International Journal of Image Processing and Vision Science

Volume 1 | Issue 4 Article 6

October 2012

ENHANCED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON TRIGONOMETRIC FUNCTIONS

M.K MOHSINA
Department of P.G, Applied Electronics, ICET, Mulavoor, m.k.mohasina@gmail.com

ROBIN ABRAHAM
Department of P.G, Applied Electronics, ICET, Mulavoor, robin.abraham@gmail.com

ENHANCED CHAOTIC IMAGE ENCRYPTION ALGORITHM BASED ON TRIGONOMETRIC FUNCTIONS

M.K MOHSINA[1] & ROBIN ABRAHAM[2]

[1,2]Department of P.G, Applied Electronics, ICET, Mulavoor.

Abstract:- The advent of wireless communications, both inside and outside the home-office environment has led to an Increased demand for effective encryption systems. The encryption of images is quite different from that of the texts due to the bulk data capacity and high redundancy of images. Traditional methods are difficult to handle the image encryption because of their small space of pseudo random sequence. At present, the chaotic maps have been widely used in image encryption for their extreme sensitivity to tiny changes of initial conditions. The chaos based algorithms have suggested a new and efficient way to deal with the problem of fast and highly secure image encryption. In this paper, we propose an algorithm in which two one-dimensional chaotic maps are used instead of a one-dimensional chaotic map. We also use an external secret key of 96-bits. Thereby it significantly increases the resistance to statistical and differential attacks. The results of experiment, statistical analysis, correlation coefficient analysis and key sensitivity tests show that the algorithm is of great security and practicability.

Keywords:-*Chaos;PseudoRandom Sequence; Chaotic Map;Trigonometric Function; Image Encryption*

I. INTRODUCTION

The amazing developments in the field of network communications during the past years have created a great requirement for secure image transmission over the Internet. Internet is a public network and is not so secure for the transmission of confidential images. To meet this challenge, cryptographic techniques need to be applied. Cryptography is the science of protecting the privacy of information during communication, under hostile conditions. In recent days, Chaos based methods are used for image Encryption. Chaos word has been derived from the Greek, which refers to unpredictability and it is defined as a study of nonlinear dynamic system. Chaos theory is a mathematical physics which was developed by Edward Lopez. Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics. The combination of chaotic theory and cryptography forms an important field of information security. In the past decade, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic maps have been proposed. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods.

Based on chaos functions, a variety of image encryption algorithms have been proposed during the past decade. In [3], a chaotic key-based algorithm (CKBA) was proposed for image encryption /decryption. The algorithm first generates a chaotic sequence by the 1-D chaos map (the logistic map), and then uses it to create two keys--two binary sequences. According to the binary sequence generated above, four operations were selected to shuffle the image pixels. They are the combination of the image pixels XOR or XNOR operation with the selected key. This method is simple but exist obvious defects in security. The defects of CKBA were pointed out in [4]: the method is very vulnerable to the chosen/known-plain-text attack with only one plain-image, and its security to brute-force cipher-text-only attack is questionable. In [5], an enhanced CKBA algorithm was proposed. The enhanced CKBA replaces the 1-D chaotic Logistic map with the piece wise linear chaotic map (PWLCM) so as to improve the balance property. It also increases the key size to 128 bits, adds two more cryptographic primitives and extends the scheme to operate on multiple rounds so that the chosen/known-plain-text attacks are no longer possible. In [7], to overcome the drawbacks of small key space and weak security in the widely used one-dimensional Logistic systems, this paper presented a new nonlinear chaotic algorithm that uses power function and tangent function instead of linear function. In [8] an algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data is introduced. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algorithm is tested with two different maps and performance analysis is done to select best suited map for encryption.

In this paper, a new image encryption algorithm based on two different chaotic maps is proposed. In the proposed algorithm, the plain-image is first encrypted by using a chaotic trigonometric function and then the shuffling of image pixels is carried out using another trigonometric function. The rest of this paper is organized as follows. In section II, a new algorithm is suggested for fast and secure image encryption based on the trigonometric functions. Section III provides a larg quantity of experiment data and makes performance analysis to the algorithm.

II. PROPOSED ENCRYPTION ALGORITHM

In this section, an algorithm based on the trigonometric function is introduced. We'll use the following trigonometric function (TF) as chaotic map for encrypting the plain image.

$$y = \frac{1}{2}(\sin(4\pi x) + 1) \quad (1)$$

After encrypting the plain image ,the following sine map is used to shuffle the image pixels.

$$X_{n+1}=0.99\mathrm{Sin}(\pi X_n) \quad (2)$$

A. ENCRYPTION ALGORITHM

Assume that we'll encrypt a 24 bit color image fp(plain image).The image size is [M,N,Z].The encryption steps are as follows Step 5. Shuffle fpm according to the perturb rule sets fl.

Step 5.1 Transform the rows of fpm.

Step 1. Randomly generate a 96-bit long binary sequence and change it into 12 ASCII codes. The K is our secrecy Key.

K=K1K2K3…..K12(ASCII)

Step 2. Generate the initial value x0, l0 of formula (1) and z0 of formula (1) according to K.. Get K1K2...K6, K7K8...K12 then calculate x0 and l0 according to formulas (3), (4)

$$X0 = (K1 * 2^{40} + K2 * 2^{32} + K3 * 2^{24} + K4 * 2^{16} + K5 * 2^{8} + K6)/2^{48} \quad (3)$$

$$l0 = (K7 * 2^{40} + K8 * 2^{32} + K9 * 2^{24} + K10 * 2^{16} + K11 * 2^{8} + K12)/2^{48} \quad (4)$$

Calculate z0 according to formula (6)

$$R = \sum_{i=1}^{12} Ki/256 \quad (5)$$

$$z0 = R - \mathrm{floor}(R) \quad (6)$$

Step 3. Generate the chaos mask fm and perturb rule sets fl.

Step 3.1 Generate fm. Use x0 as the initial value, and iterate the trigonometric function (1) 150 times so as to make the chaos system steady, then use the output as the initial value, continue iterating the trigonometric function (1) M*N*Z times, store M*N*Z output values in fm.

Step 3.2 Generate fl. Use l0 as the initial value, and iterate the trigonometric function (1) 150 times so as to make the chaos system steady, then use the output as the initial value, continue iterating the trigonometric function (1) 2*(M+N) times, store 2*(M+N) output values in fl.

Step 4. Generate fpm.

fpm = fp⊕ fm

There are 2*(M+N) values in fl. We divide them into four parts fl1, fl2, fl3 and fl4.

fl1 = fl(1)... fl(M)

fl2 = fl(M +1)... fl(M + N)

fl3 = fl(M + N +1)... fl(2M + N)

fl4 = fl(2M + N +1)... fl(2(M + N))

The fl1 and fl3 are used to confuse the rows of fpm. The fl2 and fl4 are used to confuse the columns of fpm.According to table 1, we divide the region [0,1] into 10 groups. Each group has a specific operation for encryption/decryption. For example, we need to confuse the row r1. We first get the value fl(r1). If fl(r1)=0.176. We look it up in table 1 and find the group number is 8. The corresponding operation is nonequivalent.

Group number	The range that value belonged to	Corresponding operations for Encryption/decryption
1	[0.00,0.01)[0.10,0.11).....[0.90,0.91)	Right shift this row according to the value stored in fl
2	[0.01,0.02)[0.11,0.12).....[0.91,0.92)	Use the value stored in fl as the initial value of trigonometric function and get the same number of values(Xr,Xg,Xb) as the image size in a row.Then R⊕Xr,G⊕Xg,B⊕Xb
3	[0.02,0.03)[0.12,0.13).....[0.92,0.93)	Left shift
4	[0.03,0.04)[0.13,0.14).....[0.93,0.94)	R⊕Xr,G⊕Xg,B⊕Xb
5	[0.04,0.05)[0.14,0.15).....[0.94,0.95)	Right shift
6	[0.05,0.06)[0.15,0.16).....[0.95,0.96)	R⊕Xr,G⊕Xg,B⊕Xb
7	[0.06,0.07)[0.16,0.17).....[0.96,0.97)	NOT(R),NOT(G),NOT(B)
8	[0.07,0.08)[0.17,0.18).....[0.97,0.98)	R⊕Xr,G⊕Xg,B⊕Xb
9	[0.08,0.09)[0.18,0.19).....[0.98,0.99)	Left shift
10	[0.09,0.10)[0.19,0.20).....[0.99,1.00)	R⊕Xr,G⊕Xg,B⊕Xb

Table 1: Table showing various operations for encryption and decryption

We get the value from fl(M+N+r1), and use it as the initial value to iterate the trigonometric function N*Z times and get N*Z values. Here Z is 3. We divide the N*Z value into 3 parts "X1, X2, X3" with the number N in each. Then get Xr=X1*255, Xg=X2*255, Xb=X3*255. At last, we do nonequivalent operation as follows. R ⊕ Xr , G ⊕ Xg , B ⊕ Xb

Step 5.2 Transform the columns of fpm. The step is similar to step 5.1. In order to ease the operations, we can transpose the image array. Change the column operations to row operations and we get the encrypted image.

Step 6. Separate R,G, B matrix of the encrypted Image and convert each R,G,B matrix in to single array (1×MN).

Step 7. The Sine map in formula (2) is iterated for n=1 to MxNxZ times to generate the required elements using the initial condition z0.Now divide the generated elements into three blocks of each equal to M×N.

Step 8. Now sort the elements of each block in ascending or descending order and compare the misorder between the original and sorted elements of

each block and tabulate the index change. We have got three series of index change values in according to three blocks.

Step 9. According to the obtained index, we change the intensity position to get the final encrypted image.

B. DECRYPTION PROCESS

The process of decryption is similar to the encryption. It is the inverse process of the encryption processing with the same key.

III. EXPERIMENTAL RESULTS AND

SECURITY ANALYSIS

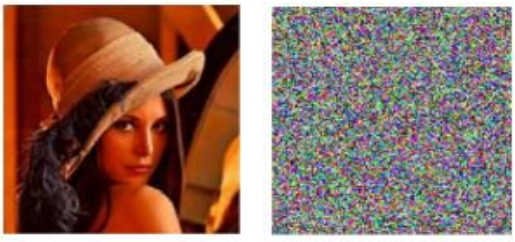
A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. To prove the robustness of the proposed image encryption procedure, we have performed statistical analysis, correlation coefficient analysis, security of key and key space analysis. If correlation coefficient is nearer to zero for an encrypted image, then algorithm is said to be better. To prove that decryption is possible only with one key, key sensitivity is calculated. In this section, we'll use the proposed algorithm to encrypt the image lena with size of 128×128×3.

A. STATISTICAL ANALYSIS

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. Histogram is widely used to evaluate the statistic feature of an image. We use the secret key "AC1FB58E39 07AD45AB1FB41C" to encrypt the image. Figure 1 shows the histograms. It is clear that the histograms of the encrypted image are fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image.

B. CORRELATION COEFFICIENT ANALYSIS

Correlation coefficient ' ' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related.



(a) (b)

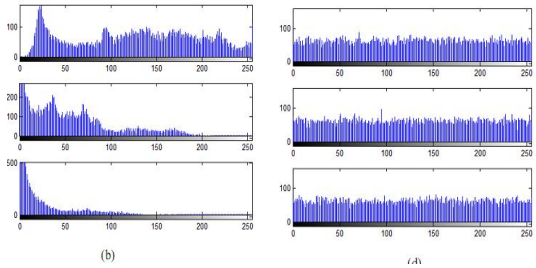


Figure 1. Histogram analysis: Frame (a) shows a plain-image. Frame(b) shows the the encrypted image .Frames (c) and (d) shows the histograms of red, green and blue channels of the plain-image and cipher image respectively.

The coefficient can be calculated by the following formulas. Where x and y are gray values of two adjacent pixels in an encrypted image. We randomly select 1000 pairs of vertically and horizontally adjacent pixels and calculate the correlation coefficients in two directions separately. The correlation coefficients among adjacent pixels of plain-image in three directions come out to be 0.9120 and 0.8645 respectively. The values of correlation coefficients obtained in encrypted images are listed in Table 2. The values of correlation coefficients show that the two adjacent pixels in the plain-image are highly correlated to each other and correlation coefficients are almost 1 whereas the values of correlation coefficients in the encrypted images are close to 0, this means that the adjacent pixels in the encrypted images are highly uncorrelated to each other.

$$\gamma(x,y) = \frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (7)$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}[xi - E(x)][yi - E(y)] \quad (8)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[xi - E(x)]^2 \quad (9)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} xi \quad (10)$$

Direction	Plain -Image	Cipher -Image
Vertical	0.9120	-0.0271
Horizontal	0.8645	-0.0089

Table 2. Correlation Coefficients of Two Adjacent Pixels In The Plain-Image And Cipher-Image.

These data prove that the chaotic encryption algorithm leads to a more secured encryption process.

C. SECURITY OF KEY AND KEY SPACE ANALYSIS

Figure 2 shows the cipher-image encrypted by 96-bit key "AC1FB58E3907AD45AB1FB41C", the decrypted images by the correct key "AC1FB58E3907AD45AB1FB41C" and the wrong key "AC1FB58E3907AD45AB1FB41A". Frame (c) shows that the image can be decrypted correctly by the correct key. Frame (d) shows that the image

Figure 2 : Image encryption and decryption experiment result: Frame (a)plain-image, Frame (b)cipher-image encrypted by key "AC1FB58E390 7AD45AB1FB41C", Frame (c) image decrypted by correct key "AC1FB58E3907AD45AB1FB41C", Frame (d) image decrypted by wrong key "AC1FB58E3907AD45AB1FB41A"

cannot be decrypted by the wrong key, and the decrypted image by the wrong key is of the same security feature to the cipher-image. We cannot get any useful information to attack from it.

IV. CONCLUSION

In this paper, a new way of image encryption scheme have been proposed which utilizes two chaotic maps and an external key of 96-bits. The initial conditions for both the maps are derived using the external secret key. In the proposed encryption process, several different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the trigonometric chaotic map. To make the cipher more robust against any attack, the pixel position of the encrypted image is changed according to the randomness of the chaotic elements, which is derived by comparing sorted and unsorted chaotic elements generated from sine map. We have carried out statistical analysis, correlation coefficient analysis and key space analysis to demonstrate the security of he new image encryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

REFERENCES

[1] R. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia, 1989, 8(1):29-41.

[6] T. Uehara, R. Safavi-Naini and P. Ogunbona, "Securing wavelet compression with random permutations," In: IEEE Pacific Rim Conference on Multimedia, 2000, p. 332-5.

[7] H.J. Gao, Y.S. Zhang, S.Y. Liang and D.Q. Li, "A new chaotic algorithm for image encryption," Published by Elsevier Ltd, 2005.

[8] "Chaos Image Encryption using Pixel shuffling" Manjunath Prasad and K.L.Sudha,DSCE, Bangalore,