International Journal of Engineering & Technology, 7 (3) (2018) 1944-1947

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.15878
Research paper

Thermal Image Encryption Based on Region of Interest (ROI) and Chaotic map

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

Most of the thermal image information concentrated on a particular region and 50% of image information stored in Most Significant Bit (MSB) plane. Based on these two strategy, proposed an thermal image encryption based on region of interest (ROI) and chaotic map. Firstly extract the MSB bit plane of thermal input image. This MSB bit plane undergo ROI calculation method. This method involves the partition of MSB bit plane into several 16*16 blocks. Apply the thresholding function to each block to separate the ROI blocks. Then selected part from input thermal image undergo XOR operation between random image generated from chaotic map.For lossless decryption at the receiver side,embedded the index of ROI blocks using LSB embedding algorithm. Simulation results shows the proposed algorithm achieves good security and more efficiency.

Keywords: *Region of Interest (ROI), MSB bit plane, Thermal images , Encryption, Decryption.*

1. Introduction

Importance of thermal images are very high at different areas like power stations, product extraction of petroleum, labs of forensic and purification centres. In case of application to medical for analysis or diagnostic few deceases and also important while analysis the humans behaviour at different conditions of different levels. Recent development in the information and communication technologies, there are multiple way of sending information from one place to other.Due to these security need to provide to secure the information. Encryption of information can provides the security.
Bin wang et.al [1] described an general image encryption using chaotic maps. which consists of permutation and diffusion operations. Nidaa et.al [2] introduced an image encryption method based independent component analysis and arnolds cat map. Mixing matrix genereted from ACM by insert square image of any size. Encryption image depends on number o sources. C. Ibarra-Castanedo et.al [11] conversed pro- cessing of infrared picture and significance of Document picture (thermograms). Various techniques are discussed to process these infrared images. FrancescoAsdrubali et.al[3] proposed an thermal bonds exposing from thermographic pictures using image estimate algorithms.This method used to develop a steps for the contours detection of thermal bonds from pictures of thermographic. It consists of two steps. Firstly improvement of the thermographic images based on optimized version of the mathematical algorithm. which uses digital image processing based theory of sampling Kantorovich operators and the threshold method for examination of the histogram of the improved thermographic pictures.

W.T.Chan et.al [4] explained how thermal image proceesing used for optical character recognition. From this method, it can be concluded that, thermal images is not suitable for recognition of optical character due to variation in temperature and also overlapping of important parts which having heat signature.
ChanghangXu et.al[5] introduced framework based on infrared thermal image processing based on super-pixel algorithm. This algorithm detects the crack automatically. Two important algorithms of super pixels are compared and out of that any one method used to obtain super pixels in this proposed method. Hybrid the features of super pixels in order to choose pixels form raw data of image and image after passed through to high pass filter.
Henning Metzmacher et.al[6] concentrating on observation of temperatures of human skin. Main goal is to develop a common design for multi-modal fusion sensor data using a data structure of centralized server. which combining depth-map based pose and face tracking with a thermal imaging device.
WenyingWen et.al[7] conclude that many selective based image cipher schemes have been existed in the past. Many algorithms uses the concept of edge data as important information compared to regions of interest. Encryption of infrared images uses different logistic maps and block based approach.
LuXu et.al[8]describes binary level based image encryption algorithm which uses piece- wise linear chaotic maps (PWLCM). Initially the source image is converted into two binary array sequence of equal size, then novel diffusion technique applied to change the binary sequence values of two images mutually. changing of these elements can be controlled by chaotic map further it can be manipulate the bit values of current plane to any other plane.
YicongZhou et.al[9] described ciphering algorithm which consider the binary images planes of input picture as a password for securing it. changing the position of these binary image bit values to get

scrambled image.
Ignacio Bosch et.al [10] introduced an general approach for characterization of objects in infrared images. before apply image processing algorithm to input source image, first we need to detect combination of hotspots that gives objects of interest and then obtain the most important features to differentiating them. Many constraints are used to represent their characteristics mathematically such as fires, region of human that would be reduces the false occurring of alarm of pixel by pixel techniques.
Novel method for securing thermal images has been proposed [14]. 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.
Lokesh B S et.al [15] presented a novel thermal image encryption method which consists of backward binary to gray conversion and chaotic map. Encrypted thermal image can be genereted by applying backward binary to gray conversion along with XOR operation of pseudo random image obtained from chaotic map.
M B Manjunath et.al [16] proposed an thermal image encryption based on histogram diffusion and permutation using chaotic map. shifting of histogram can be done by adding random number. Chaotic map based permutation applied to obtain permuted image. Finally encrypted thermal image generated by applying XOR operation between permuted and random image.

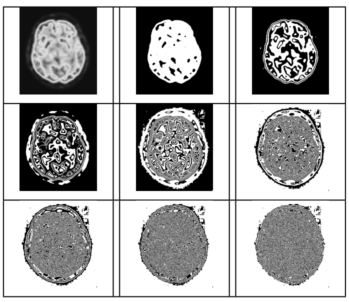
2. Bit Plane Slicing

Pixel value ranges in a gray scale image from 0 to 255. Every picture element 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.

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

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

Table 1: Bitplane Slicing



3. Chaotic Map

Important characteristics of chaos are so called "butterfly-effect". Pseudo random numbers generated form the logistic equation. In any image encryption, chaotic map is effective method used, because of its inherent behaviour like ergodicity, unpredictability, uncertainty and sensitivity to its initial conditions. The sensitivity to initial conditions means that, when a chaotic map is iteratively applied to two initially close points, the iterations quickly diverge, and become uncorrelated in the long term. Sensitivity to parameters causes the properties of the map to change quickly, when slightly perturbing the parameters, on which the map depends. Hence, a chaotic system can be used as a pseudo random number generator. Generally chaotic map control by two constraints X0 and μ. The control parameter μ range is [0,4], but it exhibits chaotic system when $\mu \in [3.5,4]$ and other parameter is initial condition value X0 $\in [0,1]$. The chaotic map equation as follows.

$$X(i+1) = \mu * X(i) * (1 - X(i)) \tag{2}$$

4. Proposed Method

System design of Proposed ROI based thermal image encryption as shown in Figure 1. The complete encryption process described in the following steps.

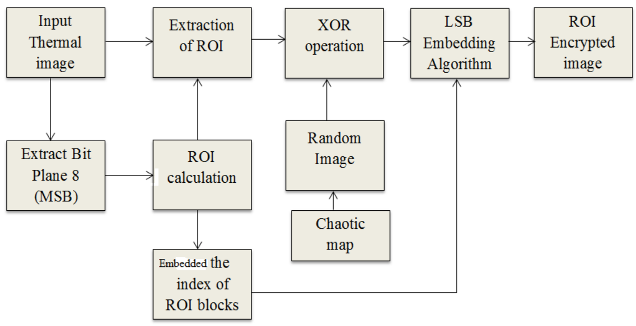


Figure 1: Block Diagram of Proposed Method

Step 1: Grayscale thermal image I of size p*q, where p indicates number of rows and q represents is number of columns.
Step 2: Extract the Bit plane 8 (MSB) of input thermal image I.
Step 3: Extracted MB plane divided into 16*16 macro blocks. Bi, where i=1,2,3......(m/16)*(n/16).
Step 4: Threshold function applied to each macro block and save the index of ROI blocks into the array P.

$$output = \begin{cases} ROIblock & if(sum(sum(Bi))) > (16*16/2)\} wherei = 1,2,3.. \\ 0 & otherwise \end{cases} \tag{3}$$

Step 5: Generate the random sequence X using Equation 2 with key X0 of length L=M*N. Obtained seqence maped into integer sequence [0,255] as follows.

$$J = mod((X * 10^14), 256) \tag{4}$$

and convert array into 2D matrix refereed as random image.
Step 6: Random image also divided to 16*16 macro blocks.Ri, i=1,2,3.........................(m/16)*(n/16).
Step 7: Perform Xor operation between ROI blocks and random blocks to get ROI encryted image.

$$Enc_i mage = XOR(Bi,Ri) wherei = 1,2,3...........(m/16)*(n/16) \tag{5}$$

Step 8: For the lossless decryption, we need to know the index of ROI blocks. So ROI blocks and total number of ROI blocks are embedded into LSB bit plane of thermal image using LSB algorithm.
Step 9: In LSB algorithm, convert the index values into binary numbers and this total number of bits are embedded into LSB bit

plane.
Step 10: Get the ROI encrypted image.

Deciphering is opposite operation of enciphering.

5. Parameters for the evaluation of an partial image encryption scheme

5.1. Histogram analysis

Histogram can be defined as discrete function by plotting number of pixels having grey level rk versus gray scale range. By using this parameter easily find the distribution of pixel values of input and encrypted image. Compared input image, encrypted image pixel values are uniformly distributed and gives no clues about original image.

5.2. 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:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \quad (6)$$

where X denotes the test image, denotes the 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.
Where X represents the image to testx_i denotes the $i^t h$ 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.

5.3. 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. 7 [12].

$$MSE = \frac{1}{h*w} \sum_{p=1}^{h} \sum_{q=1}^{w} [I1(i,j) - E1(i,j)]^2 \quad (7)$$

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

5.4. 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 [12].

$$PSNR = 20 * \log_{10} \left[\frac{255}{MSE} \right] \quad (8)$$

Where MSE is determined from using Eq. 7

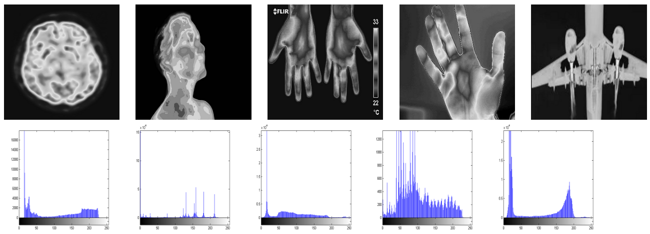


Figure 2: Plain images of Brain, Man, Hands, Hand, Legs and their histogram respectively from (left to right)

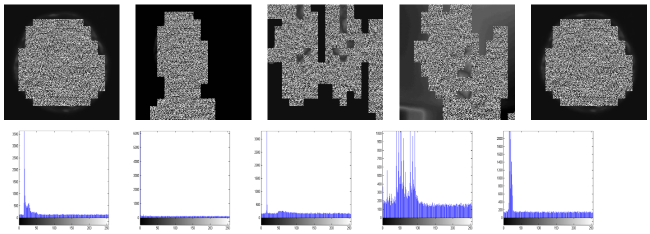


Figure 3: Encrypted images of Brain, Man, Hands, Hand, Legs and their histogram respectively from (left to right)

5.5. 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) [13]. The equation to calculate UACI is Eq. 9.

$$UACI = \frac{1}{m*n} \sum_{p,q} \frac{|I(p,q) - E(p,q)|}{255} \times 100\% \quad (9)$$

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. 10.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (10)$$

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

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

where I(i,j) and E(i,j) are the original and cipher image respectively.
Histograms of input thermal images and their encrypted images has been analysed. Fig. 2 gives the plain images of 'Brain', 'Man', 'Hands', 'Hand', 'Legs' and their histogram respectively. On the other hand,the encrypted images of 'Brain', 'Man', 'Hands', 'Hand', 'Legs' and their histogram respectively are illustrated in Fig. 3, respectively. It can be concluded that encrypted image histograms are almost uniformly distributed. As a result, the proposed algorithm can resist any statistical attack. From the performance analysis Table

Table 2: Performance analysis

Images	E1	E2	MSE	PSNR(DB)	NPCR(%)	UACI(%)
Brain	5.57	5.93	71.11	29.61	48.98	15.45
Man	3.10	4.13	46.26	31.47	38.69	12.05
Hands	4.91	6.32	42.59	31.83	63.13	21.04
Hand	7.21	7.50	67.82	29.81	58.61	16.87
Plane	5.62	6.49	63.67	30.09	53.98	17.35

3, entropy of encrypted thermal image increases compared to input image. Other parameters like MSE, PSNR, NPCR varies for different input thermal images.

6. Conclusion

Thermal image encryption based on Region of Intrest (ROI)has been proposed in this paper. Less number of work going in this field, because of only few researchers working on thermal image security. Proposed algorithm used the strategy of bit plane information and feature of thermal images. Region of interest (ROI) part selected from the MSB plane 8 and threshold function. Perform XOR operation between ROI of input blocks and blocks of random image generated from chaotic map. For the lossless decryption, embedded the index of ROI blocks sing LSB embedded algorithm. From the experimental result, we can conclude that complexity decreases and fast computation time.

References

[1] Bin Wang, Yingjie Xie, Changjun Zhou *Evaluating the permutation and diffusion operations used in imageencryption based on chaotic maps*,Optik 127 (2016) 3541–3545.

[2] Nidaa AbdulMohsin Abbas, *Image encryption based on Independent Component Analysis and Arnold's Cat Map*Egyptian Informatics Journal (2016) 17, 139–146.

[3] FrancescoAsdrubali , *Detection of thermal bridges from thermographic images by means of image processing approximation algorithms*.Applied Mathematics and Computation,Volume 317, 15 January 2018, Pages 160-171.

[4] W.T.Chan, *Application of optical character recognition in thermal image processing*,Infrared Physics & Technology,Volume 54, Issue 4, July 2011, Pages 353-366.

[5] ChanghangXu , *An infrared thermal image processing framework based on superpixel algorithm to detect cracks on metal surface*,Infrared Physics & Technology Volume 67, November 2014, Pages 266-272.

[6] Henning Metzmacher , *Real-time human skin temperature analysis using thermal image recognition for thermal comfort assessment*,Energy and Buildings elsevier journal.

[7] WenyingWen , *Infrared target-based selective encryption by chaotic maps*,Optics Communications Volume 341, 15 April 2015, Pages 131-139.

[8] LuXu, *A novel bit-level image encryption algorithm based on chaotic maps*, Optics and Lasers in Engineering, Volume 78, March 2016, Pages 17-25

[9] YicongZhou , *Image encryption using binary bitplane*,Signal Processing Volume 100, July 2014, Pages 197-207.

[10] Ignacio Bosch , *Object Discrimination by Infrared Image Processing*, springer, Bioinspired Applications in Artificial and Natural Computation pp 30-40.

[11] C. Ibarra-Castanedo, D. González, M. Klein, M. Pilla, S. Vallerand, X. Maldague, *Infrared image processing and data analysis*, Infrared Physics & Technology, Volume 46, Issues 1–2, December 2004, Pages 75–83.

[12] Yue Wu, Joseph P. Noonan, *Shannon Entropy based Randomness Measurement and Test for Image Encryption* Information Sciences 00 (2011) 1–23.

[13] Yue Wu, Joseph P. Noonan, and Sos Agaian, *NPCR and UACI Randomness Tests for Image Encryption* Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.

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

[15] Lokesh, B. S., M. B. Manjunatha, and H. T. Panduranga. "Novel Method for thermal image encryption." *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on. IEEE, 2015.*

[16] Lokesh, B. S., M. B. Manjunatha, "A Novel Thermal Image Encryption using Histogram Diffusion and Chaos Map", *Elixir Elec. Engg. 116 (2018) 50013-50016.*