Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical and Electronics Engineering

Elixir Elec. Engg. 116 (2018) 50013-50016

ISSN: 2229-712X

A Novel Thermal Image Encryption using Histogram Diffusion and Chaos Map

Lokesh B S[1], M B Manjunatha[2] and Panduranga H T[3]

[1]Research Scholar Jain University Bangalore-Karantaka India.

[2]Sampoorna Institute of Technology Channapttana-Karantaka India.

[3]Dept. of Electronics and Communication Govt. Polytechnic Turuvekere-karnataka India.

ARTICLE INFO

Article history:

Received: 26 January 2018;

Received in revised form:

27 February 2018;

Accepted: 7 March 2018;

Keywords

Histogram,
Bit Planes,
Thermal Images,
Encryp-Tion,
Decryption.

ABSTRACT

In a recent years, security for the thermal images are more necessary due to fast growing information technology. Here proposed an thermal image encryption based on histogram diffusion and permutation using chaotic map. As we know that histogram of thermal image distributed towards right (towards white pixel) and towards left (towards black). First step of proposed algorithm shift the histogram by mixing a random number. After that resultant image undergo permutation process with the help of chaotic map followed block wise histogram diffusing. In next level, apply the bit plane permutation. At last XOR operation with random image to get thermal encrypted image. The simulation results shows that proposed algorithm achieves high security.

1. INTRODUCTION

Thermal images plays an important role at Power stations, nuclear plants, petroleum products extraction and purification centers, research labs, Forensic labs, Military applications like, medical applications like - to detect few deceases (tumors/cancer etc), and during study of characteristic behavior of humans, animals or birds at some condition (treatment / injuries / biological changes). Thermal images image are different from normal images because there is a clarity of object structure in Darkness and sun glare; smoke, and smog; these images gives more information for particular applications and hence need security.

In Ref. [1], the authors are designed a real-time secure symmetric encryption scheme, which uses generalized two-dimensional chaotic cat map and 3D cat map to shuffle the spatial coordinate of image and chaotic system used in the diffusion stage. Permutation and diffusion based fast image encryption scheme was proposed in Ref. [2]. First partitioning the input image into pixel blocks. Then permutation of pixel blocks can be done with the help of spatio temporal chaos and for diffusion process, pseudo random number generator used. In Ref. [3],the authors firstly analysed the parameter sensitivity of standard map, and compared the secret key space of standard map with that of cat map and baker map. Then an improved standard map was used to realize position permutation, and the diffusion function consisted of logistic map that was used to realize the diffusion of image.

In Ref. [4], extended baker 3D map used to speed up image encryption while shuffling the position of plain-image. To diffuse the shuffled image, logistic map was used.In Ref. [5], the authors introduced sequential add-and-shift operations effect in the permutation stage. Although this may take a longer processing time in a single round, but the overall encryption time was reduced. 3D chaotic map based image encryption algorithm was proposed in Ref. [6]. The proposed algorithm was simple and efficient and based on three phases which provided necessary properties for a secure image encryption algorithm including permutation and diffusion properties. In Ref. [7], the paper proposed a novel color images encryption based on a Coupled Two-dimensional Piecewise Nonlinear Chaotic Map, called CTPNCM, and a masking process. Distinct characteristics of the algorithm were high security, high sensitivity, and high speed that can be applied in encryption of color images.

II. BIT PLANE SLICING

Pixel value ranges in a gray scale image from 0 to 255. Each pixel is composed of 8 bits (1 byte). Different amount of information contributed by the specific bits in the appearance of total image. Every gray scale image is composed of 8 binary images. Each binary image referred as bit plane. Bit plane 1 contain least amount of information and bit plane 8 (MSB) contain highest amount of information. Amount of information for each bit plane can be calculated in the equation 1.

$$I(i) = \frac{\sum_{j=0}^{i} 2^j}{256} \quad (1)$$

The following Table 1 shows the bit plane slicing of an thermal gray scale image and their amount of information.

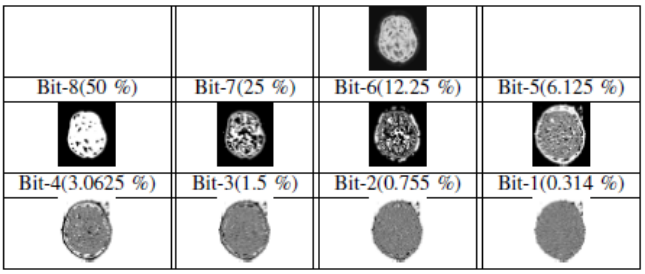
III. CHAOTIC MAP

In any image encryption, chaotic map is effective method used, because of its inherent characteristics such as ergodicity, unpredictability, randomness and sensitivity to its initial con-ditions. Generally chaotic map control by two parameters X0 and : The control parameter range is [0,4], but

Tele:
E-mail address: lokesh.hosamane1@gmail.com

it exhibits chaotic system when 2 [3:5; 4] and other parameter is initial condition value X0 2 [0; 1]: The chaotic map equation as follows.

TABLE I
BIT PLANE SLICING



$$X(i+1) = \mu * X(i) * (1 - X(i)) \quad (2)$$

Fig ?? shows a block diagram of proposed thermal image encryption.

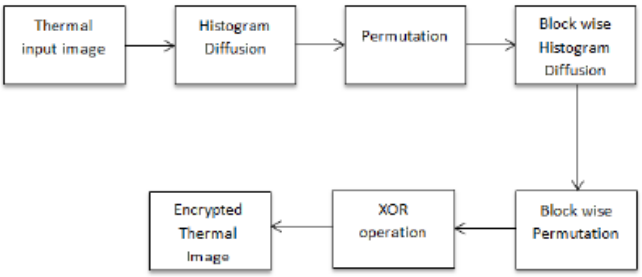


Fig 1. Block Diagram of Proposed Method

The proposed algorithm consists o 5- levels of encryption. They are

Level 1: Histogram Diffusing.
Level 2: Pixel Permutation.
Level 3: Block wise Histogram Diffusing.
Level 4: Bit Plane Permutation.
Level 5: Diffusion Operation.

Level 1: Histogram Diffusing

Histogram is pictorial representation of distributed pixels in the image. Generally thermal image histogram, the black and white pixels are highly distributed. So that it is difficult to encrypt the pixel value 0 (black value). Due to this an random number is added to image for histogram according to following equation.

$$I_H D = mod((I(i,j) + randomnumber), 256) \quad (3)$$

Where I is Input thermal image and I HD Histogram Diffused image.

Level 2:Pixel Permutation Process

As we know that original image having high correlation among the adjacent pixels. In any encryption algorithm, first we need to reduce the correlation. In order to reduce the correlation between the adjacent pixel. We need to shuffle the position of the pixel using pseudo random sequence using chaotic map. The mathematical equation for chaotic map as defined in Eq. ?? and algorithm for shuffling as described below.

Permutation using chaotic map

The detailed permutation procedure is described as follows:

Step 1:consider the input image of size m n.
Step 2: convert input image into one dimensional vector .
Step 3: based on initial key x0 and using chaotic map Eq.?? with r=3.9999 generates chaotic sequence of the iteration of m*n and obtain chaotic sequences as $X=x_1; x_2; x_3; :x_{m\,n}$
Step 4: The chaotic sequences X is sorted in ascending order and stores the index values into another variables index.
Step 5: According to the index values , one dimensional vector is permuted and converted back into matrix. Step 6:Get permuted image.

Level 3: Block Wise Diffusion Process

In this level, output of Level 2 image is divided into 16*16 macro blocks. For a each macro block a random integer number is mixed to shift the histogram of each block. This random integer number obtained from chaotic sequence according to following equation.

$$Rand_N o = Mod((chaotic\_sequence * (10^(14))), 256) \quad (4)$$

Level 4: Bit Plane Permutation

In order to increase the security of the proposed system. Output of Level 3 undergo bit plane permutation. As we now that each gray scale thermal image consists 8-bit planes. These 8-planes are divided into 8*8 blocks Between the blocks of bit planes, permutation operation can be done with the help of chaotic map.

Level 5: XOR operation

For the randomised distribution of pixel values,XOR operation performed between output of Level 4 and random image to get the thermal encrypted image.

Decryption is exact reverse process of encryption.

IV. PARAMETERS FOR THE EVALUATION OF AN PARTIAL IMAGE ENCRYPTION SCHEME

1)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:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \quad (5)$$

where X denotes the test image, x_i denotes the i^th possible value in X, and $Pr(x_i)$ is the probability of $X = x_i$, that is, the probability of pulling a random pixel in X and its value is xi.

For a truly random source emitting 2N symbols, the entropy is H(X)=N. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be H(X)=8. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

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. ?? [?].

$$MSE = \frac{1}{M * N} \sum_{i=1}^{N} \sum_{j=1}^{M} [c1(i,j) - c2(i,j)]^2 \quad (6)$$

where M, N is the width and height of digital images and C1(i,j) is input image and C2(i,j) is encrypted image.

B. Peak Signal to Noise Ratio (PSNR)

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

$$PSNR = 20 * \log_{10}\left[\frac{255}{MSE}\right] \quad (7)$$

Where MSE is mean square error between input image and encrypted image and can be calculated by using Eq. ??

C. 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) [?]. The equation to calculate UACI is Eq. ??.

$$UACI = \frac{1}{M * N}\sum_{i,j}\frac{|\,C1(i,j) - C2(i,j)\,|}{255} \times 100\% \quad (8)$$

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. ??.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (9)$$

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 II
RESULTS OBTAINED FROM HISTOGRAM DIFFUSING AND CHAOTIC MAP METHOD AND ENTROPY ANALYSIS

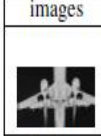
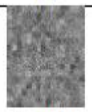
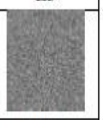
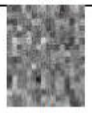
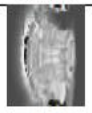
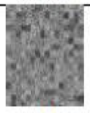
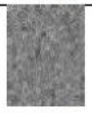
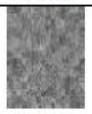
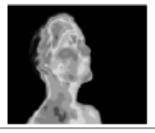
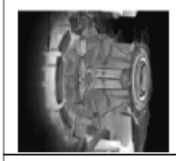
images	L1	L2	L3	L4	L5
					
5.623	5.623	5.623	7.9973	7.9907	7.9973
					
3.1090	3.1090	3.1090	7.9983	7.9944	7.9973
					
6.7992	6.7992	6.7992	7.9975	7.9969	7.9962
					
6.0891	6.0891	6.0891	7.9973	7.9944	7.997
					
7.2186	7.2186	7.2186	7.9970	7.9970	7.9968

TABLE III
PERFORMANCE PARAMETER ANALYSIS

Images	Levels	MSE	PSNR	NPCR	UACI
	L1	83.43	28.91	100	48.02
	L2	86.95	28.73	99.71	32.22
	L3	67.74	29.82	99.60	37.36
	L4	68.98	29.74	99.60	37.68
	L5	67.75	28.82	99.62	37.55
	L1	43.56	31.73	100	42.96
	L2	65.43	29.97	99.58	37.31
	L3	43.68	31.72	99.57	41.61
	L4	44.46	31.65	99.34	42.30
	L5	46.58	31.44	99.61	42.78
	L1	7.70	39.26	100	26.24
	L2	57.37	30.54	99.68	31.54
	L3	70.29	29.66	99.53	33.02
	L4	71.08	29.61	99.62	33.46
	L5	71.10	29.61	99.61	33.51
	L1	54.98	30.72	100	35.69
	L2	83.81	28.89	99.72	31.00
	L3	90.56	28.56	99.48	36.72
	L4	91.74	28.50	99.61	36.90
	L5	90.60	28.55	99.58	36.80

where C1(i,j) and C2(i,j) are the input and encrypted image respectively.

Table 2 gives the encrypted images for different input images at different levels. For each level encryption varies. entropy of each encryption level also varies.

Table 3 gives performance analysis of proposed thermal image encryption. Parameters like MSE, PSNR, NPCR, UACI varies at different encryption levels. Different levels of encryption gives the different parameter values.

V. CONCLUSION

Proposed algorithm involves 5-levels of encryption to enhance the security for thermal images. These Five level are 1)Histogram Diffusing 2) Pixel Permutation 3)Block wise Histogram Diffusing 4) Bit Plane Permutation 5) Diffusion Operation. At a different level, different encrypted images are obtained. Based the requirement of application they can select number of levels. when number of levels are increased security also increase. This type of algorithm resist brute force attack, differential attack and improves the security of the system.

REFERENCES

[1] G. Chen, et al., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals 21 (3) (2004) 749761.

[2] Y. Wang, et al., A new chaos-based fast image encryption algorithm, Appl. SoftComput. 11 (1) (2011) 514522.

[3] S. Lian, et al., A block cipher based on a suitable use of the chaotic standard map, Chaos Solitons Fractals 26 (1) (2005) 117129.

[4] Y. Mao, et al., A novel fast image encryption scheme based on 3D chaotic Baker maps, Int. J. Bifurc. Chaos 14 (10) (2004) 36133624.

[5] K.W. Wong, et al., A fast image encryption scheme based on chaotic standard map, Phys. Lett. A 372 (15) (2008) 26452652.

[6] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simul. 17 (7) (2012) 29432959, http://dx.doi.org/10.1016/j.cnsns.2011.11.030.

[7] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92(5) (2012) 12021215, http://dx.doi.org/10.1016/j.sigpro.2011.11.004.

[8] Yue Wu, Joseph P. Noonan, Shannon Entropy based Randomness Measurement and Test for Image Encryption Information Sciences 00 (2011) 123.

[9] Yue Wu, Joseph P. Noonan, and Sos Agaian, NPCR and UACI Ran-domness Tests for Image Encryption Cyber Journals:Multidisciplinary Journals in Science and Technology,Journal of Selected Areas in Tele communications (JSAT), April Edition, 2011.