Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher

Hossam Eldin H. Ahmed
Dept. Of Electronics Comm. Eng., P. Dean of the Faculty of Electronic Eng. Menouf-32952, Menufiya University, Egypt.

Ayman H. Abd El-aziem
Ph. D Student, Dept. Of Electrical Engineering, Shubra Faculty of Engineering, Benha University, Egypt. e

Abstract—Recently due to the development of computer technology many multimedia content as digital image need to be transmitted over network, digital image are used in several application as medical image, confidential video conferences and military image data base of this digital images need to be protect from unauthorized. We need to encrypt these contents of images when transmitted over unsecured network. This paper focuses on protecting digital images through using developed chaos-based encryption/decryption algorithms. We propose an image encryption based on development of chaotic logistic map and on feedback stream cipher. The proposed algorithm uses a developed chaotic logistic map and an external secret key of 256-bit. Furthermore, the proposed algorithm obtain solution by iteration, data dependent inputs, inclusion of three feedback mechanisms are verified to provide high security level. Our proposed algorithm has advantages, 1-Extend the range of the variable r by developed the chaotic logistic map. 2-New features for our proposed algorithm such as inputs(key, image). 3-The combine of feedback property with external secret key make cipherimage not depend on key only but depend on key and previous cipherimage pixel, this give the algorithm robustness against any cryptanalysis. 4-The experimental result of our proposed algorithm proof that it is an efficient method and secures way for real time image encryption. Furthermore a simple implementation of our algorithm achieves high encryption rates on general-purpose computers.

Keywords—Image encryption, stream cipher, development of logistic map, information security.

I. INTRODUCTION

In recent years, owing to frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakage that require reliable, fast, and robust security system to store and transmit digital images. The requirements to fulfil the security needs of digital images have led to the development of good encryption techniques. During the last decade, numerous encryption algorithms [1-2-10-11] have been proposed in the literature based on different principles. Among them, chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power.

In this paper we propose a new approach for image encryption based on feedback steam cipher by using a developed chaotic logistic map it consist of two modules, first the encryption module which encrypt the image pixel-by-pixel, by using external secret key 256-bit are consider in each iteration, the values of the previously encrypted pixels, the second module is decryption module which decrypt the cipherimage pixel by pixel to retrieve the original image using the same key.

The feedback property, combined with the external secret key of 256-bit are verified to provide high security level, also, makes our proposed stream cipher robust against cryptanalytic attacks. The results of security analysis show that the proposed model provides an efficient and secure way for real-time image encryption and transmission. Our proposed chaotic logistic map with generated session key is compared with some different map as Bernoulli map, Genhous map, tent map and logistic map 1. Compare between them in several experimental, statistical analysis and key sensitivity tests. Also our proposed chaotic algorithm is compared with the RC5 , RC6 algorithms.

The rest of this paper contains different chaotic map and its analysis in Section 2 ,the proposed algorithm which is consist of two modules are mention in section 3, Section 4 test and verify of algorithm by applied algorithm using different map and verification for encryption and decryption. Section 5 the security analysis, the Section 6 comparing between proposed algorithm and RC5, RC6 and summery of paper is in Section 7.

II. DIFFERENT CHAOTIC MAP AND ITS ANALYSIS

We introduce some different chaotic maps and analysis the results simulation of these maps.

A. Bernoulli Map

Bernoulli map is chaos function and we use it in cryptography application. Its function is expressed as:

$$X_{n+1} = r \times X_n \bmod 1 \quad (1)$$

Where

- X_n takes values from interval 0, 1, $r \in [0, 1]$.
- r is a variable and takes values from 0 to ∞ , $r \in [0, \infty]$.
- Initial value $X_n = 0.1$.
- Loop iteration = 8000 for r incremented by 0.001.

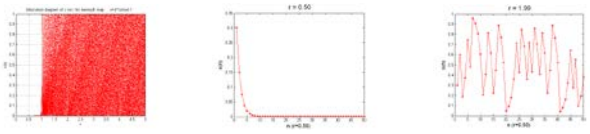
ISBN: 978-1-61804-262-0

The simulation result is shown in figure 1 the parameter r can be divided into two segments which can be experiments on the following condition,

1. When r ϵ [0, 1] as shown in figure 1.b the calculation result come to the same result after several iteration without chaotic behavior.
2. When r ϵ [1, ∞] it become a chaotic system without periodicity as shown in figure 1.c.

From the previous discussion we can conclude that:

- When r $\in$ [0, 1] the point concentrate on several values could not use in image cryptosystem.
- When r $\in$ [1, 4.99] Bernoulli map have small change in the range of r to exhibit chaos behavior and hence the property of sensitive dependence so it can use for image cryptosystem in this small range.
- We obligezed that not use integer value of r when use Bernoulli map in image cryptosystem, it must use a fraction value for r and this is one of its disadvantage.



a) Bifurcation for r ϵ [0,4.99], X_0 = 0.1 b) Iteration property when r = 0.50 c) Iteration property when r = 1.99

Fig 1: Analysis of Bernoulli Map

B. *Genhous map*

Genhous map is chaos function and we use it in our cryptography applications. Its function is chaos generator with a recursive structure expressed as,

$$X_n = f(r_1 \times X_{n-1} + r_2 \times X_{n-2} + r_3 \times X_{n-3}) \quad (2)$$

And

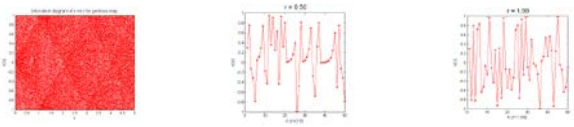
$$f(X_n) = X - 2 \text{ floor } ((X+1)/2) \quad (3)$$

Where

- r_1 arbitrary, $r_2 = r_3 = 1$.
- X_n take values from interval 0, 1, $X_n \epsilon [0,1]$.
- r_1 is variable and takes value from 0 to ∞ $r_1 \epsilon [0, \infty]$.
- Initial value X_1 = 0.1.
- Loop iteration=6000 for r incremented by 0.001.
- Floor is function takes the integer part of number as floor (5.5) = 5.

The simulation are shown in figure 2, for different values of parameter r it become a chaotic system without periodicity except in integer value of r as shown in figure 2.b,c. Also we use MATLAB software to graph the bifurcation diagram of Genhous map as show in Figure 2.a, for r ϵ [0,4.99] from the simulation result the chaotic behaviour occurs as shown in From the previous discussion we can conclude that:

- when r ϵ [0,499] Genhous map exhibit chaos behavior for integer r and hence the property of sensitive dependence .It can used for image cryptosystem with disadvantage of r must be fraction and have small range , so we recommend that not use integer value of r when use Genhous map in image cryptosystem.



a) Bifurcation for r ϵ [0.499], x_0 = 0.1 b) Iteration property when r = 0.50 c) Iteration property when r = 1.99

Fig 2 Analysis of Genhous Map

C. *Tent Map*

Tent map is a chaos function can be used it in cryptography application. It expressed as:

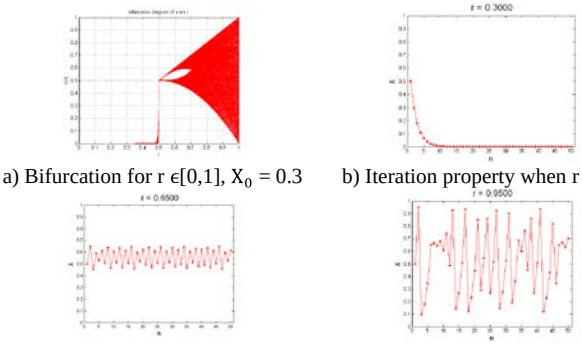
$$X = r \times (1 - |1 - 2 \times X|) \quad (4)$$

Appling under the following conditions:

- X_n take value from interval 0, 1 $X_n \epsilon [0,1]$
- r is variable, r ϵ [0,4].
- Initial value X_n = 0.3.
- Loop iteration = 6500 for r incremented by 0.001.

The simulation are shown in figure 3, the parameter r can divided into three segment which can be experiments on the following condition.

1. When r ϵ[0, 0.5] as shown in figure 3.b the calculation result come to the same result after several iteration without any chaotic behavior.
2. When r ϵ [0.5, 0.7] as shown in figure 3.c the phase space concludes several point the Systems appear as periodic behavior.
3. When r ϵ [0.7, 1] it become a chaotic system without periodicity as shown in figure 3.d.



a) Bifurcation for r ϵ[0,1], X_0 = 0.3 b) Iteration property when r = 1.6

c) Iteration property when r = 0.65 d) Iteration property when r = 0.95

Fig 3. Analysis of tent map

Also we use MATLAB software to graph the bifurcation diagram of tent map as show in figure 3.a

From the previous discussion we can conclude that,

- When r ϵ [0, 0.7] values could not use in image cryptosystem.

ISBN: 978-1-61804-262-0

- When r ϵ [0.7, 1] Tent map exhibit chaos behavior and hence the property of sensitive dependence so it can used for image cryptosystem for r ϵ [0.7,1], but this range of applied r is very small and not enough for a secure cryptosystem

D. Logistic Chaotic Map 1

Logistic map is developed to give a chaos function can be used it in cryptography application. This logistic map 1 is expressed as:

$$X_{n+1} = r^2 \times X_n \times (1-X_n) \times (1-2 \times X_n) \quad (5)$$

Appling under the following conditions:

- X_n take value from interval 0, 1 , $X_n \epsilon [0,1]$.
- r is variable, r ϵ [0,4]
- Initial value X_0 = 0.3.
- Loop iteration = 9000 for r incremented by 0.001.

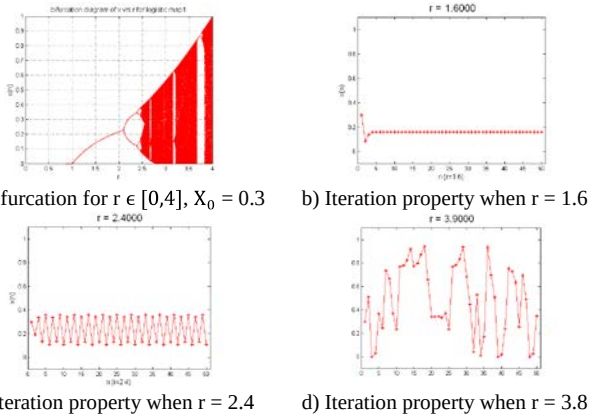
The simulation are shown in figure 4, the parameter r can divided into three segment which can be experiments on the following condition.

- When r ϵ [0.2, 1] as shown in figure 4.b the calculation result come to the same result after several iteration without any chaotic behavior.
- When r ϵ [2.1, 2.47] as shown in figure 4.c the phase space concludes several points the Systems appear as periodic behavior.
- When r ϵ [2.47, 4] it become a chaotic system without periodicity as shown in figure 4.d.

Also we use MATLAB software to graph the bifurcation diagram of logistic chaotic map1 as show in figure 3.a

From the previous discussion we can conclude that:

- When r ϵ [2.47, 4] values could not use in image cryptosystem.
- When r ϵ [2.47, 4] logistic map1 exhibit chaos behavior and hence the property of sensitive dependence so it can used for image cryptosystem for r ϵ [2.47, 4] but this range of applied r is small and not enough for a secure cryptosystem .



a) Bifurcation for r ϵ [0,4], X_0 = 0.3 b) Iteration property when r = 1.6

c) Iteration property when r = 2.4 d) Iteration property when r = 3.8

Fig 4: Analysis of logistic chaotic map1

E. Our Proposed Logistic Chaotic Map 2

A proposed logistic map 2 which is a chaos function also but we can be used it in cryptography applications under certain conditions. This logistic map function is express as:

$$X_n = r \times X_{n-1} \times (1-X_{n-1}) \quad (6)$$

And

$$X_{n+1} = 4 \times X_n \times (1-X_n) \quad (7)$$

We substitute from equation (6) into equation (7) and Appling under the following conditions,

- X_n take value from interval 0, 1, $X_n \epsilon [0,1]$
- r is variable, r ϵ [0, 4].
- Initial value X_1 = 0.3.
- Loop iteration = 6000 for r incremented by 0.001.

We use Matlab software to simulate our logistic map applied to images. We start our program by the initial value , X_1 = 0.3 the simulation are shown in figure 4, Where the parameter r can divided into three segment which can be resume to these three following condition:

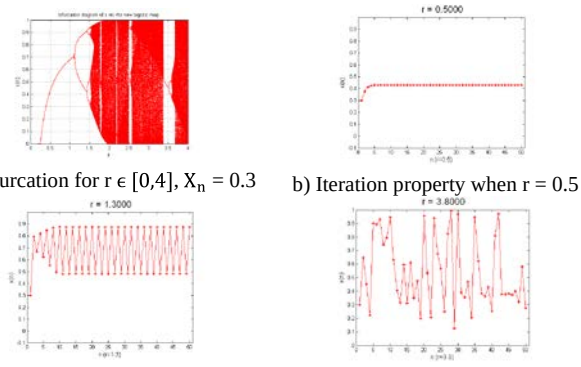
1. When r ϵ [0, 1.1] as shown in figure 5.b, the calculations results come to the same results after several iteration without any chaotic behavior.
2. When r ϵ [0, 1.5] as shown in figure 5.c, the phase space concludes several points the system appear as periodic behavior.
3. When r ϵ [1.5, 4] it become a chaotic system without periodicity as shown in figure 5.d.

Also we use MATLAB software to graph the bifurcation diagram of logistic map 2 as show in figure 4.a and we can conclude that:

1. The case of r ϵ [0, 1.] from the simulation result the trajectory of equation convergence to fixed point as illustrate in figure 5.a.
2. The case of r ϵ [1.1, 1.5] from the simulation result the phenomena of period double bifurcation as shown in figure 5.a.
3. The case of r ϵ [1.5, 4] from the simulation result a chaotic behavior as shown in figure 5.a.

We refer to these three regions as convergences, bifurcations, and have chaos behavior respectively from the previous discussion one can conclude that,

1. For r ϵ [0, 1.5] the point concentrate on several values could not use in image cryptosystem.
2. For r ϵ [1.5, 4] the logistic chaotic map2 exhibit chaos behaviour and hence the property of sensitive dependence so it can be use for image cryptosystem.



a) Bifurcation for r ϵ [0,4], X_n = 0.3 b) Iteration property when r = 0.5

c) Iteration property when r = 1.3 d) Iteration property when r = 3.8

Fig 5. Analysis of our proposed logistic chaotic map 2

F. Another Proposed Logistic Chaotic Map 3

We introduce another developed logistic chaotic map 3 where the range of r increased chaotic area for all applications of as will as shown below.

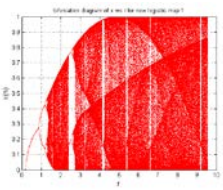
$$X_{n+1} = r\times X_n\times (1-X_n)\times(1-1.2\times X_n)^2 \qquad (8)$$

And substitute from equation (8) into equation (7) Appling these under the following conditions,

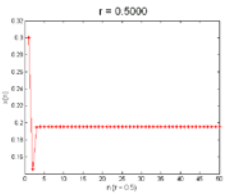
- X_n take value from interval 0,1 r ϵ[0, 1].
- The variable r takes value from 0, to 9.5 r ϵ [0,9.5].
- Initial value $X_1 = 0.3$.
- Loop iteration =8000 for r incremented by 0.001.

By using Matlab software to simulate bifurcation and iteration results where the initial value X_1 =0.3. These simulations are given in figure 6 where the parameter r divided into three segments given as follow:

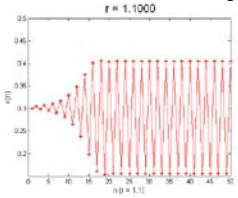
- When r ϵ [0,1.1] as shown in figure 6.b, the calculation result come to the same result after several iteration without any chaotic behavior.
- When r ϵ [1.1, 1.5] as shown in figure 6.c, the phase space concludes several point where the system appear as periodic behavior.
- When r ϵ [1.1,9.5] it become a chaotic system without periodicity as shown in figure 6.d.



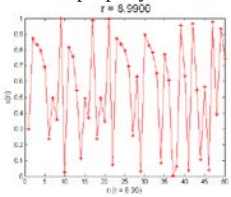
a) Bifurcation for r ϵ [0,9.5], X_1= 0.3



b) Iteration property when r = 0.5



c) Iteration property when r = 1.1



d) Iteration property when r = 8.99

Fig 6. Analysis of our proposed logistic chaotic map 3

- The case of r ϵ [0,1.1] from the simulation result the trajectory of equation convergent to fixed point as illustrate in figure 6.a.
- The case of r ϵ[0, 1.3] from the simulation result, the phenomena of this period is double bifurcation, as shown in figure 6.a.
- The case of r r ϵ [1.3, 9.5] from the simulation result the chaotic behavior occurs as shown in figure 6.a.

We can refer to these three regions as convergences, bifurcations and exhibit chaos behavior respectively. From the above discussion we can conclude that.

- When r ϵ [0, 1.3] the point concentrate on several values could not use in image cryptosystem.
- For r ϵ [1.3, 9.5] which is a long range for r, the proposed new logistic map1 exhibit chaos behaviour and hence the property of sensitive dependence, so as an advantage to use it for a wide range r image cryptosystem analyses and applications.

From the above discussion we can conclude that, these three proposed logistic chaotic maps can be used for different forms of logistic maps and for wide range of r that give a good chaotic behaviour and can be applied in our proposed algorithm.

III THE PROPOSED ALGORITHM

We propose a new approach for image encryption based on developed of chaotic logistic maps in order to meet the requirements of the secure image transfer, we propose algorithm based on feedback steam cipher by using a developed chaotic logistic map it consist of two modules, first the encryption module, the second module is decryption module.

A. The Encryption Module

The proposed is a simple block cipher with block size of 8-bit and 256-bit secret key. The key is used to generate a pad that is then merged with the plaintext a byte at a time, as shown in figure 6**.**

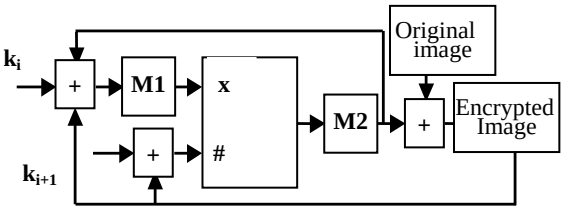


Fig 6: Diagram of Encryption Module

We can obtain the cipherimage from the following steps:

1. For the encryption/decryption, we divide plainimage/cipherimage into blocks of 8-bits (pixel). Plainimage and cipherimage of i blocks can be presented as:

$$P = P_1P_2P_3P_4P_5\ldots\ldots\ldots\ldots P_i \qquad (9)$$

$$C = C_1C_2C_3C_4C_5\ldots\ldots\ldots\ldots P_i \qquad (10)$$

2. The proposed image encryption process utilizes an external secret key of 256-bit long. Further, the secret key is divided into blocks of 8-bit each block referred as session keys the secret key can be represented in ASCII mode as,

$$K = K_1K_2K_3K_4K_5\ldots\ldots\ldots\ldots K_i \qquad (10)$$

Where, each K_i represents one 8-bit block of the secret key i.e. session key.

3. The initial condition (X_0) for the chaotic map and the initial code C_0 are generated from the session keys as:

ISBN: 978-1-61804-262-0

$$R = \sum_{i=1}^{32} M1[K_i] \quad (11)$$

$$X_0 = R - \lfloor R \rfloor \quad (12)$$

$$C_0 = [\sum_{i=1}^{32} [K_i]] \bmod 256 \quad (13)$$

Where K_i, $\lfloor \ \rfloor$, and M1 are, respectively, the decimal equivalent of the ith session key, the floor function (result the integer part of number), and mapping from the session, key space, all integers between 0 and 255, into the domain of the logistic map, all real numbers in the interval [0,1].

4. Read a byte from the image files (that represent a block of 8-bits) and load it as plainimage pixel P_i.
5. Encryption of each plainimage pixel P_i to produce its corresponding cipherimage pixel C_i can be expressed mathematically as:

$$C_i = \left(P_i + M2 \left[\sum_{i=1}^{\#_i} chaoticmap \right] \right) \bmod 256 \quad (14)$$

Where chaotic map is one of map which we mention in Section 2 the output of each cipherimage pixel is feedback to input for chaotic map to calculate the input of chaotic map and the iteration of chaotic map. Where represents the current input for logistic map and computed as:

$$X_i = M1[k_i + C_{i-1} + X_{i-1}] \quad (14)$$

$$\#_i = k_{i+1} + C_{i-1} \quad (15)$$

Where $\#_i$ is the number of iteration of chaotic map for its current input X_i and calculated as:

And M2 maps the domain of the chaotic map [0,1] back into the interval [0,255].

6. Repeat steps 4-5 until the entire image file is exhausted.

We have three feedback in our module first the output of cipherimage pixel to the input of chaotic map input second to the number of iteration third the output of chaotic map is input to input of chaotic map this three feedback make the cipherimage pixels not depend on key only but on the previous cipherimage pixel and the number of iteration depend on next session key and previous cipherimage pixel, we applied this module by using the different chaotic map which is mention in section 2 and using the optimum value which in listed in table 1 to generate the pad which is merged with plain image pixel to produce cipherimage.

We introduce the development of chaotic logistic map to extend the range of variable r which gives chaotic properties for logistic map it is from 3.57 to 4 [7, 8], after we develop it becomes

- for logistic map 2 it become from 1.5 to 4
- And for logistic map 3 it become from 1.3 to 9.55.

We use one of chaotic map which mention in section 2 to generate session key which is a pad which is merged to plainimage to generate cipherimage we add the decimal value of K_i to value of the output of pervious chaotic map X_{i-1} to the value of pervious Ciphertext C_{i-1} and mapping this value to chaotic map domain to produce X_i which is input to new logistic map and use number of iteration equal the value of next session key to the previous cipherimage pixel And map the output of this chaotic map to interval [0,255].to generate a pad which is merged with plaintext byte to produce Ciphertext byte we repeat that until we finish the image file.

TABLE I THE RANGE OF R FOR DIFFERENT CHAOTIC MAP

Chaotic map	Range for chaotic	Optimum Value of r
Bernoulli map	1 : ∞	1.99
Genhous map	0 : ∞	1.99
Logistic map 1	2.5 : 4	3.6
Logistic map 2	1.5 : 4	3.8
Logistic map 3	1.3 : 9.5	8.99

B. The Decryption Module

Decryption is very simple it is similar to encryption module except in this case the same pad is generated but this time un-merged with the cipherimage to retrieve the plainimage**,** the decryption module receives an encrypted image (cipherimage) and the 256-bit secret key and returns the original image (plainimage).

$$P_i = \left(C_i - M2 \left[\sum_{i=1}^{\#_i} chaotic\ map \right] \right) \bmod 256 \quad (16)$$

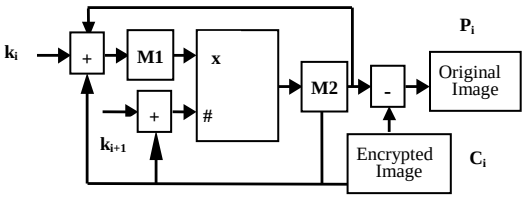


Fig 7 Diagram of decryption Module

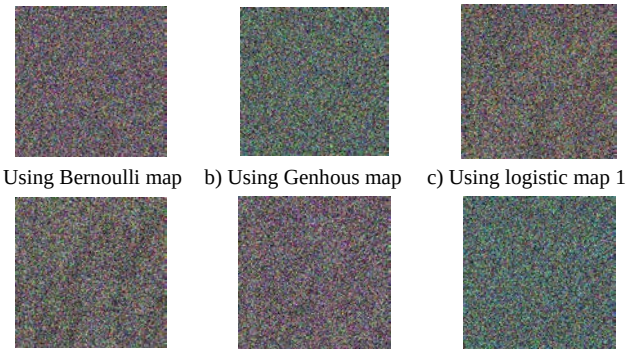
The proposed algorithm by using development logistic map it appear to sensitive to any change because each cipherimage depend on session key and previous cipherimage pixel so that any change in plainimage makes great change in cipherimage And it is data dependent iteration because the input of chaotic map map are computed as function of session key and previous computed cipher pixel and previous new logistic output.

IV TEST, VERIFICATION AND EFFICTIONCY OF OUR PROPOSED ALGORITHM

We apply our proposed algorithm by using different chaotic map to image Lena, which size 256 x 256 Gray-scale (0-255) as original image (plainimage) and use secret key (k1="12345789012345678901234567890l2") (in ASCII) is

used for encryption whose long is 256-bit. As shown in Fig 9 Application of proposed algorithm using different chaotic map and RC6 algorithm to original image Lena , it is clear that the results encrypted images (cipherimages) regions are totally invisible by applied our algorithm using different chaotic map and by applied RC6 algorithm, the decryption method takes (cipherimage) as input together with the same secret key (k1="12345789012345678901234567890l2") (in ASCII) and return the plainimage, One of the important examining of encrypted image is the visual inspection, where the more hidden features of the image are, the better the encryption algorithm. But it is not suffusion to determine the quality of our proposed algorithm by visual inspection so that we evaluate different testes to determine the efficiency of our proposed algorithm.

a)Original image



a) Using Bernoulli map b) Using Genhous map c) Using logistic map 1

d) Using logistic map 2 e) Using logistic map 3 f) Using RC6

Fig 9.Application of proposed algorithm using different chaotic map and RC6 algorithm to image Lena

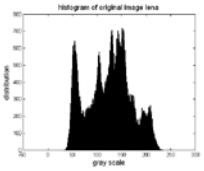
V SECUTITY ANALYSES

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. In this section, we discuss the security analysis of the proposed image encryption scheme such as statistical analysis, sensitivity analysis with respect to the key and plaintext and key space analysis. To prove that this proposed cryptosystem is secure against the most common attacks [3, 4].

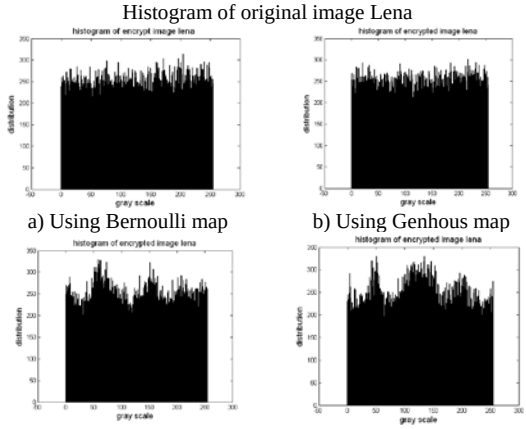
A. Statistical Analysis

It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. To prove the robustness of the proposed image encryption procedure by using different chaotic map, we have performed statistical analysis by calculating the histograms, the correlations between two adjacent pixels in the original images and its corresponding encrypted images.

1) Histogram Analysis: An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted image that the histograms of the encrypted image are fairly uniform and significantly different from the histogram of original image we analyze and calculate the histogram of original images and its cipherimages, by using different chaotic map. We find that as shown in fig 10 the histogram of plainimage and cipherimage by applied our algorithm using different chaotic map are fairly uniform and significantly different from the histogram of original and using it bears no statistical resemblance to the plainimage, so that it is appear no statistical attack against our proposed by using different chaotic map. Also histogram of applied RC6 algorithm give good result its histogram is fairly uniform and different from the histogram of original image.



Histogram of original image Lena



a) Using Bernoulli map b) Using Genhous map

c)Using logistic map 1 d) Using logistic map 2

e)Using logistic map 3 f) Using RC6 algorithm

Fig 10. Histogram of cipherimage by using different chaotic map in our proposed algorithm and RC6 algorithm

2) Correlation Coefficient Analysis: We analyzed correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plainimage/cipherimage respectively, by select 1000 pairs randomly of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas

$$\mathrm{cov}(x, y) = E(x - E(x))(y - E(y)) \qquad (17)$$

ISBN: 978-1-61804-262-0

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (18)$$

Where x and y are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used, Fig 11 shows the correlation distribution of two horizontally adjacent pixels in plainimage/cipherimage for our proposed using logistic map 3 chaotic map and. The correlation coefficients are and respectively for both plainimage/cipherimage.

It is clear that there is no correlation between two adjacent pixels in cipherimage and there are high correlated between adjacent in plainimage.

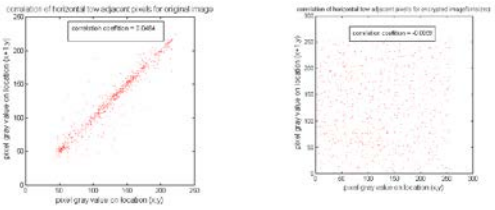


Fig 11. Two horizontally adjacent pixels Correlation in plainimage/cipherimage Using chaotic logistic map 3

In the next table we list the correlation coefficients of two horizontally, vertical and diagonal adjacent pixels in plainimage/cipherimage for our proposed in different chaotic map and RC6 algorithm in plainimage and cipherimage.

TABLE II CORRELATION COEFFICIENTS IN PLAINIMAGE/CIPHERIMAGE FOR OUR PROPOSED ALGORITHM USING DIFFERENT CHAOTIC MAP AND RC6 ALGORITHM

Chaotic map	Direction of Adjacent pixels	Plainimage	Cipherimage
Bernoulli map	Horizontal	0.9575	0.0177
	Vertical	0.9353	0.0
	Diagonal	0.9155	0.0
Genhous	Horizontal	0.9686	0.0586
	Vertical	0.9363	0.0330
	Diagonal	0.9191	0.0
Logistic map 1	Horizontal	0.0169	0.0160
	Vertical	0.9216	0.0036
	Diagonal	0.9129	0.0148
logistic map2	Horizontal	0.0721	0.0
	Vertical	0.9294	0.0
	Diagonal	0.8894	0.0307
logistic map 3	Horizontal	0.0484	0.0
	Vertical	0.9307	0.0
	Diagonal	0.9166	0.0153
RC6	Horizontal	0.0091	0.0571
	Vertical	0.9296	0.0161
	Diagonal	0.9071	0.0405

in previous table we calculate C.C between to adjacent pixel in horizontal , vertical and diagonal. For our proposed algorithm using different chaotic map and RC6 we find that:

- Our proposed algorithm using logistic map 3 have the smallest correlation coefficient compared to other algorithm , also our proposed algorithm using Bernoulli map has small C.C , the rest algorithm has small C.C but his values greater than the proposed algorithm using logistic map 3 and Bernoulli map.
- There is negligible correlation between the two adjacent pixels in the encrypted image in all directions. However, the two adjacent pixels in the original image are highly correlated that for our proposed algorithm and RC6.

B Sensitivity Analysis

An ideal image encryption procedure should be sensitive to any small change in plainimage and secret key.

1)Key Sensitivity Analysis: An ideal image encryption procedure should be sensitive with respect to the secret key i.e. the change of a single bit in the secret key should produce a completely different encrypted image. For testing the key sensitivity of the proposed image encryption by using chaotic logistic map 3, we have performed the following steps:

- As shown in fig 12.a is original image, b) is in encrypted image by using the secret Key(k1='12345678901234567890123456789012' (in ASCII).
- the same original image is encrypted by making the slight modification in the secret key to become (k2=12345678901234567890123456789013) the least significant bit is changed in the secret key) as shown in fig 13.c.
- Again, the same original image is encrypted by making the slight modification in the secret key to become (k3=11345678901234567890123456789012) the most significant bit is changed in the secret key) and the resultant image referred as encrypted image in Fig. 13.d.
- Finally, the three encrypted images A, B and C are compared.

We have shown the original image as well as the three encrypted images produced it is not easy to compare the encrypted images by simply observing these images. So that to compare between three images, we have calculated the correlation between the corresponding pixels of the three encrypted images. For this calculation, we have used the same Formula as given in Equation (17). Except that in this case x and y are the values of corresponding pixels in the two encrypted images to be compared. In table III, we have given the results of the correlation coefficients between the corresponding pixels of the three encrypted images A, B and C. It is clear from the table 3 that no correlation exists among three encrypted images even though these have been produced by using slightly different secret keys.

ISBN: 978-1-61804-262-0

TABLE III CORRELATION COEFFICIENTS BETWEEN THE CORRESPONDING PIXELS OF THE THREE DIFFERENT ENCRYPTED IMAGES OBTAINED BY USING SLIGHTLY DIFFERENT SECRET KEY

Image 1	Image 2	Correlation coefficient
Encrypted image A	Encrypted image B	0.0
Encrypted image B	Encrypted image C	0.0186
Encrypted image C	Encrypted image A	0.0211

We have also measured the number of pixels change rate (NPCR) to see the influence of changing a single pixel in the original image on the encrypted image by the proposed algorithm. The NPCR measure the percentage of different pixel numbers between the two images. We take two encrypted images, C1 and C2, whose corresponding original images have only one-pixel difference. We define a two-dimensional array D, having the same size as the image C1/C2. The D(i,j) is determined from C1(i,j) and C2(i,j). If C1(i,j) = C2(i,j) then D(i,j) =1 otherwise D(i,j) = 0. The NPCR is defined by the following equation.

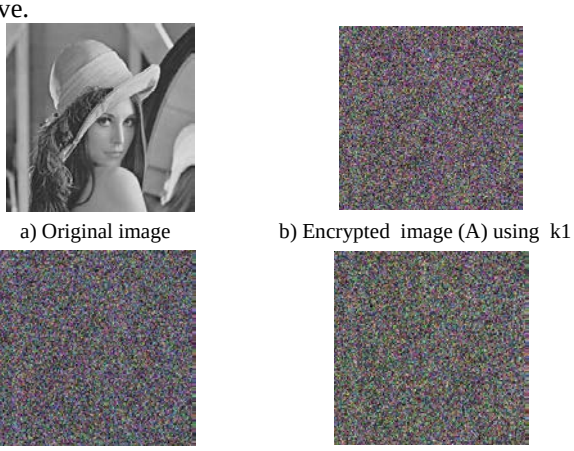
$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (18)$$

Where w and h are the width and height of encrypted image. We obtained NPCR for a large number of images by using our encryption scheme and found it to be over 99% as listed in table .4 so that the encryption scheme is very sensitive with respect to small changes in key secret.

TABLE IV. NPCR FOR THREE DIFFERENT ENCRYPTED IMAGES IN FIG. 13

Image 1	Image 2	NPCR
Encrypted image A	Encrypted image B	% 99.4812
Encrypted image B	Encrypted image C	% 99.5041
Encrypted image C	Encrypted image A	% 99.4522

Moreover, in Fig. 13, we have shown the results of some attempts to decrypt an encrypted image with
slightly different secret keys than the one used for the encryption of the original image, in fig 13.a is the original image and b) is the encrypted image produced using the secret key '12345678901234567890123456789012' in (ASCII), (c) the decrypted image with the secret keys '12345678901234567890123456789012' (in ASCII) and decrypted image with the secret keys '12345678901234567890123456789011' respectively, the images after the decryption of It is clear that the decryption with a slightly different key fails completely and hence the proposed image encryption procedure is highly key sensitive. High key sensitivity is required by secure image cryptosystems, which means that the cipherimage cannot be decrypted correctly although there is only a slight difference between encryption and decryption keys. It is clear that the decryption with a slightly different key fails completely and hence the proposed image encryption procedure is highly key sensitive.



a) Original image b) Encrypted image (A) using k1
c) Encrypted image (B) using k2 d) Encrypted image (C) using k3

Fig 12: key sensitive result with proposed using chaotic logistic map 3

a) Original image b) Encrypted image (A) using k1
b)Decrypted image using k1 b) Decrypted image using k2

Fig 13:key sensitive result with by using chaotic logistic map 3

2) Plainimage Sensitivity Analysis: We have also measured the number of pixels change rate (NPCR) to see the influence of changing a single pixel in the original image on the encrypted image. The NPCR measure the percentage of different pixel numbers between the two images. We take two encrypted images, C1 and C2, whose corresponding original images have only one-pixel difference. We define a two-dimensional array D, having the same size as the image C1/C2. The D (i,j) is determined from C1(i,j) and C2(i,j). If C1(i,j)=C2(i,j) then D(i,j)=1 otherwise D(i,j)=0.

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \qquad (18)$$

The UACI is defined as the measures of the average intensity of differences between the two images. One performed test is on the one-pixel change influence on a 256 grey-level Lena image of size 256 x 256.

ISBN: 978-1-61804-262-0

TABLE V. NPCR AND UACI FOR PROPOSED ALGORITHM USING DIFFERENT CHAOTIC MAP AND RC6 ALGORITHM.

Chaotic map / RC6	NPCR		UACI	
	Lena	Eivel	Lena	Eivel
Bernoulli map	% 99.21	% 99.59	84.90	85.65
Genhous map	% 99.23	% 99.62	85.42	86.14
Logistic map 1	% 98.87	% 99.27	83.90	84.32
logistic map 2	% 99.33	% 99.39	82.00	83.28
logistic map 3	% 99.08	% 99.05	82.05	84.16
RC6	% 99.24	%99.60	84.82	85.06

From table 5 we find that the proposed algorithm is sensitive to small change in plainimage show that the proposed algorithm is very sensitive with respect plainimage (plainimage have only one pixel difference).

C Key space analysis

Key space should be long enough to make brute force infeasible we use key length 256 -bit so that we have 2^{256} different key. Additionally the number of iterations supported by the logistic map module is between 0 and 767, as cipher pixels take values in the interval [0,512] and the session keys take values in the interval [0,255].

C. speed analysis

Apart from the security consideration is measure running speed for real-time image encryption/decryption. By measure the time required to encrypted/decrypted image we applied our proposed algorithm using development chaotic logistic map 3 to image in dimension 256 ×256 by using the simulator compiler Borland C++ Development Suite 5.0. Performance was measured on a 2.16 GHz Core 2 Duo with 1 GB of RAM running Windows XP. to improve the accuracy of our timing measurements, was executed 10 times, and we take the average, the time for encryption = 0.335 sec, the time for decryption = 0.4106 sec so that our proposed algorithm success in real time application.

VI COMPARISION BETWEEN OUR PROPOSED ALGORITHM AND RC5, RC6 ALGORITHMS

We compare between our proposed algorithm and RC5 and RC6 in optimum parameter[7,9] by measuring two encryption evaluation metrics to determine the quality of encryption, first we calculate the histogram deviation (DIV-1) Measures the deviation between the original and the encrypted image[5], the higher value of D_H is the better quality of the encrypted image second we measures the irregular deviation it Measures how much the deviation caused by encryption on the encrypted image (is irregular)[5].The lower value of D_I (DIV-2) is the better encryption quality.

BY Analyzing the results of the images in the table 6 which measure the (DIV-1) and (DIV-2) we can conclude the following:

- For lena.bmp image, the greater value of
  - (DIV-1) are at our proposed algorithm which mean that the proposed algorithm has high maximum deviation rather than the other algorithms and the smallest value of (DIV -2) at RC6 in CFB mode which mean the best irregular deviation at this algorithm.
  - For evel.bmp image the greater value of (DIV-1) is at RC5 in ECB mode which has high maximum deviation rather than the other algorithms, (DIV -2) have small value at RC6 in CBC mode which mean the best irregular deviation at this algorithm.
  - For camera man.bmp image the greater value of (DIV-1) are at proposed algorithm which mean that the proposed algorithm has high maximum deviation rather than the other algorithms and (DIV -2) small value at RC6 in CFB mode and RC5 in OFB mode which has equal value which mean the best irregular deviation at this two algorithms.

By analyzing the results of the images given by the table V which measure the encryption quality we have the following:

- The encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one [6].
- For lena.bmp image encryption quality has a good result with our proposed algorithm comparing with other ciphers and has a little good result in RC5 in OFB mode.
- For evel.bmp image encryption quality has a good result in RC5 for ECB mode than the other ciphers.
- For cameraman.bmp image encryption quality has a good result for our proposed algorithm than the other ciphers as RC6 CBC mode.

TABLE VI. THE MAXIMUM DEVIATION (DV-1) AND THE IRREGULAR DEVIATION (DV-2) FOR RC5, RC6 AND OUR PROPOSED ALGORITHM

		RC5				**RC6**				**Proposed**
		CBC	CFB	ECB	OFB	CBC	CFB	ECB	OFB	
Lena	DEV-1	46245	46561	46457	46006	46888	46746	46355	46138	**49005**
	DEV-2	46508	46356	46282	46230	46204	**46114**	46540	46264	50730
Eivel	DEV-1	71879	71611	**74262**	71637	71772	71529	71868	71696	71313
	DEV-2	36056	35834	39042	36146	**35794**	36080	37708	36124	41144
C_man	DEV-1	64322	64195	64144	64456	63931	63930	64414	64212	**72401**
	DEV-2	26788	26776	26778	26584	26868	**26584**	27048	26726	38122

ISBN: 978-1-61804-262-0

TABLE VII ENCRYPTION QUALITY MEASURES FOR RC6, RC5, AND PROPOSED ALGORITHM USING CHAOTIC LOGISTIC MAP 3

	RC5				**RC6**				**Proposed**
	CBC	CFB	ECB	OFB	CBC	CFB	ECB	OFB	
Lena	182.757	182.757	183.546	181.750	185.164	184.468	183.109	182.281	**193.578**
Eivel	283.554	282.406	**292.726**	282.677	283.101	282.054	283.359	282.796	281.460
C_man	252.421	251.750	251.542	252.843	250.664	250.726	252.710	251.929	**283.648**

From previous two comparisons table we can conclude that:
Our proposed algorithm is better than RC5 and RC6 when we use it at these cases

- Encrypted Lena .bmp and cameraman.bmp that from measuring encryption quality.
- Has very low C.C in cameraman encrypted.
- Has higher Maximum Deviation when use it in encrypt Lena and cameraman.

RC5 and RC6 are better than our proposed algorithm in these cases
Encrypted Eivel.bmp that from measuring encryption quality for RC5 in ECB mode

- Has very low C.C in Lena and cameraman encrypted.
- Has lower Irregular Deviation when use it in encrypt Lena, eivel and cameraman.

VI CONCOLUTION

In this paper, a new way of image encryption scheme using development of chaotic logistic map based on feedback stream cipher using an external secret key of 256-bit.

We use a developed logistic map to increase the range of the variable r which change from 3.57 to 4 in logistic map [8] to a wide chaotic range from 1.3 to 9.55 for logistic map 3.

Several test images are used for inspecting the validity of the proposed algorithm. The robustness of the proposed algorithm based on a feedback mechanism, which leads the cipher to a cyclic behaviour so that the encryption of each plain pixel depend on the output of the used chaotic map and the previous cipher pixel.

We have carried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security of the new image encryption procedure. According to the results of our security analysis, we conclude that the proposed algorithm is expected to be useful for real-time image encryption and transmission application.

REFERANCES

[1] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, Chaos Solitons Fractals 21 (2004) 749–761.

[2] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn. 25 (1992) 567–581.

[3] S. Lian, J. Sun and Z. Wang. "Security analysis of a chaos-based image encryption algorithm," Physica A: Statistical and Theoretical Physics, vol. 351, Issues 2-4, 15 June 2005, pp. 645-661.

[4] T. Paraskevi, N. Klimis, K. Stefanos. "Security of Human Video Objects by Incorporating a Chaos-Based Feedback Cryptographic Scheme," ACM Multimedia '04, October, 10-16, 2004, New York, NY USA.

[5] O. S. Faragallah, "Utilization of Security Techniques for Multimedia Applications", Ph. D. Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2007.

[6] I. F. Elashry, "Image Encryption", Ms. D. Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2010.

[7] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images" International Journal of Computer, Information, and Systems Science, and Engineering 1:1 PP.33-39, 2007, ISSN1307-2331.

[8] 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". International Journal of Computing and Informatics, VOL. 31, No. 1 PP. 121-129, 2007, ISSN 0350-5596242007.

[9] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm forDigital Images." Journal of Optical Engineering, vol. 45(10), 107003(1-7), 2006.

[10] Fridrich. "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcation and Chaos, 8(6):1259–1284, 1998.

[11] . K. Pareek, V. Patidar and K. K. Sud. "Cryptography using multiple one-dimensional chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 10, Issue 7, October 2005, pp. 715-723.