INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 5 ISSUE 2 – MAY 2015 - ISSN: 2349 - 9303

Color Image Encryption and Decryption Using Multiple Chaotic Maps

V.Kumar[1]
[1]P.A College of Engineering and Technology
Computer Science and Engineering
kumarpride@gmail.com

M.Yuvaraja[2]
[2]P.A college of Engineering and Technology
Electronics and Communication Engineering
yuvarajmuthusamy@gmail.com

Abstract— Owing to advances in communication technology, a bulk of visual digital data is being stored and transmitted over the internet now-a-days. Particularly millions and millions of images transfer through the network per day as per the statistics and a result, the security of image data is an important requirement. Image encryption algorithm is used to provide this security. In this paper, an image encryption algorithm based on confusion diffusion architecture that uses dynamic key space is proposed. An internal key generator is used to generate the initial seeds for the overall encryption scheme is proposed. With these initial seeds logistic map generates pseudo random numbers then these numbers are converted into permutation order for permutation. The diffusion bits are generated in parallel using the logistic map and manipulated with pixels confused. The image pixels are iteratively confused and diffused using permutation order and diffusion bits respectively to produce cipher image in minimum number of rounds. This paper proposes a new kind of initial seed generation that utilizes the combo of logistic and tent maps. Even all external seeds are same. The internal seeds will be totally different. This ensures the key sensitivity. The simulation results and analysis confirm that the satisfactory level of security is achieved in three rounds and overall encryption time is saved**.**

Index Terms— Confusion Order, permutation, Diffusion, Logistic maps, tent maps

1 INTRODUCTION

. The network technology and multimedia technology have more advanced in development digital images are used more widely in day to day activities. The security of the digital images has been taken as a greater effort in protection due to the access on the internet. In order to protect the image the confidentiality of images encryption is necessary. The traditional cryptographic tools such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) are used in encryption, but they are not suitable for encrypting digital images without any modification because of a size that is larger than that of the text. These methods require a great deal of computation time.

The various form of cryptography has their own approaches but the main goal of data hiding is to conceal the hidden data by the carrier media is to transfer data without drawing suspicion. These hiding algorithm are to maintain the natural appearance on the data or image by keeping uninvolved from thinking the information exists. The random number generators have proven invaluable in simulating natural phenomena and in sampling data. The copying a digital data is very easy and fast too so, issues like, protection of the content and misuse of the same, arise. Image encryption came as a technique and a tool to overcome shortcomings of current secured transmission of digital data. Many encryption methods have been proposed in literature, the most common used to protect large multimedia file is by using conventional encryption techniques. Some of the popular techniques are DES, and AES. Implementation of these algorithms cannot provide suitable encryption rates while security of these algorithms relies on the difficulty of quickly factorizing large numbers or solving the discrete logarithm problem, topics are seriously challenged by recent advances in number theory and distributed computing.

The encryption technique used in this paper is not a conventional one. Chaotic cryptographic scheme is a private encryption scheme, used here to encrypt the image. Chaotic map presents desired cryptographic qualities such as simplicity of implementation leads to higher encryption rates and excellent security. In this work two maps are used to encrypt the image, maps used are standard logistic map and tent map. The parameters of these two maps are used as a key for encryption.

2. REQUIREMENTS OF MULTIMEDIA ENCRYPTION

Due to special characteristics of multimedia data, such as large data volumes, high redundancy, interactive operations, and requires real-time responses, sometimes multimedia applications have their own requirements like security, invariance of compression ratio, format compliance, transmission error tolerance. For multimedia encryption, security is the requirement, thus the usage of chaotic maps should guarantee the security of a multimedia datum. Generally speaking, an encryption algorithm is regarded as secure the cost for cracking is no smaller than the One paid for the authorization of video content. For example, in broadcasting, the news may be of no value after an hour. Thus, the attacker cannot break the encryption algorithm during an hour, and then the encryption algorithm may be regarded as secure in this application Saikai et al (2014). Security of an encryption usually consists of perceptual security, key space, key sensitivity, and the ability against potential attacks.

3. GENERAL CHAOTIC SYSTEM

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behavior regarding complexity, chaotic cycle length, chaotic interval, periodic windows, sensitivity to initial conditions and reaction to trajectory perturbations, influence the structure or behavior of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map and efficiency; is desirable to provide some independency between the cryptosystem and the chaotic map under consideration.

The encryption algorithms based on chaos offer the advantages to be very sensitive to the initial conditions, periodicity, randomness and simplicity. Chaotic encryption systems generally have high speed with low cost, makes them better candidate than conventional methods for multimedia data encryption.

The architecture of substitution diffusion type chaos image cryptosystems is shown in Figure1. There are two stage are repeated for n and m times. In the substitution stage the pixels are permuted is the spatial correlation between the pixels are broken by permutation method. In the diffusion stage the value of each pixel is changed by adding and shifting operations. In a m rounds are performed together with the permutation. The existing system is a modified version of the Ravisankar et al (2006) cryptosystem.

The whole substitution-diffusion round repeats for a number of times to achieve a satisfactory level of security, the parameter of the chaotic maps governing the permutation and diffusion should better be distinct in different rounds. This is achieved around key generator with a seed secret key is input. In this cryptosystem, the substitution process is realized by solely by permuting gall pixels by an invertible discredited 2D standard map, without mixing their values. As the corner pixels is not permuted at all under the standard map, a random scan couple (r_x,r_y) is included to permute this corner this pixel together with other pixels. The modified standard map equations are given by equation (1) and (2).

$$X_{k+1}=(x_k+y_k+r_x+r_y)\mathrm{mod}N \qquad (1)$$

$$Y_{k+1}=(y_k+r_y+K_c\sin 2x_{k+1}/N)\mathrm{mod}N \qquad (2)$$

($x_{k,}y_k$) and ($x_{k+1,}y_{k+1}$) is the original and permuted pixel position of an N*N image, respectively. The standard map parameter KC is a positive integer.

In the diffusion stage, each pixel of the 2D permuted image is scanned sequentially; usually start form the upper left corner. The diffusion effect in this stage is achieved by the following equation (3) and (4). In vi the value of the ith pixel of the permuted image, c_{i-1} and c_i is the value of the (i-1) th and the ith pixel of the image, respectively. The seed of the diffusion function is c is obtained from the diffusion key $K_{d.}$ The nonlinear function $f(c_{i-1})$ is the logistic map is given by
equation (3).

$$f(c_{i-1})=4c_{i-1}(1-c_{i-1}) \qquad (3)$$

The quantization function q (c_{i-1}) takes the L bits just after the decimal points, as defined by equation (4).

$$q(X,L)=2^{L}X \qquad (4)$$

$X=0\ b_1b_2b_3\ldots b_l..$ is the binary representation of X and b_i is either 0 or 1

The new pixel value obtained by exclusive –OR (XOR) the current pixel value vi of the permuted image with an L-bit sequence from the logistic map taking the previous diffused pixel value c_{i-1} as input. As the previous diffused pixel will affect the current one, a tiny change in the plain image is reflected in more than one pixel in the cipher image and so the diffusion effect is introduced in this stage.

4. PROPOSED SCHEME FOR ENCRYPTION

The proposed schema is a modification of the one suggested by Ravisankar et al (2006). In their cryptosystem, an explicit diffusion function based on a logic map is used to spread out the influence of single plain image pixels over many cipher image elements. Although the diffusion function is executed at a fairly high rate, it is still the higher cost, in terms computational time, of the whole cryptosystem

The encryption speed can be accelerated substantially fewer diffusion rounds are required. The diffusion effect is downgrade we simply reduce the number of diffusion rounds and keep other parts unchanged. A better way is to introduce certain diffusion effect in the permutation stage as well. The architecture of the proposed method is shown in Figure 1. In the permutation stage both the permutation on pixel position and the change of are carried out at the same time while the diffusion process remains unchanged. As a result, the pixel value of that mixing effect of the whole cryptosystem is contributed by two levels of diffusion operation.

The modified permutation process and the original diffusion function. As the diffusion effect is not solely contributed by the diffusion function, the same level of security is achieved in fewer cipher rounds. Thus the encryption speed is that accelerated.

In this modified permutation stage, the new position of a pixels is calculated according to equation below. Before performing the pixel relocation, diffusion effect is injected by adding the current pixels value of the plain image to the previous permutated and then performs a cyclic shift. Other simple logical operation such as XOR can be used instead of the addition operation. Simulation results found the add and then shift combination leads to the best performance and so it becomes the choice in our cryptosystem. The new pixel value is then given by equation (5).

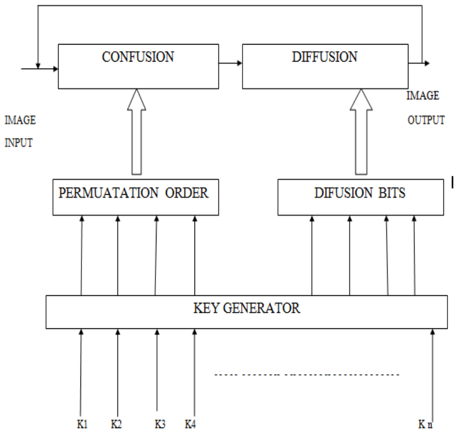

Figure 1 Proposed Encryption Structure

$$V_i=cyc[(p_i+v_{i-1})modL,LSB3(v_{i-1})] \qquad (5)$$

pi is the current pixel value of the plain image, L is the total number of grey levels of the image,v_{i-1} is the value of the (i-1) th pixel after permutation, Cycle [s, q] is the q-bit right cyclic shift on the binary sequences s, LSB3(s) refers to the value of the least three significant bits of s, v_i is the resultant pixel value in the permutated image. Similar to the effect of using higher-dimensional chaotic maps for image encryption, this modification makes the histogram of confused image uniform in a few rounds. Take a 256*256 white square image as an example of homogenous image.

The existing cryptosystem gives noisy cipher image and a uniform histogram in only three permutation rounds. By the property of pixels value mixing, the value of every single pixel is diffused over the image. It is regarded as the first level diffusion of the proposed system.

A key generator is proposed on the tent map as shown in Figure 2. The advantages of the tent map over the logistic map is calculation are simplified dramatically .In particularly, the higher order iterates of the tent map, are involved in the study of the asymptotic dynamics, are themselves piecewise linear maps and are easy to compute. This form is mainly designed to increase the sensitivity of the key as shown below. In Figure2 each tent map in the formation is feed with the initial seed is external keys k_1, k_2 and iterated for number of times. The final values obtained from the iteration are feed to the next tent map. Internal keys k_{in1}, k_{in2} are obtained at the final tent maps and this kind of feeding will increase the sensitivity of key.

A small changes in the external keys scattered through the neighbors at each rounds and the final result will be different one is a small change in a key dramatically change the results and thus the structure proposed to generate the internal keys will highly resist the brute force attack.

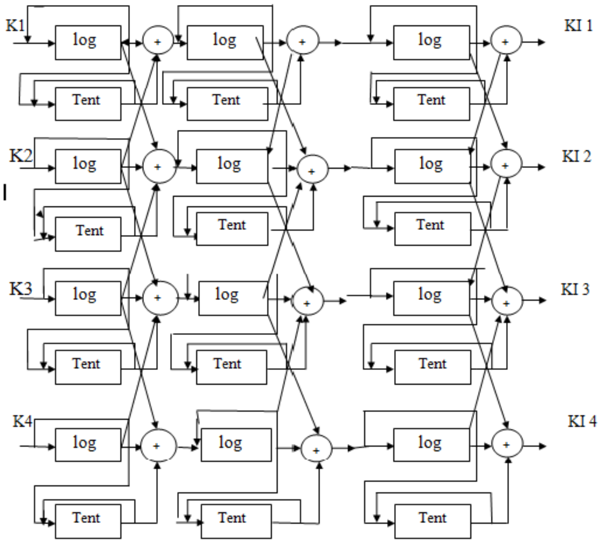

Figure 2 Internal Seed Generation

For example if four external keys are used then the total number possible keys will be equal to 2^{212}approx $6.58*10^{63}$. Given today's computer speed, it is commonly accepted a key space of a a size smaller than 2^{128} is not secure enough. In the present case this phenomena is satisfied and this structures more suitable, very sensitive and good enough to generate the internal keys in a unpredictable manners.

Following analysis shows the sensitivity of the proposed key generator,

Internal key space is,
Kspace=[0.1234567891234567,0.9876543219876543,0.4569871234569871,0.65412398745698874]

After the 200 iteration (or) at the end of level 1 the key space will be,
Kspace=[0.806566923490395,0.433024531300489,0.326873336834747,0.977189373512217]

At the end of 16 levels, the generated internals keys will be,
Kspace=[0.322426612184176,0.146663977532628,0.522539285981829,0.439739833426830].

Small change in KSpace will produce entirely different key as shown below, number in bold show the challenge,
Kspace=[0.1234567891234567,.9876543219875543,0.4569871234569871,0.65412398745698874]

Final key after 16 levels,
Kspace=[0.612998181420386,0.337221761924433,0.371654212088910,0.890801990516176]

Key sensitivity is clear from the above analysis; the proposed structure for generating the initial seed is very sensitive to its initial conditions. A small change in K space shown in bold is the change made, as a result the final result is completely deviated from the original one. Internal key will be 53 bits each.

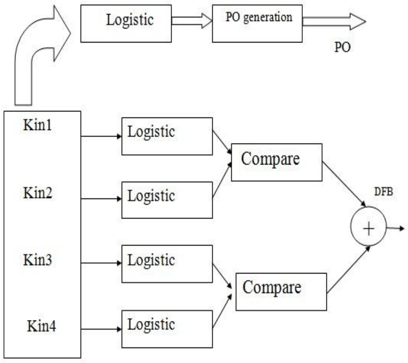

Figure 3 PO and DFB Generation

In the Figure3 shows the generations of keys are used to produce diffusion bits used for dispersing the correlation among the pixels. Internal keys (Kin1, Kin2.., K inn) are given to the logistic maps grouped as shown in Figure 3.Each of the map is iterated for N time where n equal to the length of bit stream and the resulting values are compared to produce the diffusion bits, if map-1 produces values X and map-2 produces values-y then the random bits are generated by the following relation.

5. EXPERIMENTAL RESULTS

The grey-level images Lena of a a size 256*256 are used as the plain image. The corresponding cipher image is shown in the following Figure 3 respectively. Decryption of the encrypted image and its respective histograms with the variation in its initial secret key shows in the results. The histogram distributions of all encrypted images are flat. This analysis proves there is no chance for statistical attacks on the proposed scheme.

The histogram of several original images is widely different. Results shows the encrypted images at different rounds and their histograms and encrypted image at initial set of key and its histogram. Encryption and decryption for this elapsed time varying based on the images a sizes. For this method taking image a a size is 256*256 based on this elapsed time is calculated as 1.2953.

The existing cryptosystem gives noisy cipher image and a uniform histogram in only three permutation rounds. By the property of pixels value mixing, the value of every single pixel is diffused over the image. It is regarded as the first level diffusion of the proposed system.

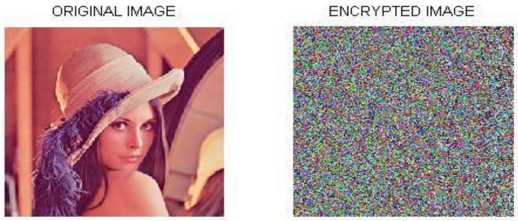

Figure 3 Image Encryption

6. SECURITY ANALYSIS

The proposed encryption algorithm has been tested with several test images of differing content. The visual inspection of the original encrypted and decrypted images of different images after applied only one round of encryption algorithm. The first row shows the original images there second row shows the encrypted images and the last row shows the decrypted images. The encrypted images are non-recognizable in appearance, unintelligible, random and noise-like images without any leakage of the original information. This demonstrates the proposed algorithm can be used to protect various images for that is diverse protection. The decrypted images are exactly same as the original images.

A. HISTOGRAM ANALYSIS

The histograms present the statistical characteristics of images. An image histogram plots the frequency of occurrences of each gray level. An encrypted image is expected to have no statistical similarity with the original image to prevent the leakage of information. The histogram of several plain images are computed and analyzed. The histogram image is shown in Figure4. The histogram of the encrypted image is uniformly distributed and is completely different from of the original image, and bears no statistical resemblance to the original image. Hence the proposed algorithm is resistant to statistical attacks. The diffusion function is employed to modify the gray values of the image pixels to confuse the relationship between the plain image and the encrypted image. The diffusion function is to almost all pixels in the whole image.

The encrypted images are non-recognizable in appearance, unintelligible, incomprehensible, random and noise-like images without any leakage of the original information. This demonstrates the proposed algorithm can be used to protect various images for diverse protection. The decrypted images are exactly same as the original images.

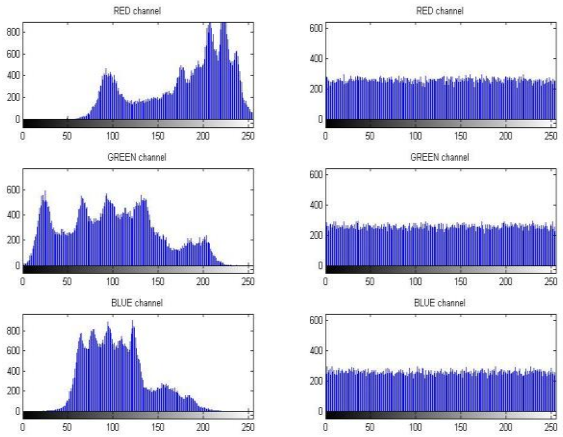

Figure 4 Encrypted histogram analyses

B. KEY SPACE ANALYSIS

The key-space of an encryption system should be sufficiently large enough to resist brute-force attacks. Brute-force attack is an attack an opponent tries to break the cryptosystem by exhaustive search with all possible keys. In our schema key space is increased as 53 bit. It is resist against the brute force attack.

C. CORRELATION COEFFICIENT ANALYSIS

Correlation between the pixels of the image must also be to check the robustness against the statistical attacks. The best encryption scheme the correlation between the pixels must be zero. This analysis shows the correlation between the randomly selected pairs of both plain image and encrypted image. This analysis carried out by following the procedures, Randomly 5,000 pairs are selected and they are selected like horizontally, vertically and diagonally adjacent.

Moreover, we have also calculated the correlation between two vertically as well as horizontally adjacent pixels in the original encrypted images. For this calculation, we have used the following formula,

$$r_{xy} = \frac{E\{[x-E(x)][y-E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (6)$$

$$E(x) = \frac{1}{s}\sum_{i=1}^{s} x_i \qquad (7)$$

$$D(x) = \frac{1}{s}\sum_{i=1}^{s}[x_i - E(x)]^2 \qquad (8)$$

Where x and y are the value of two adjacent pixels in the image and N is total number of pixels selected from the image for the calculation. However, the two adjacent pixels in the original image are highly correlated.

Table.1 Correlation Co-efficient Analysis

Parameters	Horizontal	Vertical	Diagonal
Plain image.lena	0.9311	0.9301	0.9321
Encrypted image.lena	-0.0299	-0.0170	-0.0358
Plain image.house	0.9532	0.9512	0.9567
Encrypted image.house	-0.0203	-0.0154	-0.0201

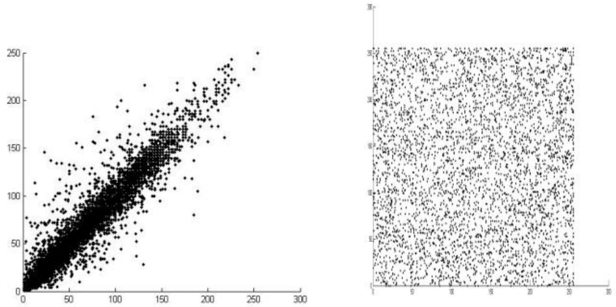

Figure 5 Plain and Encrypted image plot

D. DIFFERENTIAL ATTACK

The range of NPCR is [0, 1]. When N (C1, C2)00, it implies that all pixels in C2 remain the same values as in C1. When N (C1, C2)01, it implies that all pixel values in C2 are changed compared to those in C1. In other words, it is very difficult to establish relationships between this pair of cipher-image C1 and C2. However, N(C1, C2)01 rarely happens, because even two independently generated true random images fail to achieve this NPCR maximum with a high possibility, especially when the image a size is fairly large compared to 255. The range of UACI is clearly [0, 1] as well, but it is not obvious that what a desired.

Table.2 Differential Analysis

Parameters	NPCR	UACI	NBCR
Plane	99.6038	33.7276	50.0638
Lena	99.6048	33.0178	49.8825
Baboon	99.6099	33.1335	50.0435
Pepper	99.6068	33.9751	49.7653
House	99.7078	33.4236	50.0312
Tree	99.7341	33.7634	49.9354
Jelly Beans	99.8081	33.6734	49.9675
Aerial	99.6759	33.7650	50.0312
clock	99.7856	33.5634	50.0231
Boat.512	99.8654	33.5432	50.0010
Elaine.512	99.5641	33.2318	50.0321
Fishing Boat.512	99.9341	33.2243	49.9801
Air plane.512	99.5674	33.5320	50.0176
Airport.1k	99.8726	33.8765	50.0129

7. CONCLUSION AND FUTURE SCOPE

The typical structure of chaos-based image encryption schemes has been studied. In this work an efficient method for encrypting the images using two chaotic maps have been proposed and simulated. Permutation is applied to each pixel in the image and its order assigns for that pixels. The proposed chaotic algorithm is quite simple and compact. The result shows that using this algorithm in image encryption results in accuracy and faster than traditional algorithms. This work is also extended to color image.

The main objective of this work is to develop a secure image encryption scheme that can provide more security in a real time for sending and receiving the images. Simulation result shows that the scheme performs well with number of images with reduced time for encryption.

Chaotic technique can be use in video encryption hence in future video encryption algorithm can be proposed. Chaotic technique works on two steps hence reverse of these two steps can be apply on the encryption of data where data will be converting in image data. Hence in future a lot of work can be done in chaotic technique like designing of algorithm for video, graphs, text any kind of data and in reverse for design of decryption algorithms.

REFERENCES

[1] Ankit Gupta, Namrata Joshi and ChetanNagar (2012), 'A Review New Symmetric Image Encryption Scheme Based On Correlation Pattern', International Journal on Emerging Technologies 3(1): 102-104.

[2] Bhagwati Prasad, Kunti Mishra (2014), 'A Combined Encryption Compression Scheme Using Chaotic Maps', Cybernetics and Information Technologies Volume 13, No 2, Print ISSN: 1311-9702; Online ISSN: 1314-4081,International Conference on Signal Processing and Integrated Networks (SPIN)236.

[3] Pareek N.K. Vinod Patidhar and Sud K.K. (2004), 'Image encryption using chaotic logistic map', Image and Vision Computing 24 926-934, Received 10 August 2004; received in revised form 11 August2005; accepted 6 February 2006.

[4] Ravishankar K.C. and Venkateshmurthy M.G. (2006), 'Region Based Selective Image Encryption', International Conference on Computing & Informatics. ICOCI '06, pg: 1-6.

[5] Ranjith Kumar R. and Bala Kumar M. (2014), 'A new chaotic image encryption using parametric switching based permutation and diffusion', ISSN: 0976-9102(online) ictact journal on image and video processing, volume: 04, issue: 04.

[6] ShiguoLian, Jinsheng Sun, Dengfeng Zhang and Zhiquan Wang (2005), 'A Selective Image Encryption Scheme Based on JPEG2000Codec', Multimedia Information Processing - PCM, Lecture Notes in Computer Science Volume 3332, pp 65-72.

[7] Saikia M. Bora S.J and Hussain A. (2014), 'A Review on Applications of Multimedia Encryption', ISBN: 987-81-8487-088-6 in national conference on Network Security-issues, challenges and Techniques, at Tezpur University.

[8] Saikia M. and Majumder S. (2011), 'Spread Spectrum Embedding of Colluder Traceable Codeword in Multimedia', Emerging Applications of Information Technology (EAIT), 2011 Second International Conference, pp.190,193, 19-20 Feb 2011.

[9] Shahid Z. Chaumont M. and Puech W. (2005), 'Spread Spectrum-based Watermarking for tardos Code-based Fingerprinting for h.264/avc Video', ICIP Year 2005.

[10] Xiliang Liu, Ahmet and Eskicioglu (2005), 'Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions', CRC Press, Pg 43-85.