specified and avoid non-chaotic regions.

Rule 6 The useful chaotic region, i.e., the key space K, should be discretized in such a way that the avalanche effect is guaranteed: two cipher texts encrypted by two slightly different keys k1, k2 should be completely different.

Rule 7 Partial knowledge of the key should never reveal partial information about the plaintext nor the unknown part of the key.

Rule 8 The algorithm or process of generating valid keys from the key space K should be precisely specified.

Rule 9 For two keys (or two plaintexts) with the slightest difference, no distinguishable difference between the corresponding cipher texts can be found by any known statistical analysis.

Rule 10 The cipher text should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all keys.

Rule 11 It should be checked whether the designed cryptosystem can be broken by the relatively simple known-plaintext and chosen-plaintext attacks, and even chosen-ciphertext attacks.

Rule 12 Resistance to differential and linear cryptanalysis should be proved or checked very carefully in digital block ciphers.

Rule 13 It should be checked whether the cryptosystem can be broken by all known chaos-specific attacks.

Rule 14 It should be checked whether the cryptosystem can be broken by all known application specific attacks.

Rule 15 To provide a sufficient security against brute-force attacks, the key space size should be $K > 2^{100}$.

Rule 16 When a keystream cipher is used, the security study should include the statistical test results conducted on the pseudo-random number generator.

Rule 17 A designed secure communication system should work in a real channel environment with−40 dB signal/noise ratio, with a certain limited bandwidth, and with attenuation between 0 dB and 16 dB.

Performance evaluations of the reviewed chaotic colour image encryption algorithms based on the above rules are summarized in Table 2.

6. CONCLUSIONS

As more and more image transmission go online, the responsibility to safeguard this, falls on the shoulders of cryptologists. Chaotic image encryption is one of the best ways to ensure security of image transmission. Numerous image encryption schemes using chaotic maps have been proposed. Each one is unique in designing their algorithms and its performance. Picking the precise one is totally dependent on the respective applications. In this analysis, we investigate issues like key related issues, security analysis and channel issues. Correlation and Histogram analysis were specified in all [2,4,5,6,7,8,12,13,14,15,16,17,18,19,20] the reviewed research articles. NPCR and UACI were carried out by most [2,4,5,6,7,8,12,14,15,16,18] of the research papers in order to prove the efficiency of their algorithms. Details like implementation, key related issues, encryption type, resistance against cryptographic and chaos specific attacks are not specified clearly in most of the papers. In some articles, security measures like Mean Absolute Error [8], Mean Square Error [13], Entropy Analysis [4,5,6,12,13,14,15,18], Deviation Measuring Factors [20] and FIPS Test [8] were incorporated. To summarize, if the rules recommended by Gonzalo Alvarez and Shujun Li are followed, a reasonable degree of security and most acceptable features of cryptography can be guaranteed.

Table 2. Performance Analysis of Reviewed Colour Image Encryption Algorithms based on its Cryptographic Requirements

S No				Ref. No.	[3.1]	[3.2]	[3.3]	[3.4]	[3.5]	[3.6]	[3.7]	[3.8]	[3.9]	[3.10]	[3.11]	[3.12]	[3.13]	[3.14]	[3.15]
1.	Encryption Schemes	Symmetric		Stream			↵								↵				
				Block	↵						↵						↵		
		Asymmetric																	
		Hashing																	
2.	Encryption Algorithm				Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algm.+RC 4 designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors	Algorithm designed by Authors
3.	Chaotic Map Used (Dimension & Map Name)				1D – 2 Logistic Map	Chen & Lorenz	2D ACM & Chebyshev Map	1D Henon Map	Lorenz, Chen LU	3D standard & 3D cat map	ACM 3D, 2D Hyper-Chaotic map	Logistic Map	Logistic Map	CHEN'S CHAOTIC SYSTEM	NPWLCM	Logistic Map & Henon Map	2 Logistic Map	Logistic Map	Logistic, Chebyshev & Sine Map
4.	Performance Parameter	Chaotic Cipher	Analog																
			Digital	1.C P	-	-	↵	-	-	-	-	-	-	-	-	-	-	-	-
				2.DA	-	-	↵	-	-	-	-	-	-	-	-	-	-	-	-
				3.HSC	P4, 256RAM	-	AMD II, 2GB RAM	-	-	INTEL, 2GB RAM	-	-	-	INTEL I3, 3GB RAM	-	-	INTEL I3, 4GB RAM		INTEL,1.96 GB RAM
		Key Related Issues		Key Size	80-Bit		153 Bits	-	16 Byte	148 Bits		IMAGE	256 Bytes	-	96 Bits		80 Bits		
				Key Space	-	10^{120}	2^{153}	-	-	2^{148}	10^{-14}	Very Large	-	-			2^{80}	10^{68}	2^{128}
			Key Space Analysis	Brute - Force Attacks($K>2^{100}$)	-	↵	↵	-	-	↵		-		-				↵	↵
				Key Sensitivity Test	-	↵	↵	Encryption & Decryption	↵	↵	↵ [NA]	Encryption & Decryption	↵	↵			↵	↵	↵
			Key Sensitivity Analysis	Para Sensitivity	-	↵	↵	-	-	-	-	-	-	↵	-	-	-	↵	-
				I C Sensitivity	-	↵	↵	-	-	-	-	-	-	↵	-	-	-	-	-
				Ergodicity	↵	↵	↵	↵	↵	↵	-	↵	↵	↵	-		↵	↵	↵

Parameters applied - ↵

CP	Computing Precision	DA	Digital Arithmetic	HSC	Hardware Software Configuration	SA	Statistical Analysis
HA	Histogram Analysis	CAP	Correlation of Adjacent Pixels	CA	Cryptographic Attacks	DCA	Differential Crypt Analysis
LCA	Linear Crypt Analysis	CSA	Chaos Specific Attacks	EMS	Extraction Message Signal	ECC	Extraction of Chaotic Carrier Signal
ESP	Estimation of Secret Parameters	EA	Efficiency Analysis	AE	Avalanche Effect	ET	Encryption Time
NPCR	Number of Pixels Change Rate	UACI	Unified Average Changing Intensity	MSE	Mean Square Error	DMF	Deviation Measuring Factor

ACKNOWLEDGEMENTS

I cannot express enough thanks to my family members, my mentors and to my innumerable friends and colleagues within and outside Presidency College who have helped to nurture an environment of creativity and support.

My deepest gratitude goes to Dr. (Mrs.) N. Rama who listened with endless patience and enthusiasm to my thoughts and long stories. Without her this could not have been possible.

Finally I would like to thank Secretary, ITCCMA – 2015 and the reviewers for their help and support.

REFERENCES

[1] Gonzalo Alvarez and Shujun Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.

[2] Dongming Chen, Yunpeng Chang, "A Novel Image Encryption Algorithm based on Logistic Maps", Advances in Information Sciences and Service Sciences Issues, Vol. 03, No.7, August 2011, pp. 364-372.

[3] Hao B. 1993, "Starting with parabolas: an introduction to chaotic dynamics", Shanghai China: Shanghai Scientific and Technological Education Publishing House.

[4] Ni G. A. P. Harry Saptarini, YosuaAlberth Sir, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map", Information Systems International Conference, December 2013, pp. 459-464.

[5] Huibin Lu, Xia Xiao," A Novel Color Image Encryption Algorithm Based on Chaotic Maps", Advances in information Sciences and Service Sciences(AISS), Volume3, Number11.

[6] Jianjiang CUI, Siyuan LI, DingyuXue, "A Novel Color Image Encryption Algorithm Based on Chaotic Maps"

[7] Joshi Rohit A, Joshi Sumit S, G. P. Bhole, "A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map", International Journal of Computer Science Issues, Vol. 10, Issue 3, No.2, May 2013, pp. 63-69.

[8] Kamlesh Gupta, Sanjay Silakari, " New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, 2, 139-150.

[9] IgorMishkovski&Ljupcokocarev, 2011, Chaos-Based Public-Key Cryptography, Chaos-Based Cryptography, SCI 354, pp. 27-65, Springer-Verlag Berlin Heidelberg 2011.

[10] Lorenz EN. 1993, "The Essence of Chaos", University of Washington Press, Seattle, WA.

[11] Mao, Y., & Chen, G. 2005, "Chaos-based image encryption.", Handbook of Geometric Computing, 231-265.

[12] Musheer Ahmad and Hamed D Al-Sharari, "An Inter-Component Pixels Permutation Based Color Image Encryption Using Hyper-chaos"

[13] Nashwan A. Al-Romema, Abdulfatah S. Mashat, Ibrahim AlBidewi, "A New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Sciences and Engineering, 2012, 2(5); pp. 77-85.

[14] Osama M. Abu Zaid, Nawal A. El-Fishawy, E. M. Nigm, "High Security Nested PWLCM Chaotic Map Bit-Level Permutation Based Image Encryption", International Journal of Communications, Network and System Sciences, 2012, 5, pp. 548-556.

[15] QassimNasir, Hadi H. Abdlrudha, "High Security Nested PWLCM Chaotic Map Bit-Level Permutation Based Image Encryption", International Journal of Communications, Network and System Sciences, 2012, 5, pp. 548-556.

[16] R. Raja Kumar, Dr. A. Sampath, Dr. P. Indhumathi, "Enhancement and Analysis of Chaotic Image Encryption Algorithms", Computer Science & Information Technology, Vol. 10, No.2, 2011, pp. 143-153.

[17] Ravindra K. Purwar, Priyanka, "An Improved Image Encryption Scheme Using Chaotic Logistic Maps", International Journal of Latest Trends in Engineering and Technology, Vol. 02, Issue.3, May 2013, pp. 220-224.

[18] Rui Liu, Xiaoping Tian, "New Algorithm For Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation", Journal of Theoretical and Applied Information Technology, Vol. 43, No.1, 2012, pp. 89-93.

[19] K. Sakthidasan, B. V. Santhosh Krishna, "A New Chaotic Algorithms For Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No.2, June 2011, pp. 137-141.

[20] S. Shyamsunder, Ganesan Kaliyaperumal, "Image Encryption and Decryption Using Chaotic Maps and Modular Arithmetic", American Journal of Signal Processing, 1(1), 2011, pp. 24-33.

[21] Wallace K. S. Tang and Ying Liu, "Formation of High-Dimensional Chaotic Maps and Their Uses in Cryptography", Chaos-Based Cryptography, SCI 354, pp. 27-65, Springer-Verlag Berlin Heidelberg 2011.

[22] William Stallings, "Cryptography and Network Security Principles and Practice", Prentice Hall, Fifth Edition.

[23] Zhaopin Su, Guofu Zhang and Jianguo,"Multimedia Security: A Survey of Chaos-Based Encryption Technology", Jiang School of Computer and Information, Hefei University of Technology China.

[24] Zonghua Liu, " Review Article Chaotic Time Series Analysis" , Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2010, Article ID 720190.

[25] http://en.wikipedia.org/wiki/Logistic_map

AUTHOR BIOGRAPHIES

K. S Tamilkodi received her B. Sc. (Mathematics) in 1992, M.C.A. in 1995 from University of Madras and M.Phil. (Computer Science) in 2001 from Mother Teresa University, Kodaikanal. She is now an Assistant Professor of Computer Science in PresidencyCollege, Chennai and Ph.D. student in Bharathiar University, Coimbatore. Her research is in the area of information security.

N Rama received her B.Sc.(Mathematics) in 1986, M.C.A. in 1989 and Ph.D. in 2003 from the University of Madras. Presently, she is an Associate Professor of Computer Science in Presidency College, Chennai and Guiding Ph. D. in various Universities. Her research is in the area of information security, image processing and compression. She is a co-author of about 12 research articles in national, international conference proceedings and journals. She has produced 5 Ph. D. scholars.