ISSN:0975-9646

Rakhi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2204-2207

Partial Image Encryption Using Block Shuffling and Affine Transform

Rakhi
M. Tech,CSE
Dept. of CSE, LNCT College
BHOPAL, MP, INDIA

Rekha Pandit
Assistant Professor
Dept. of CSE, LNCT College
BHOPAL, MP, INDIA

Abstract-Information security becomes important with the immense growth of internet applications. The information that is transmitted on the network is more in the form of text, audio, vedio and image. An image has larger amount of data, higher redundancy and stronger correlation between pixels. Security of these pixels becomes crucial. Image encryption is used to protect and transform images into various forms. Some applications like SCAN based technique perform total encryption and consume a lot of computational time. However, some applications like Pay-TV do not require total encryption. This paper presents a Partial Image Encryption based on Block Shuffling using Affine Transform. Original image is divided into blocks and then the block positions are permuted using affine transform. Partially encrypted images are attained by selecting the different block size. Decryption follows the reverse process of encryption.

Keywords-Partial Encryption, Affine Transform, Encryption, Decryption.

INTRODUCTION-

The rapid growth of technology a lot of sensitive data are transmitted over the network. To protect this data from unauthorized access information security becomes extremely important in data storage and transmission. **Parameshchari B D,Dr. K M Sunjiv Soyjaudah,Dr. Sumitha Devi K A** in this paper they presented a novel solution for partial encryption to achieve data protection, confidentiality and integrity effectively. They proposed a partial image encryption using Single bit manipulation technique, it convert each byte/character of the message to be encrypted to its binary equivalent. Now length of password is considered for bit left shift i.e., Number of bits to be shifted to left will be decided by the length of password [1]. **Panduranga H T , NaveenKumar S K** they proposed a selective image encryption in two ways Firstly divide the image in two sub blocks, then these selected blocks are applied to encryption process, in the second method automatically detects the position of the objects , and then selected objects are applied to encryption process[2].**Marc Van Droogenbroeck and Raphaël Benedett,** presented a selective encryption of compressed image and they used JPEG compression, the Huffman code aggregates zero coefficients into runs of zeros and uses symbols that combine the run of zeros with magnitude categories for the non-zero coefficients that terminate the runs. These symbols are assigned 8-bit code words by the Huffman coder. The code words precede the appended bits that specify the sign and magnitude of the nonzero coefficients. In the proposed scheme, the appended bits corresponding to a selected number of AC coefficients are encrypted. The DC coefficients are left unencrypted because, it is argued, they carry important visible information and are highly predictable [3].**Sukalyan Som ,Atanu Kotal,Abhijit Mitra,Sarbani Patil,B.B. Chaudhari** They proposed a chaos based symmetric key partial encryption of gray level images. In this algorithm, the plain images after decomposing them to bit planes are classified into different categories. A threshold based on the autocorrelation of blocks of different bit planes is used to identify the significant and insignificant bit planes. Then the correlated bit planes of an image are encrypted with key stream sequences generated by a chaos based pseudo random binary number generator [4].**Tao Xiang et.al** most existing selective image encryption schemes are designed based on image compression algorithms, and thus they are codec specific. As different bit planes of an image contribute differently to visualization effect, a selective gray-level image encryption scheme is proposed in this paper. In this scheme, only a portion of significant bits of each pixel is encrypted by the key stream generated from a one-way coupled map lattice that exhibits good chaotic dynamics even after discretization[5].**Panduranga H T ,Dr. Naveen Kumar S K ,Kiran** they describe a partial image encryption based on block wise shuffling using chaotic map.In this method pixel positions are shuffled within the block by using chaotic map[6]. **S. Fong-In, S. Kiattisin, and A. Leelasantitham,W. San-Umin** In their method they presents a partial encryption scheme using absolute-value chaotic map for secure electronic health records(EHR)[7].

The remaining paper is organized as follows(II)briefly explains the concept of Affine Transform.(III)described the proposed partial image encryption technique algorithm(IV)security of the scheme is evaluated.(V)shows the experimental results.(VI)Conclusion.

(II)AFFINE TRANSFORM

The affine transform cracks the correlation between adjacent pixels of an image[8]. Affine transform is one to one mapping, i.e. a symbol in the plain text can be altering to a unique symbol in the cipher text.The relationship between plain text and cipher text is given as follow:-

$$C = (K_0 + K_1 \times P) \bmod N$$

$$P = (C + (-K_0) \times K_1^{-1}) \bmod N$$

Where $\gcd(k_1 , N)=1$, K_1^{-1} is the multiplicative inverse of K_1 and $(-K_0)$ is the additive inverse of k_0.

(III)PROPOSED PARTIAL ENCRYPTION TECHNIQUE

Block diagram of partial image encryption using block shuffling and Affine Transform is shown in figure 1.There is a input image of size n x n and initially block size is of 4 X 4 .Input image is divided into several 4 X 4 blocks and the positions of these blocks is shuffled using Affine Transform to get a partially encrypted image ,in order to find different partially encrypted images we select different block size from the block size list table shown in table 1 and each time previous partially encrypted image is act as a input image .

Table 1

Block size
4 × 4
8 × 8
16 × 16
32 × 32
.
.
.
n/2 × n/2

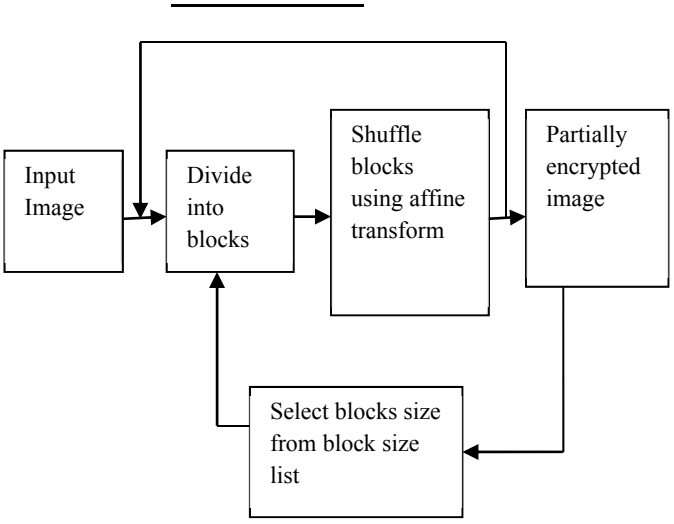


Figure 1

Encryption Algorithm-

Input- A 256 gray level secret plain image S of size M X N and a 32 – bits Secret key.

Output- A 256 gray level cipher image C of size N X N.

Step 1 Split 32-bit secret key into four sub-keys k_0,k_1,k_2 and k_3.

Step 2 Decompose secret plain image S into several blocks according to block size from block size list.

Step 3 For each block B(i , j) transform the location (i , j) in S to (i' ,j') in C using the formula

$$i'=(k_0 + k_1 \times i) \bmod M$$
$$j'=(k_2 + k_3 \times j) \bmod N$$

Step 4 Combined all the blocks into an image.

Step 5 Repeat step 2 again and again for next block size until the block size becomes M/2 × N/2 number of 2 × 2 blocks.

Step 6 END.

Plain Image

Decryption Algorithm-

Input- A M X N cipher image C and a 32-bit symmetric key.

Output- A M X N secret plain image S of size M × N.

Step 1 Split 32-bits secret key into four sub keys k_0, k_1, K_2 and k_3.

Step 2 Decompose C into M/2 × N/2 number of 2 × 2 blocks.

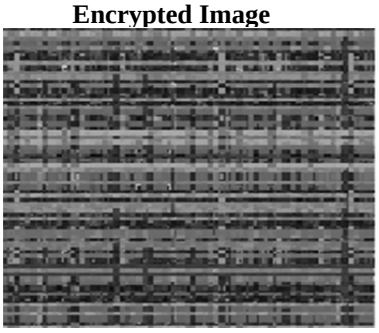
Step 3 For each block B(I', j') transform the location (I', j') in C to (I ,j) in S using the formula

$$i=(I' + (-k_0) \times k_1^{-1}) \bmod M$$
$$j=(j' + (-k_2) \times k_3^{-1}) \bmod N$$

Step 4 Repeat the step 2 again and again for next block size taken from the block size list bottom to top until the block size becomes 4 X 4 .

Step 5 END.

Encrypted Image



(IV)PARAMETERS FOR THE EVALUATION OF AN PARTIAL IMAGE ENCRYPTION TECHNIQUE-

(1)**Mean Square Error(MSE)**-Mean Squared Error is the average squared difference between a reference image and a distorted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

For images A = $\{a_1 \ldots a_M\}$ and B = $\{b_1 .. b_M\}$, where M is the number of pixels:

$$MSE(A,B) = 1/M \sum_{i=1}^{M} (a_i - b_i)^2$$

(2)**Peak Signal to Noise Ratio(PSNR)-** Peak Signal-to-Noise Ratio is the ratio between the reference signal and the distortion signal in an image, given in decibels. The

higher the PSNR, the closer the distorted image is to the original. In general, a higher PSNR value should correlate to a higher quality image, but tests have shown that this isn't always the case. However, PSNR is a popular quality metric because it's easy and fast to calculate while still giving okay results.
For images A = {a1 .. aM}, B = {b1 .. bM}, and MAX equal to the maximum possible pixel value (2^8 - 1 = 255 for 8-bit images):

$$PSNR(A,B) = 10\log_{10}(\frac{MAX^2}{MSE(A,B)})$$

(3)UACI and NPCR-In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys. Two tests are bring out in this paper Number of Pixel Change Rate and Unified Average Changing Intensity. NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image. Suppose ciphertext images before and after one pixel change in a plaintext image are C1 and C2 , respectively; the pixel value at grid(i , j) in C1 and C2 are denoted as c1(i , j)and C2(i , j) ; and a bipolar array D is defined in Eqn. (1). Then the NPCR and UACI can be mathematically defined by Eqns. (2) and (3), respectively, where symbol T denotes the total number pixels in the ciphertext, symbol F denotes the largest supported pixel value compatible with the ciphertext image format.

D(i, j) = {0, if(C1(i, j)=C2(i,j))
1,if(C1(i,j)≠C2(i,j)) ……(1)

NPCR:

N(C1,C2)= $\sum_{i,j} \frac{D(i,j)}{T} \times 100\%$ …….(2)

UACI:

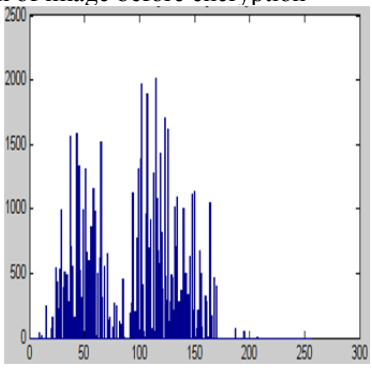
U(C1,C2)=$\sum_{i,j} | C1(i,j) - C2(i,j) |/(F.T)\times 100\%$… (3)

(IV)RESULT ANALYSIS

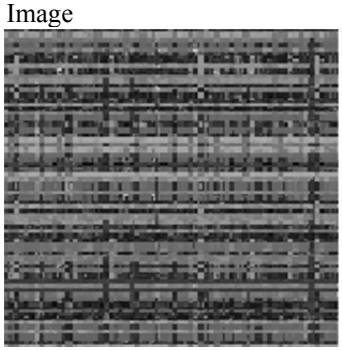
Histogram Analysis-A histogram is the most commonly used graph to show frequency distributions. It is a graphical representation of the distributed data. To plot the density of the data Histogram is used.

(i)Image

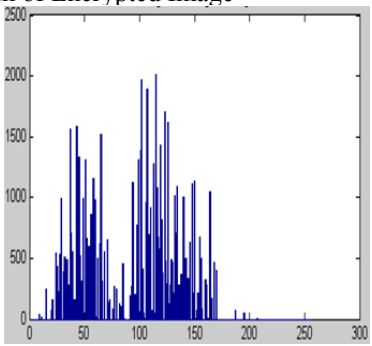
(ii)Histogram of image before encryption



(iii)Encrypted Image



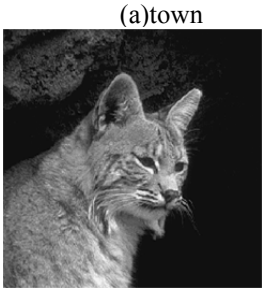
(iv)Histogram of Encrypted Image



(v)Results Obtained from the proposed method-

(a)town

(b)Airplane



(c)Animal

(d) Lena

Image Name	MSE	PSNR	NPCR	UACI
(a)town	3085.0512	26.5527	98.5016	0.24261
(b)Airplane	4086.1268	24.0354	98.4589	2.7115
(c)Animal	6552.8776	19.933	86.3602	7.1442
(d)Lena	5695.3761	21.1512	99.4827	4.731

(VI)CONCLUTION-

In this paper we proposed partial image encryption using block shuffling and Affine Transformation. A symmetric key image encryption technique is proposed in which the original image is divided into blocks and the block positions are scramble using the four 8-bit sub-keys.The encryption and decryption process are simple enough for large sized image. This technique can be very helpful in various applications where partial encryption is required.

REFERENCE-

[1] Parameshchari B D,Dr. K M Sunjiv Soyjaudah,Dr. Sumitha Devi K A,"Secure Transmission of an Image using Partial image encryption based Algorithm",International Journal of Computer Applications(975-8887),Vol. 63,no.16,February 2013.

[2] Panduranga H T , NaveenKumar S K ," Selective image encryption for Medical and Satellite Images", Panduranga H T et al. / International Journal of Engineering and Technology (IJET), Vol 5 No 1 Feb-Mar 2013.

[3] Marc Van Droogenbroeck and Raphaël Benedett, Techniques for a selective encryption of uncompressed and compressed images,Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 9-11, 2002.

[4] Sukalyan Som ,Atanu Kotal,Abhijit Mitra,Sarbani Patil,B.B. Chaudhari,"A Non-adaptive Partial Encryption of Grayscale Image based on Chaos",First international conference on Computational Intelligence:Modelling ,Techniques and applications(CIMTA-2013).

[5] Tao Xiang, Kwok-wo Wong, and Xiaofeng Liao, Selective image encryption using a spatiotemporal chaotic system, American Instituteof Physics 2007.

[6] Panduranga H T , NaveenKumar S K,kiran,"Partial Image Encryption Using Block Wise Shuffling and Chaotic Map",Proceedings of International Conference onOptical Imaging Sensor and Security,Coimbatore,Tamil Nadu,India,July 2-3,2013.

[7] S. Fong-In, S. Kiattisin, and A. Leelasantitham,W. San-Um,"A Partial Encryption Scheme UsingAbsolute-Value Chaotic Map for Secure Electronic Health Records",JICTEE-2014.

[8] Amitava Nag ,Sushant Biswas,"Image Encryption Using Affine Transform and XOR Operation",proceedings of 2011 International conference on Signal Processing,Communication Computing and Networking Technologies(ICSCCN 2011).