International Journal of Engineering & Technology, 7 (3) (2018) 1948-1950

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.15880
Research paper

A Novel Partial Thermal Image Encryption Scheme Based on Multiple Chaotic Systems

Lokesh B S[1*] and Dr. M B Manjunatha[2]

[1] *Research Scholar, Jain University, Karnataka, India*
[2] *Principal, RRIT, Bangalore-Karnataka,India*
[*] *Corresponding author E-mail:lokesh.hosamane1@gmail.com*

Abstract

In this paper, proposed an novel partial encryption scheme for protecting thermal images during transmission. The adopted technique having pixel level and bit level permutation process. To reduce time and computational complexity , an partial encryption technique is adopted. Arnold cat map technique involved in the pixel level permutation process to decrease correlation of original image. The proposed scheme selects only higher four binary planes for the bit level shuffling process. Where this process consists of row and column wise circular shift operation with the help of pseudo random numbers generated from chaotic map system. Mixing of binary planes of the thermal image will leads to prevent the differential attacks. Experimental results shows that proposed scheme exhibits good performance in terms entropy, NPCR and the speed of system.

Keywords: *Arnold map,Chaotic map,encryption,thermal image.*

1. Introduction

Now a days fast growing of information and communication technologies, there are many ways of transmitting information from source to destination. While transmitting, securing of information is very important. Thermal image is one which requires security. Ciphering is one way to achieve security of thermal images.
Yueping etc. al[1] proposed a hyper chaos based image encryption algorithm. which consists of both pixel and bit level permutation process. where 5-D multi-wing hyper chaotic system enabled to generate key stream and pseudo random numbers.Chaos based expand and shrink techniques [2] applied for image encryption to increase the security. Multiple times of chaos based permutation technique applied to reduce the correlation among the pixels and substitution increases the entropy of encrypted image.Sukalyan Som etc.al [3] presents an chaos based partial image encryption scheme. Plain image decomposed to bit planes. in order to separate significant and insignificant bit planes threshold based autocorrelation techniques adapted. Anish Goel and Kaustubh Chaudhari[4] explained abut median based pixel selection for partial image encryption. Encrypted masks are used to select the pixels of interest and AES technique applied to each region of interest blocks to encrypt.Infrared target based selective encryption of thermal image proposed[5]. Which uses the chaotic maps for the encryption Contour model used to detect the infrared region. Next block cross model used for encrypting pixels of extracted infrared region of interest. Panduranga etc. al[6] introduced an partial image encryption scheme based on block wise shuffling and chaotic systems. plain image divided into non overlapping blocks of different size and pixels of each blocks gets permuted with the help of random sequence generated from the chaotic systems.Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh[7] explained about medical image encryption based on improved EIGamal algorithm. Separate encoding of plain message adopted and data expansion case is removed and that will enhance the execution speed of the system. Novel method for securing thermal images has been proposed [8]. proposed method depends on chebyshev chaotic map and s8 symmetric group of permutation based substitution boxes. Parameters to map are considered as the secrete key of the encryption system.

2. Chaotic Map

Selecting proper map has been one of the important stages in a digital chaotic. As far as the complexity is concerned, chaotic maps exhibit important characteristics such as, chaotic interval, cycle length, chaotic properties, periodic windows, etc. and it has highly sensitive to its initial conditions. There are instances where the weaknesses of the chaotic map were ignored and the systems suffered a breakdown. Hence there is necessity to design cryptosystems independent of the chaotic maps. That is, there is no necessity to possess complete knowledge of chosen chaotic map to make the good and efficient cryptosystem independent. In order to simplify the mathematics concepts, either logistic map or tent map can be used. Below equation represents the logistic map:

$$X_{n+1} = r * X_n * (1 - X_n) \quad (1)$$

Xn [0; 1] and r [3 : 57; 4] represent the primary values used by the logistic map chaotic signal.

Copyright © 2018 Author. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Proposed Partial Thermal Image Encryption

The following block diagram of proposed partial thermal image encryption scheme contain two processes namely

a. Pixel Level Permutation
b. Bit Level Permutation

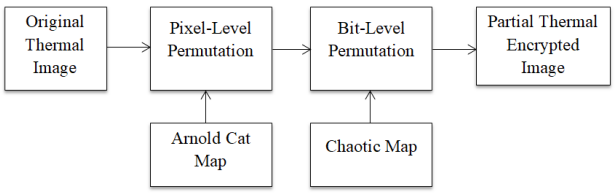

Figure 1: Block Diagram of Proposed Method

a. Pixel Level Permutation Process: Normally any two dimensional image having highly correlation with its adjacent pixels. For the better encryption we need to break the correlation property. For that a simple and effective pixel position manipulation technique called Arnold cat map involved. Arnold map permute the pixel position of original thermal image in random way by using following equation.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ c & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} ModN \tag{2}$$

where c and d are two positive integers.Parameters c,d, N can be considered as a secrete key of the proposed system. This cat map linearly permute the location of each pixel and reduce the correlation.

b. Bit Level Permutation Process: After pixel level permutation process, permuted thermal image obtained and these undergo bit level permutation process which selects only significant information of the image. As we all know that any grey scale image contains eight binary planes where the information distributed in specific way and around 93% of information concentrated only at higher 4 bit planes. Due to this fact only 4 bit planes are selected for the bit level permutation. Upper 4 bit planes are transformed into vector where higher bit planes are arranged from top to bottom and left to right fashion.
Given the initial conditions x0 and y0 and then updated by Eq. (1), we can get an iteration set
$X = x0, x1, x2, \ldots\ldots\ldots\ldots x_{m-1}$
$Y = y0, y1, y2, \ldots\ldots\ldots\ldots y_{4n-1}$
However, we should perform a preprocess for X and Y using Eq. (3) to transform into integers.

$$\begin{cases} Row_{int} = floor(mod(X*(10^{14})), m)+1 \\ Col_{int} = floor(mod(Y*(10^{14})), 4*n)+1 \end{cases} \tag{3}$$

for the permutation operation circular shifting of row and column of the image is considered. The first Row_int values are used for shifting the rows while the left Col_int values are used for shifting the cyclic. it means that we shift the first row with first element of Row_int units to the right and circulate in the left, the second row with second element of Row_int 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 1st column is moved with first element of Col_int units to the bottom and circulate at the top. The Entire permutation function is finished if every row and column is shifted. Then, we can obtain the Bit level permuted image. Finally combined the permuted 4 bit planes and other insignificant 4 bit planes to obtain partially encrypted thermal image.

4. Parameters for the evaluation of an partial thermal image encryption scheme

4.1. Information entropy analysis

Entropy defined as amount of information, which also indicates important characteristics of image disorder and randomness. Entropy H(X) of a source x, we have:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \tag{4}$$

Where X represents the image to testx_i denotes the i^th possible value in X, and Pr(x_i) is the probability of X =x_i. Theoretical value for H(X)=8 then it indicates that randomness of image is more and that will secure the input image [10].

4.2. Mean Square Error (MSE)

MSE can be calculated between input and encrypted image by taking mean of squared difference between them. MSE value more amount of nose introduced more and decreases signal strength. Let I1 and E1 are source image and cipher image respectively, then MSE given by Eq. 5 [11].

$$MSE = \frac{1}{h*w} \sum_{p=1}^{h} \sum_{q=1}^{w} [I1(i,j) - E1(i,j)]^2 \tag{5}$$

where h, w is row and column of picture and I1(p,q) is source image and E1(i,j) is cipher image.

4.3. Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio inversely pro- portional to Mean Square Error (MSE). PSNR re ects the ciphering quality. MSE is more PSNR is less and vice versa. PSNR value indicates how signal strength is more. Mathematically as in [11].

$$PSNR = 20*\log_{10}\left[\frac{255}{MSE}\right] \tag{6}$$

Where MSE is determined from using Equation 7.

4.4. UACI and NPCR

To check the proposed ciphering technique is sensitive to source image and keys, they are two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [9]. The equation to calculate UACI is Eq. 7.

$$UACI = \frac{1}{m*n} \sum_{p,q} \frac{|\, I(p,q) - E(p,q)\,|}{255} \times 100\% \tag{7}$$

Where, m represents number of rows, n indicates number of column, I(p,q) and E(p,q) are the original and cipher image respectively. NPCR can be calculated by Eq. 8.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{8}$$

Where, m represents number of rows, n indicates number of column and where D(i,j) defined as follows

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

where I(i,j) and E(i,j) are the original and cipher image respectively. Figure 2 shows the Plain images of MRI, Man, Hand and Legs respectively. Each image size of 256*256 and undergo permutation

Figure 2: Plain images of MRI, Man, Hand and Legs respectively (from left to right)

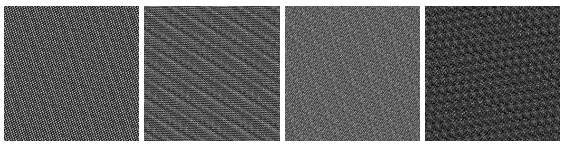

Figure 3: Permuted images of MRI, Man, Hand and Legs respectively (from left to right)

process with the help of Arnold cat map and obtained the permuted images of MRI, Man, Hand and Legs respectively as shown in figure 3. Figure 4 shows the encrypted images of MRI, Man, Hand and Legs respectively.

From the table 1, E1 and E2 are the entropy of original image and encrypted image respectively. It is observe that entropy of encrypted image is increased and approached to ideal value. Amount of encryption increases as the means square error value increases. Other Parameters are also increased and approached to ideal values. Because of encrypting only upper four bit planes of thermal image, encryption speed of the system increased.

5. Conclusion

Partial encryption technique for protecting thermal image have been proposed to reduce time and the computation complexity of traditional encryption algorithms. Arnold cat map technique involved in the pixel level permutation process. The proposed scheme selects only higher four binary planes for the bit level shuffling process. Where this process consists of row and column wise circular shift operation with the help of pseudo random numbers generated from chaotic map system. Proposed method can be adopted for practical image transmission due to its fast encryption speed and robustness against cryptanalytic attacks.

References

[1] Li Y, Wang C, Chen H. "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation". *Optics and Lasers in Engineering. 2017 Mar 1;90:238-46.*

[2] Naveenkumar SK, Panduranga HT, Kiran P." Chaos Based Image Encryption using Expand-Shrink Concept", *International Journal of Informatics and Communication Technology (IJ-ICT). 2014 Jul 7;3(2):103-12.*

[3] Som S, Kotal A, Mitra A, Palit S, Chaudhuri BB." A chaos based partial image encryption scheme", *InBusiness and Information Management (ICBIM), 2014 2nd International Conference on 2014 Jan 9 (pp. 58-63). IEEE.*

[4] Goel A, Chaudhari K." Median based pixel selection for partial image encryption", *InImage Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on 2016 Dec 12 (pp. 1-5). IEEE.*

[5] Wen W, Zhang Y, Fang Z, Chen JX. "Infrared target-based selective encryption by chaotic maps", *Optics Communications. 2015 Apr 15;341:131-9.*

[6] Panduranga HT, Naveenkumar SK. "Partial image encryption using block wise shuffling and chaotic map", *InOptical Imaging Sensor and Security (ICOSS), 2013 International Conference on 2013 Jul 2 (pp. 1-5). IEEE.*

[7] Laiphrakpam DS, Khumanthem MS. "Medical image encryption based on improved ElGamal encryption technique", *Optik-International Journal for Light and Electron Optics. 2017 Oct 1;147:88-102.*

[8] Hussain, Iqtadar, Amir Anees, and Abdulmohsen Algarni. "A novel algorithm for thermal image encryption", *Journal of integrative neuroscience Preprint (2018): 1-15.*

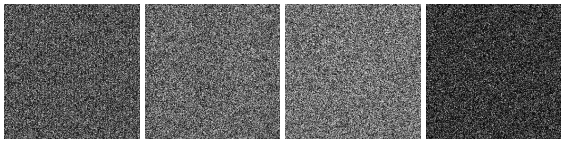

Figure 4: Encrypted images of MRI, Man, Hand and Legs respectively (from left to right)

Table 1: Performance analysis

Image	E1	E2	MSE	PSNR (DB)	NPCR(%)	UACI(%)
MRI	5.57	6.90	103.75	27.97	96.73	33.03
Man	3.10	4.13	46.26	31.47	38.69	12.05
Hands	7.21	7.92	102.71	28.01	99.54	29.39
Legs	4.87	6.02	91.06	28.53	91.13	28.98

[9] Wu Y, Noonan JP, Agaian S. "NPCR and UACI randomness tests for image encryption", *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT). 2011 Apr;1(2):31-8.*

[10] Wu Y, Noonan JP, Agaian S. "Shannon entropy based randomness measurement and test for image encryption", *arXiv preprint arXiv:1103.5520. 2011 Mar 29.*

[11] Jawad Ahmad and Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04.*