Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.343 – 348

Image Encryption Using Scrambling and Diffusion Operation Using Chaotic Map

Usha Salagundi[1], Nilam Chheda[2], Kiran[3]
[1]M.Tech Student, Digital Electronics, BITM College, Bellary
[2]Assistant Professor, Department of ECE, BITM College, Bellary
[3]Assistant Professor, Department & ECE, GMIT, Mandya
[1] ushe.10@gmai.com; [2] nilamg.engr@gmail.com; [3] kiran.mtech12@gmail.com

Abstract— Security of image data has become increasingly important for many applications like video conferencing; secure facsimile, medical, military applications etc. In this paper we are proposed image encryption technique which includes scrambling and diffusion stages. In scrambling stage, Input image undergo row scrambling and column scrambling with the help of chaotic map. In diffusion stage manipulating the pixels value based on parity function. The result shows that proposed method achieves good security in terms of entropy and NPCR. Decryption is the reverse process of encryption.
Keywords— Encryption, row scrambling, column scrambling, chaotic map, parity function

I. INTRODUCTION

With the rapid development of computer network technology, a lot of sensitive information is transmitted over the network. Hence information security becomes more and more important. Image information transmission has increased rapidly and hence image encryption technology has drawn more attention. Nowadays, image encryption schemes include two processes: substitution and diffusion. The substitution stage permutes all the pixels as a whole, without changing their values. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in a pixel spreads to as many pixels in the cipher-image as possible. The two processes can achieve a satisfactory level of security.

There are several areas like medical image security, satellite image transmission, military information security, confidential video-conferencing, tele-medicine and so on which needs image encryption for its security. There is a huge demand of information security in internet banking, mobile banking, patient information security, confidential research result security, confidential photography, and confidential laboratory images[1-4].

Vinod patidar et.al [5] presented a secure chaotic based permutation-substitution scheme of image encryption. This is loss-less symmetric block cipher. They are used secret key of length 161 bit and this key can be used as initial condition and system parameter of chaotic map. Number of rounds depends on secret key. To increase the speed of encryption they convert 3D image matrix into 2 D image matrix. Permutations are done by row by row and column by column using pseudo random number sequence generated from chaotic sequence. In substitution process uses chaotic sequence and initial vector depends on secret key and mixed with plain image.

Chong FU et.al [6] presented a novel chaos based bit level permutation scheme for digital image encryption and provides a fast and high security. To overcome the drawbacks of conventional algorithms they propose significant diffusion effect in permutation procedure through a two stage bit level shuffling algorithm. Arnald cat map and chaotic sequence are used for shuffle all bit planes. This method decreases computational complexity and real time image communication applications.

Xindyuan Wang.et al [7] presented a novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. Secret keys will be processed by key generator before they can really be used in the encryption scheme, and in this stage this paper associates plain image with secret keys; Secondly, by imitating the trajectory of water wave movement, encryption algorithm will do scrambling operations to the image. Finally combines water drop motion and dynamic look up table to realize diffusion operations. For an 8 bits pixel, this algorithm will just dispose the higher 4 bits, which is because the higher 4 bits contain the vast majority of information of the image.

Ruisong Ye [8] presented a novel chaos based image encryption scheme with an efficient permutation diffusion mechanism. Generally permutation diffusion mechanism permuting the positions of image pixels in order to reduce the high correlation between adjacent pixels of plain image and change the pixel value in diffusion stage. In the permutation process, a generalized Arnold map is utilized to generate one chaotic orbit used to get two index order sequences for the permutation of image pixel positions; in the diffusion process, a generalized Arnold map and a generalized Bernoulli shift map are employed to yield two pseudo-random gray value sequences for a two-way diffusion of gray values. Encryption scheme is easy to manipulate and can be applied to any image with unequal width and height as well.

Ahmed A.abd El-Latif et.al [9]have proposed a hybrid chaotic system and cyclic elliptic curve for image encryption and provides a external secret key of 256 bit and one generalized chaotic logistic map. using the cyclic elliptic curve to derive generated key stream are mixed with key sequences.

II. CHAOTIC MAP

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behaviour regarding complexity, chaotic properties cycle length, chaotic interval, periodic windows, etc., sensitivity to initial conditions and reaction to trajectory perturbations, etc., that 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, it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to full the security and efficiency requirements of a good cryptosystem. For their mathematical simplicity there are two options: logistic map and tent map.

The logistic map is represented by

$$Xn+1=r*Xn*(1-Xn)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

The logistic map chaotic signal used has primary values of Xn€ [0; 1]and r € [3 : 57; 4]:

III.PROPOSED ALGORITHM

Block diagram of proposed technique as shown in figure 1. Block diagram mainly consists of scrambling and diffusion stages. In scrambling stage input image undergo row and column scrambling with the help of chaotic map and initial conditions. Circular operation in row and column scrambling is considered continuously in this algorithm. sorted value X used for row cyclic shift while the left Y sorted values are used for column cyclic shift. This means that we shift the first row with x1 units to the right and circulate in the left, the second row with x2 units to the right and circulate in the left, the same function is applied until the last row of the plain-image has been processed. Similarly, the ith column is moved with y i units to the bottom and circulate at the top. The whole scrambling function is finished if each row and column is shifted. Then, we can obtain the scrambled image B. The algorithm of circular operation can be found in Algorithm 1 and generation of random numbers using chaotic map as described below.

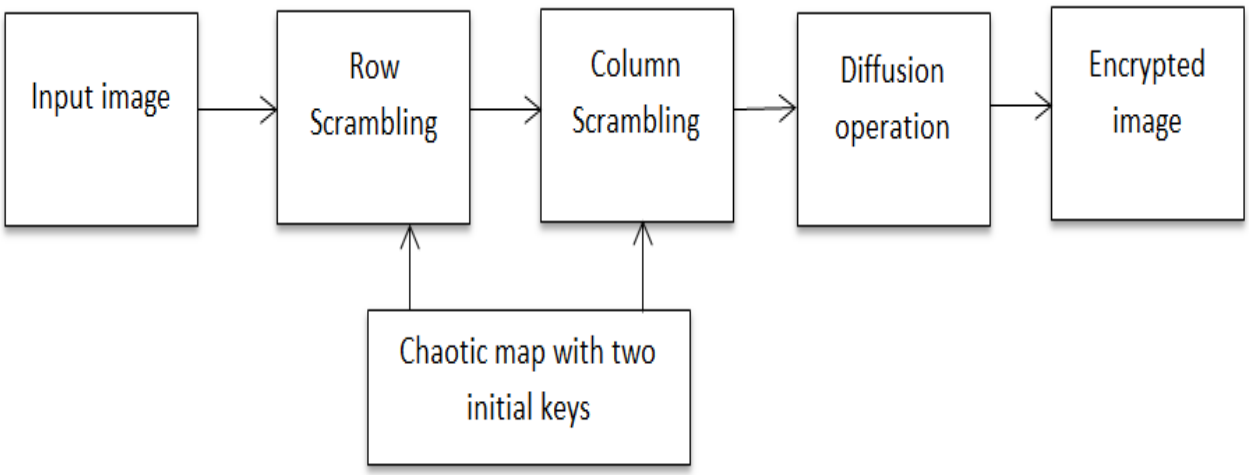

Figure 1: Block diagram of proposed algorithm

Step 1:With a given initial parameter X0 and r=3.99999 by using Eq.1 chaotic sequence generated. X = X1,X2,……Xm.
Step 2:The chaotic sequence X is sorted in ascending order and we get a new set
x = sort(X) = x1, x2,…… xm.
Step 3:According to set x value, Input image is permuted and to get an encrypted image.

In diffusion process, apply the parity function for each pixel of permuted image and flip bit 0 into bit 1 and vice versa when parity function outputting even input. Parity function defined as count the number of bit 1 in each pixel if it is even flip the all the bits.

Diffusion operation further can be extended using chaining method. In chaining method each pixel of diffused image go for parity function by checking the previous pixel parity.

IV. PARAMETERS FOR THE EVALUATION OF AN IMAGE ENCRYPTION SCHEME

A. Mean Square Error (MSE)

Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect. Let C1 and C2 are input image and encrypted image respectively, then MSE can be calculated as in Eq. 2 .

$$MSE = \frac{1}{M * N} \sum_{i=1}^{N} \sum_{j=1}^{M} [c1(i,j) - c2(i,j)]^2 \qquad (2)$$

B. Information Entropy Analysis

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \qquad (3)$$

C. Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio can be used to evaluate an encryption scheme [1]. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext image and the cipher text image. Mathematically as in.

$$PSNR = 20 * \log_{10} \left[\frac{255}{MSE} \right] \qquad (4)$$

D. UACI and NPCR

A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change

rate (NPCR) and Unified average changing intensity (UACI) [8]. The equation to calculate UACI is Eq. 5.

$$UACI = \frac{1}{M * N} \sum_{i,j} \frac{| C1(i,j) - C2(i,j) |}{255} \times 100\% \quad (5)$$

Where, M stands for image's width, N stands for image's height, C1(i,j) and C2(i,j) are the input and encrypted image respectively. NPCR can be calculated by Eq. 6.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (6)$$

Where, M stands for image's width, N stands for image's height and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1 & \text{if C1(i,j)} \neq \text{C2(i,j);} \\ 0 & \text{if C1(i,j)} = \text{C2(i,j).} \end{cases}$$

TABLE I
CHAOS BASED DOCUMENT IMAGE ENCRYPTION

Input Image	Permuted image	Encrypted Image	Decrypted Image
			
			
			

TABLE II
PARAMETERS FOR PROPOSED ALGORITHM

Imag	Ent_in	Ent_enc	NPCR	UACI	MSE	PSNR
lena	7.2719	7.6351	99.4584	25.9309	106.3724	28.2077
parrot	7.5043	7.7418	99.4851	27.7084	96.4359	28.3860
vegetable	7.2978	7.6513	99.3816	30.2581	101.9726	28.3367

From the table II we can conclude that MSE value increases amount of encryption increases and NPCR value approximately equal to 100 % that indicates all the pixels of original image gets altered.

V. CONCLUSIONS

This paper describes image encryption technique which includes scrambling and diffusion stages. In scrambling stage, input image undergo row scrambling and column scrambling with the help of chaotic map. In diffusion stage manipulating the pixels value based on parity function. From the experimental -result, we conclude that the proposed method simple and easy to implement. This method can be used for real time applications.

REFERENCES

[1]. A Chalechale and F Safaei. Visual-based Interface using Hand Gesture Recognition and Object Tracking, In Iranian Journal of Science and Technology, Transaction B, Engineering, 32(B3):279–293, 2008.
[2]. CheWei-Gang, Chung-Lin Huang and Wen Liang Hwang. Automatic EyeWinks Interpretation System for Human-Machine Interface, In EURASIP Journal on Image and Video Processing, 564–572, 2007.
[3]. Rathgeb and Uh. A Survey on Biometric Cryptosystems and Cancelable Biometrics, In EURASIP Journal on Information Security, 3, 2011.
[4]. Aditya Ramamoorthy. Recognition of Dynamic Hand Gestures, In Pattern Recognition, 36:2069–2081, 2003.
[5]. V Patidar, N Pareek, G Purohit and K Sud. A Robust and Secure Chaotic Standard Map based Pseudorandom Permutation Substitution Scheme for Image Encryption, Optics Communications, 284(19):4331–4339,2011.
[6]. C Fu, B b Lin, Y S Miao, X Liu and J J Chen. A Novel Chaos-based Bit-level Permutation Scheme for Digital Image Encryption, Optics Communications, 284(23):5415–5423, 2011.
[7]. X Wang and L Yang. A Novel Chaotic Image Encryption Algorithm based on Water Wave Motion and Water Drop Diffusion Models, Optics Communications, 2012.
[8]. R Ye. A Novel Chaos-based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism, Optics Communications, 284(22):5290–5298, 2011.
[9]. A A Abd El-Latif and X Niu. A Hybrid Chaotic System and Cyclic Elliptic Curve for Image Encryption, AEU-International Journal of Electronics and Communications, 2012.

