Implementation of Secured Image Encryption Using Chaotic Logistic Map: Comparative Study

Wut Yee Pwint Hlaing, Dr. Zin May Aye
University of Computer Studies, Yangon
wutyeepwinthlaing.wyph@gmail.com,zinmayaye.ucsy@gmail.com

Abstract

Nowadays, image information is routinely used in many applications. This paper presents comparative study for image encryption based on Chaotic Logistic Map with external secret key of both 80 bit and 256 bit with different logistic maps. Security is critical issue when images are sent from journalist to editor via communication channel. To apply image security on this media system, journalist encrypts and sends cipher image to editor and only authorized editor can decrypt cipher image. Chaotic Logistic Map with 80 bit is implemented in web based system because of its randomness, less correlation and unpredictable behavior in long term that are secure and safe. Chaotic Logistic encryption scheme provides good combination of highly secured, fast processing, efficient and secure way for image encryption. Correlation coefficient, NPCR (change rate of the number of pixels of ciphered image) and histogram are analyzed to prove security of algorithm used in this system.

1. Introduction

In recent years, with the rapid development of computer science and network technology, people are obtaining, using and processing digital images more frequently. This situation brings us convenience, as well as potential threats. How to protect the information within the digital images from the attacks of intruders is becoming a more and more serious problem.

Encryption is a good solution of this problem because of the certain characteristics of digital images: redundancy of data, strong correlation among adjacent pixel, less sensitive comparing to the text data, especially the large quantities of data and the requirement of real-time processing. To solve this problem, new encryption algorithms derived from chaotic systems are proposed and owning to the important properties of chaotic systems, such as the sensitive dependence on initial conditions and pseudo-random array which is hard to predict after a certain times of iteration. Chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, reasonable computational overheads and computational power etc.

This paper proposed the symmetric key encryption algorithm for securing images based on chaos. Then, the system compares correlation coefficient, NPCR, histogram and analyzes the processing time of these algorithms with comparative study. Besides, image encryption with chaotic logistic map is applied in media system, journalists can send cipher images to editors and editors decrypt that cipher in order to improve security of media system.

This paper is organized as follows: The first section is the introduction of the system. Section 2 explains related work for the system. Section 3 explains cryptography and image encryption.

Section 4 explains chaotic system and chaotic logistic map which is used in this paper. Section 5 and 6 describe proposed system and the implementation of the system. Experimental result of the system is explained in section 7 and the paper is concluded in section 8.

2. Related work

Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data. However, conventional cryptosystem is not suitable for image encryption because of the special storage characteristics of an image. Thus, the idea of using chaos in data encryption has been introduced and discussed.

Deterministic oscillations, called chaos, used to be treated as stochastic and unpredictable phenomena [1]. Nowadays, this stochastic-like behavior that chaotic oscillations presents, characterized by a large broadband frequency spectrum, has been used to hide information, in order to safely transmit secret messages. Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, Shinsaku Mori proposed a secret key cryptosystem by iterating a one dimensional chaotic map based on characteristics of chaos, which are sensitivity of parameters, sensitivity of initial points, and randomness of sequences obtained by a chaotic map [2]. Jui-Cheng Yen and Jiun-In Guo proposed a new chaotic key-based design for image encryption and its VLSI architecture and proved Chaotic key-based Algorithm features low computational complexity, high security and no distortion [3]. Shiguo Lian, Jinsheng Sun, Zhiquan Wang proposed through studying the strengths of the confusion and diffusion properties, some enhancement can improve the cryptosystem, diffusion function and iteration time [4]. Smet Öztürk1 and Brahim analyze and compare Image Encryption algorithms [5]. N.K. Pareek, Vinod Patidar, K.K. Sud proposed a new approach for image encryption based on chaotic logistic maps in order to meet the requirements of the secure image transfer. In the proposed image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed [6]. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah proposed new features of the proposed stream cipher include the heavy use of data-dependent iterations, data-dependent inputs, and the inclusion of three independent feedback mechanisms. These proposed features are verified to provide high security level [7]. Nidhi Sethi proposed a new method to develop secure image-encryption techniques using a Chirikov Standard Map and Logistic Map [8]. Nisha Kushwah, Madhu Sharma proposed a cryptographic algorithm using one-dimensional chaotic maps and an external secret key [9]. Prabir Kr. Naskar, Atal Chaudhuri proposed a symmetric image encryption based on bit-wise operation and proved secure cryptosystem [10].

3. Cryptography

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity and entity authentication. It enables you to store sensitive information as it transmit across insecure networks like internet to keep information secure from unintended audience of encrypting it. Only the use of a secret key can convert the cipher back into human readable form. Cryptography can be broadly classified into the symmetric key system both the sender and recipient have a single secret key and for public-key system that use two different keys, a public key known to everyone and a private key belongs to only the recipient.

Encryption can be applied to text, image and video for data protection. Image encryption techniques try to convert an image to another one that is hard to understand. The main aim of digital image encryption is to transform a meaningful image into a meaningless in order to enhance the power to resist invalid attack and in turn enhance security. Image encryption is somehow different from text encryption due to some features of images, such as bulk data capacity and high correlation among pixels. Conventional cryptographic techniques such as DES, IDEA and RSA are no longer suitable for practical image encryption because of special storage characteristics of an image, especially for real-time communication scenarios. Due to the tight relationship between chaos and cryptography, chaotic systems have been widely used in image encryption to realize diffusion and confusion in a good cipher.

4. Chaotic system

Chaos-based techniques have been involved in data security and confidential communication system. The rule's repeated application the long-term behavior and becomes quite complicated and difficult or impossible to predict. The two basic properties of chaotic systems are the sensitivity to initial conditions and mixing property. Sensitivity to initially close points, they iterates quickly diverged, and bear no correlation after a few iterations. Sensitivity to parameters causes the properties of the map to change quickly when the parameters on which the map depends on mildly disturbed. Mixing is the tendency of the system to quickly confuse small portions of the state space into an intricate network so that two nearby points in the system totally lose the correlation they once shared and get scattered all over the state space. These properties are the key aspects of chaotic maps that have allowed them to be used to generate complicated patterns of pixels and the gray levels in an image.

There are two iterative stages in this cryptosystem: confusion and diffusion. Confusion permutes the pixels in the image, without changing its value. Diffusion is modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image called substitution. Chaotic Logistic Map is a symmetric key encryption. Therefore, Logistic Maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, efficient and excellent security.

4.1. Chaotic Logistic Map

The logistic map is very simple mathematical system and a sort of dynamical system which involves no derivatives and no integrals. But this function exhibits the universal features of the behavior, such as the period-doubling leading to chaos. It is defined as follows.

$$x_{n+1}=3.9999\,x_n(1-x_n) \tag{1}$$

where x_n takes values in the interval [0,1].

4.2 Chaotic Logistic Map with 80 bit external secret key

In this algorithm, a symmetric secret key of 80 bit is needed. Two chaotic logistic maps are needed for the key expansion and applied in encryption or decryption and key modification processes.

4.2.1. Key Expansion In this algorithm, secret keys which are 20 4-bit blocks of hexadecimal characters are needed. $k=k_1k_2k_{20}$ Each group of two alphanumeric characters constitutes a session key. $K = K_1 K_2 K_{10}$ where K_i represents one 8 bit block in ASCII of a session key. In addition, we expanded ASCII value of session keys in the background.

4.2.2 Chaotic Logistic Map with external 80 bit secret key and two logistic maps

Two logistic maps are used in order to obtain chaotic sequences with improved cryptographic feature. All these advantages make this more secure cryptosystem for the use information transmission over insecure channel and secure application.

To generate initial conditions of operations, an 80 bit long secret key is utilized. The secret key is divided into 20 4-bit blocks, referred as 10 session keys of 8 bit each. At key initialization phase, a chaotic logistic map is used, and after each block encryption, another chaotic logistic map is used for key transformation. This algorithm use two chaotic logistic maps to make the confusion and diffusion and also operations to encrypt the original image. The original coordinates (x_n ,y_n) can be translated into the new coordinate (xn+1 , yn+1) by using the following formulas. Use first logistic Map to decide which operation to choose to encrypt the image.

$$X_{n+1} = 3.9999X_n(1-X_n) \qquad (2)$$

Use the initial parameter for the second logistic map which is used to do the key transformation.

$$Y_{n+1} = 3.9999Y_n(1-Y_n) \qquad (3)$$

After n times of interaction, we assign different type of operations corresponding to different value of Y_0 . In each interaction, we use a map to convert Y0 into an integer In.

$$I_n=(Y_n * 100000 + f(data)) \bmod 10 \qquad (4)$$

where f(data) computes the no of binary 1 in the last cipher image block.

Table 1. The corresponding operation on the different values of I_n

Group No	I_n value	Operation of encryption/decryption
1	1	$Data \oplus (K_1 + K_2 + K_9)$
2	2	$Data \oplus (K_2 + K_4 + K_8)$
3	3	$Data \oplus (K_3 + K_6 + K_8)$
4	4	$Data \oplus (K_4 + K_8 + K_7)$
5	5	$Data \oplus (K_5 + K_1 + K_6)$
6	6	$Data \oplus (K_6 + K_3 + K_4)$
7	7	$Data \oplus (K_7 + K_5 + K_3)$
8	8	$Data \oplus (K_8 + K_7 + K_2)$
9	9	$Data \oplus (K_9 + K_9 + K_1)$
10	0	$Data \oplus K_{10}$

After the encryption of an 8 bit block of image file, modify session keys K1 to K10.

$$(K_i)_{10} = ((K_i)_{10} + I_n) \bmod 256 \quad (1 \le i \le 10) \quad (5)$$

If the image file is not completely encrypted, algorithm repeats steps (3) to (5) until the entire image file is exhausted. Thus, in this Chaotic

Logistic Map with 80 bit encryption algorithm, second logistic map is used to transform the session keys, which assures the unpredictability of the session keys. The encryption and decryption process will take some time because of several iterations on second logistic map and key modification. It will take some time depend on the number of pixels in image file. The decryption process is similar to the encryption process.

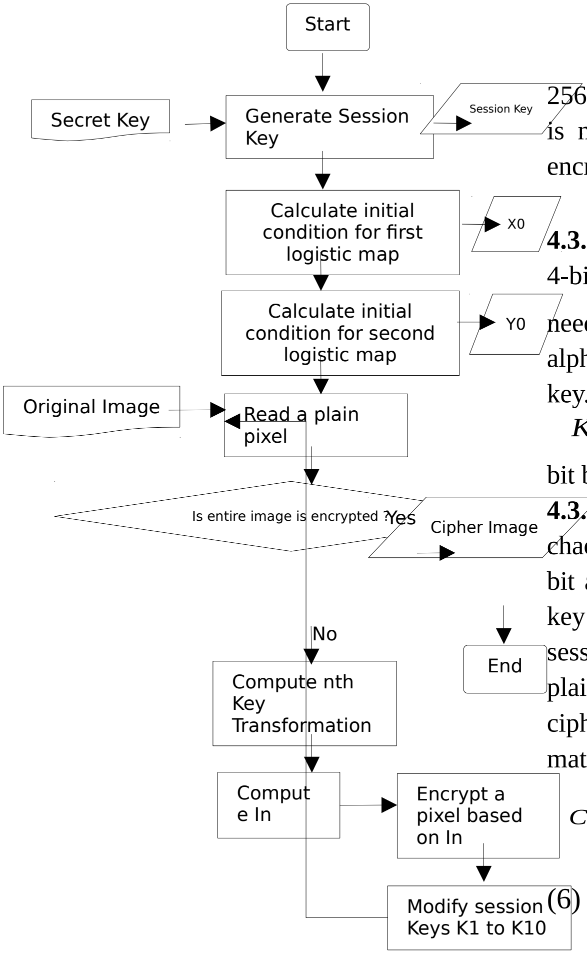

Start
Secret Key
Generate Session Key
Session Key
Calculate initial condition for first logistic map
X0
Calculate initial condition for second logistic map
Y0
Original Image
Read a plain pixel
Is entire image is encrypted ?
Yes
Cipher Image
No
End
Compute nth Key Transformation
Comput e In
Encrypt a pixel based on In
Modify session Keys K1 to K10

Figure 1. Chaotic Logistic Map with 80 bit secret key Encryption Scheme

4.2.3. Key Modification After the encryption of an 8 bit block of image file, modify session keys K1 to K_{10}.

$$(K_i)_{10} = ((K_i)_{10} + I_n) \bmod 256 \ (1 \le i \le 10)$$

Then next plain pixel is read until entire image is encrypted as in figure 1.

4.3 Chaotic Logistic Map with 256 bit external secret key

In this algorithm, a symmetric secret key of 256 bit is needed. Only one chaotic logistic map is needed for the key expansion and used for encryption or decryption processes.

4.3.1. Key Expansion Secret keys which are 64 4-bit blocks of hexadecimal characters are needed. $k = k_1 k_2 k_{64}$. Each group of two alphanumeric characters constitutes a session key.

$K = K_1 K_2 K_{32}$ where Ki represents one 8 bit block in ASCII of a session key.

4.3.2. Encryption In this algorithm, only a chaotic logistic map is used and block size of 8-bit and 256-bit secret key is utilized. The secret key is divided into 64 4-bit blocks, referred as 32 session keys of 8 bit each. Encryption of each plain image pixel P_i to produce its corresponding cipher image pixel C_i can be expressed mathematically as:

$$C_i = \left(P_i + M2\left[\sum_{i=1}^{¿_i} rX_i(1-X_i)\right]\right) \bmod 256 \qquad (6)$$

where X_i represents the current input for logistic map and computed as:

$$X_i = M1\left[X_{\text{i-1}} + C_{i-1} + K_i\right]$$

(7)

#$_i$ is the number of iteration of logistic map for its current input X$_i$ and calculated as: $\text{¿}_i = K_{i+1} + C_{i-1}$

(8)

A chaotic logistic map is used for diffusion key transformation.

$$X_{n+1} = 3.9999\,X_n(1 - X_n)$$

(9)

M1 is mapping from the session, key space, all integers between 0 and 255, into the domain of the logistic map, M2 maps the domain of the logistic map back into the interval [0,255].

4.3.3. Decryption The decryption module works in the same way as the encryption module but now the output of the logistic map is subtracted from the corresponding cipher image pixel C$_i$. To decrypt each cipher image pixel *C*$_i$, corresponding plain image pixel *P*$_i$ can be expressed mathematically as:

$$P_i = \left(C_i - M2\left[\sum_{i=1}^{\text{¿}_i} rX_i(1 - X_i)\right]\right) \text{ mod } 256 \qquad (10)$$

5. Proposed System

This system consists of two main parts. The first part is algorithm implementation and comparative analysis. Both Chaotic Logistic Map with 80 bit key and 256 bit key is implemented and analyzed with the following procedure. Input image file is opened to encrypt and decrypt. Then, the user chooses Chaotic Logistic Map with 80 bit or 256 bit algorithm for encryption and decryption processes by entering respective secret keys. After encryption and decryption process, their analysis results are compared and displayed.

According to three type of analysis applied on both 80 bit and 256 bit described in section 6, Chaotic Logistic Map with 80 bit is applied in Media system because of its characteristics. The second part is to design and implement image encryption algorithm on Media System by using Chaotic Logistic Map that can enhance security of a community sharing. Sending plain images from journalist to editor via communication channel cannot be secured enough. It is needed to consider secured image encryption scheme for security. To apply the strength of image encryption on media system and enhance security on the system, only cipher image encrypted from journalist is stored in database and editor will retrieve it and decrypt with secret key which is both agree as symmetric key.

Figure 2 delineates algorithm implementation of both 80 bit and 256 bit with correlation coefficient, NPCR and histogram analysis.

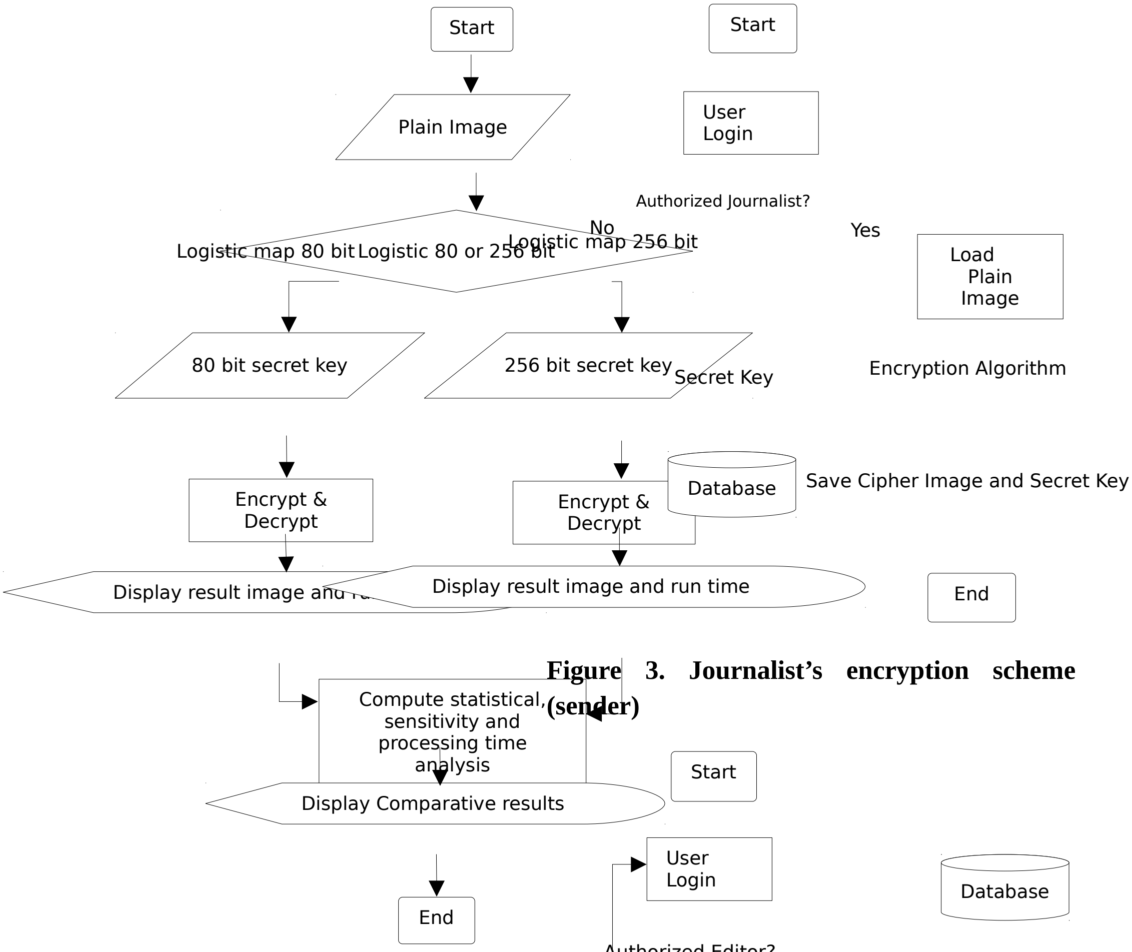


Figure 2. System flow diagram for algorithm implementation and analysis

Figure 3 and 4 describe encryption and decryption process from sender and receiver sides of the media system.

Figure 3. Journalist's encryption scheme (sender)

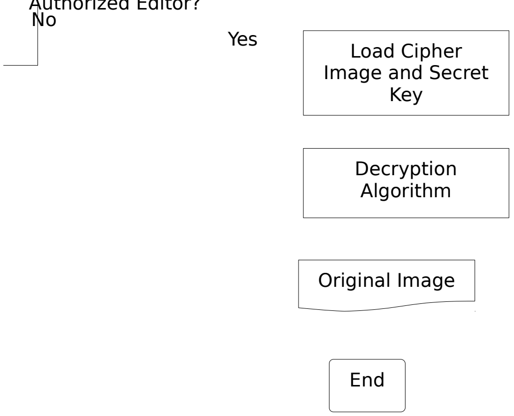
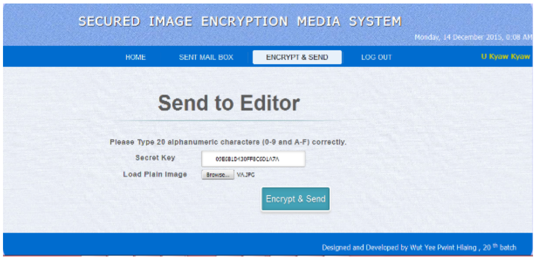


Figure 4. Editor's decryption scheme (receiver)

6. System Implementation

The second part of system is implemented as web based system using Eclipse, Oracle 11g and Apache Tomcat Server. In this system, media system is implemented where different journalists can encrypt images and send to editors. Then, each editor can view list of journalists, incoming cipher mails and can decrypt each cipher mail.



SECURED IMAGE ENCRYPTION MEDIA SYSTEM

Monday, 14 December 2015, 0:08 AM

U Kyaw Kyaw

Send to Editor

Please Type 20 alphanumeric characters (0-9 and A-F) correctly.

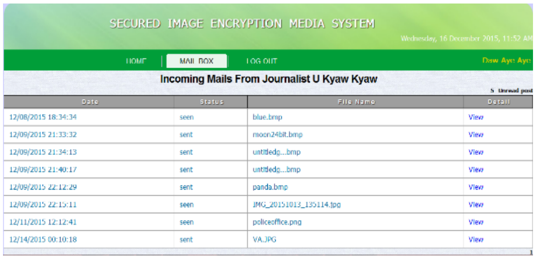
Secret Key: 09E6B1D430FF8C6D1A7A

Load Plain Image: Browse... VA.JPG

Designed and Developed by Wut Yee Pwint Hlaing , 20 th batch

Figure 5. Defining 80 bit external secret key and Loading plaing image from Journalist

In figure 5, journalist named ‘U Kyaw Kyaw’ defines 80 bit secret key and load plain image for the editor to send. When he clicks ‘Encrypt & Send’ button, plain image is encrypted with secret key. The resulting cipher image is stored in database .



SECURED IMAGE ENCRYPTION MEDIA SYSTEM

Wednesday, 16 December 2015, 11:52 AM

Daw Aye Aye

Incoming Mails From Journalist U Kyaw Kyaw

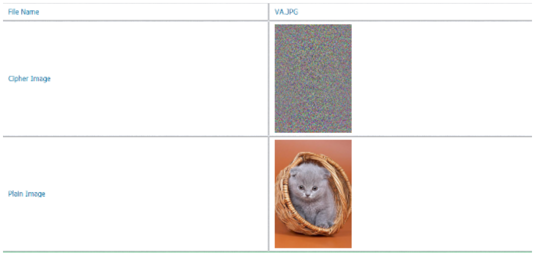
5 Unread post

Date	Status	File Name	Detail
12/08/2015 18:34:34	seen	blue.bmp	View
12/09/2015 21:33:32	sent	moon24bit.bmp	View
12/09/2015 21:34:13	sent	untitledg....bmp	View
12/09/2015 21:40:17	sent	untitledg....bmp	View
12/09/2015 22:12:29	sent	panda.bmp	View
12/09/2015 22:15:11	seen	IMG_20151013_135114.jpg	View
12/11/2015 12:12:41	seen	policeoffice.png	View
12/14/2015 00:10:18	sent	VA.JPG	View

1

Figure 6. Displaying incomming cipher image list to editor

In figure 6, after editor ‘Daw Aye Aye’ logging into the system, she can know which journalist has sent cipher images from mail. When she clicks **‘View’** on a mail, the system will ask to enter secret key.Then,cipher image will be extracted from database and decrypted with secret key to get the original image as shown in figure7.



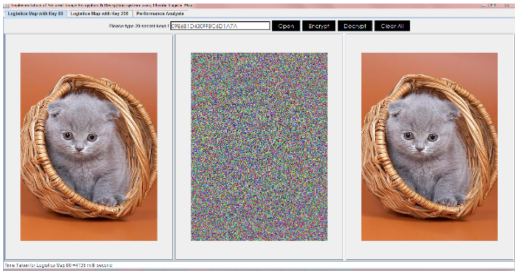
File Name	VA.JPG
Cipher Image	
Plain Image	

Figure 7. Cipher decryption from editor

7. Experimental Results

A good encryption procedure should be robust against all kinds of cryptanalytic and statistical. In this section, we discuss the security analysis of the proposed image encryption scheme such as key space analysis and statistical analysis etc. to prove that the proposed cryptosystem is secure against the most common attacks. Sample encryption process for 363×510 dimension with true color jpg image is shown in figure 8. This original image is encrypted and decrypted with 80 and 256 bit key respectively.

To prove the security of the algorithm, histogram analysis of plain image, 80 bit and 256 bit key algorithm on cipher image is described in figure 9, 10 and 11. The correlation coefficient between two horizontal adjacent cipher pixels and (NPCR) number of pixels of ciphered image while one pixel of the plain image is changed are analyzed in table 2 and 3. Performance is measured on a 1.60 GHz Intel (R) Core i5 with 4200U CPU of 4GB RAM running Windows 7 Ultimate.



Please type 20 secret keys : 09E6B1D430FF8C6D1A7A

Time Taken for Logistics Map 80 =4135 milli second

Figure 8. Image encryption with Chaotic Logistic Map with 80 bit

7.1. Key space analysis

For a secure image cryptosystem, the key space should be large enough to make the brute force attack infeasible. Chaotic Logistic Map with 80 bit key has 2^{80} different combinations of the secret key and Chaotic Logistic Map with 256 bit key has 2^{256} different combinations of the secret key. These ciphers with such a long key space are sufficient for reliable in practical use. In chaos system, a logistic map is employed which is sensitive on the initial condition and that initial condition for logistic map is calculated from the secret key.

7.2. Number of Pixels Changed Rate (NPCR)

NPCR means the change rate of the number of pixels of ciphered image while one pixel of the plain image is changed. Let two ciphered images, whose corresponding plain images have only one pixel difference, be denoted by C1 and C2. Label the grayscale values of the pixels at grid (i,j) in C1 and C2 by C1(i,j) and C2(i,j), respectively. Define a bipolar array D with the same size as images C1 and C2. D(i,j) is 0 if the gray values of the position C1(i,j) and C2(i,j) are different, otherwise, D(i,j) is 1.The NPCR is defined as

$$NPCR=\frac{\sum_{i,j} D(i,j)}{W\times H}\times 100$$

(11)

where W and H are the width and height of C1 or C2. Table 2 and 3 shows some results of the NPCR value of different images with Chaotic Logistic Map with 80 bit key and 256 bit key.

7.3. Histograms analysis

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. Histogram analysis of a sample plain image is given in figure 9. Its encrypted image with chaotic logistic map with 80 bit is shown in figure 10 and its encrypted image with chaotic logistic map with 256 bit is shown in figure 11.

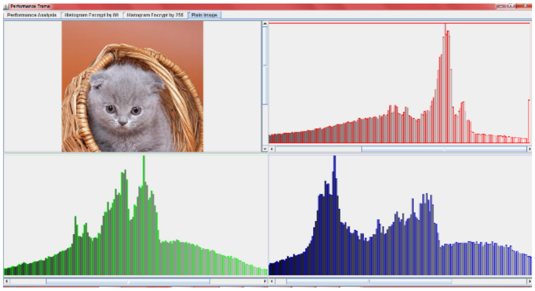


Figure 9. Histogram of original image

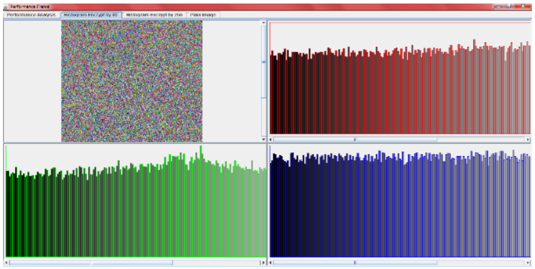


Figure 10. Histogram analysis of cipher image with Chaotic Logistic Map 80 bit

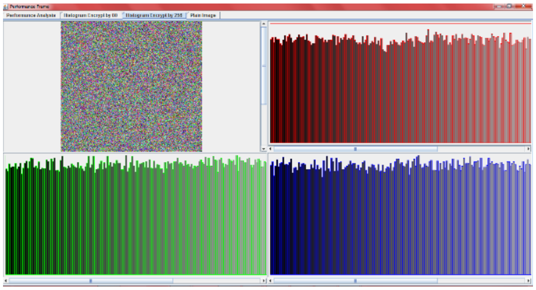


Figure 11. Histogram analysis of cipher image with Chaotic Logistic Map 256 bit

These figures 10 and 11 show that the histogram of the ciphered image is fairly uniform and are significantly different from that of the original image. Thus, they demonstrates that the encryption algorithms have covered up all the characters of the plain image and depend the statistics of the output on the statistics of the input.

7.4. Correlation Coefficient Analysis

In addition to the histogram analysis, we have also analyzed the correlation between two horizontal adjacent pixels in plain image and cipher image. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

Dimensions	Correlation Coefficient	NPCR
284 x 177	-0.0344	99.68%
760 x 506	-0.0158	99.91%
2000 x 1333	-0.0200	99.99%
1600 x 1200	-0.0381	99.94%
5000 x 200	0.0260	99.99%
7000 x 200	0.0123	99.99%
9000 x 200	0.0113	99.99%

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

(12)

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

(13)

where x and y are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i(14)$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2(15)$$

The two adjacent pixels in the plain image are highly correlated and approximately ‘1’. If the correlation coefficient is zero, it signifies that there is no linear relationship between the variables. When the value of correlation coefficient is close to zero, generally between -0.1 and +0.1, the variables are said to have no linear relationship or a very weak relationship. Among nearly 200 tested images, some of tested images with different dimensions are described by their NPCR and correlation coefficient distribution in cipher image for chaotic logistic map algorithms with 80 bit and 256 bit analysis in table 2 and 3.

Table 2. Statistical Analysis for Chaotic Logistic Map with 80 bit tested by secret key ‘09E6B1D430FF8C6D1A7A’

Table 3. Statistical Analysis for Chaotic Logistic Map with 256 bit tested by secret key ‘60CD207E3E5273ABC0172B3D6F307AAB9DEE8B5011AA66CC99FF2B6D96BEDC06’

Dimensions	Correlation Coefficient	NPCR

284 x 177	0.0272	99.75%
760 x 506	0.0052	99.99%
2000 x 1333	0.0533	99.99%
1600 x 1200	0.0068	99.98%
5000 x 200	-0.0390	99.99%
7000 x 200	-0.1433	99.99%
9000 x 200	-0.0516	99.99%

In table 2 and 3, NPCR values of both algorithms are over 99.50%. Therefore, both algorithms are dynamically sensitive and has good protection ability. Correlation coefficient analysis of Chaotic Logistic Map with 80 bit key are mostly negative correlated meanwhile most of 256 bit key are positive correlated. Thus, Chaotic Logistic Map with 80 bit key algorithm encrypt cipher images with inverse relation between adjacent pixels because of high key sensitivity. It means that modifying secret key makes statistical analysis difficult and using the changed key in next encryption process can provide more inverse correlation. The change of a single bit in the secret key produce a completely different encrypted images.

7.5. Performance Evaluation

The encryption and decryption rate for several colored images of different sized are measured by using the proposed image encryption scheme. The average encryption and decryption time taken by the algorithm for different sized images are shown in the table 4.

Table 4. Average ciphering speed of a few different sized color image

Image size (in pixels)	Bits/pixels	Average encryption/ decryption time (s)	
		80 bit	256 bit
284 x 177	24	0.3~0.4	0.002 ~ 0.08
518 x 354	8	0.8~0.9	0.09~0.08
1600x 1200	24	8.0~8.1	0.52~0.54
9000 x 200	24	8.11~8.12	0.59~0.61

According to table 4, average running time by Chaotic Logistic Map with 256 is faster than Chaotic Logistic Map with 80 bit. It is because in Chaotic Logistic Map with 80 bit key, that makes the cipher more robust against any attacks, the secret key is modified after encrypting an 8 bit pixels block of the image. Without doubt, this will bring great safety threats. In Chaotic Logistic Map with 80 bit encryption algorithm, a logistic map is used to transform the session keys, which assures the unpredictability of the session keys. This process occurs in each iteration until the whole image is encrypted and it will take some time depend on the number of pixels in image file.

8. Conclusion

In this paper, two image encryption algorithms which utilize different logistic maps and different key space are analyzed and studied comparatively. This system can encrypt any type of image file formats as well as gray and color images. Security is a critical issue when images are transferred from journalist to editor via communication channel. That critical issue can be solved by applying image encryption algorithm in this system. The both sides of system already agree a symmetric key. In this system, journalist sends cipher images to editor and editor encrypts ciphers with that symmetric secret key. Chaotic Logistic Map with 80 bit is implemented in this system because of its randomness and unpredictable behavior in long term that are secure and safe for image encryption.

To conclude the two algorithms, Chaotic Logistic Map with 256 bit algorithm makes heavy use of data dependent essentials. In Chaotic Logistic Map with 80 bit key algorithm, the key is mainly conducted to generate the initial conditions of a first logistic map. The second logistic map is used to transform the key after the encryption of every block data and there is data-dependent. To make cipher more robust, algorithm modifies session keys after each block of an 8 bit encryption. Any changes in the plain image are cascaded forward throughout the cipher image, which means that two almost identical plain images will encrypt to have completely different cipher images.

With comparative experiments above, Chaotic Logistic Map encryption algorithm with 80 bit has taken some time because of several modifying of secret key but it provides lower correlation coefficient distribution in cipher pixels than Chaotic Logistic Map encryption algorithm with 256 bit because of high key sensitivity, dynamic changes in secret key and using that secret key in next encrypting and decrypting processes. Therefore, Chaotic Logistic Map encryption algorithm with 80 bit is implemented and applied in Media system for secure image transmission. Improving the algorithm to be faster without degrading correlation is farther extension.

References

[1] M.S. Baptista, ”Cryptography with chaos”, Phys. Lett. A, vol.240, pp.50-54,1998.

[2] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, Shinsaku Mori “A secret key cryptography by iteration a chaotic map” IEICE E, 73(7):1041-1044, 1998.

[3] Jui-Cheng Yen and Jiun-In Guo “A new chaotic key-based design for image encryption and decryption” proceedings of the IEEE International SymposiumCircuits and Systems, vol. 4, 2000.

[4] Shiguo Lian , Jinsheng Sun, Zhiquan Wang , ”Security Analysis of A Chaos-based Image Encryption Algorithm”, Phisica A, Elsevier Science, 2005.

[5] Smet Öztürk1 and Brahim “Analysis and Comparison of Image Encryption Algorithms”, proceedings of world academy of science, engineering and technology volume 3 January 2005.

[6] N.K.Pareek, Vinod Patidar, K.K.Sud “Image encryption using chaotic logistic map”, Image and Vision Computing 2006.

[7] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah “An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption”, Informatica 2007.

[8] Nidhi Sethi “A New Image Encryption Method using Chirikov and Logistic Map”, International Journal of Computer Applications (0975 – 8887) Volume 59– No.3, December 2012.

[9] Nisha Kushwah, Madhu Sharma “Chaotic Map based Block Encryption”, International Journal of Computer Applications (0975 – 8887) Volume 71– No.16, June 2013.

[10] Prabir Kr. Naskar, Atal Chaudhuri “A Secure Symmetric Image Encryption Based on Bit-wise Operation”, I.J. Image, Graphics and Signal Processing, 2014.