Partial Image Encryption based on Block wise Shuffling using Arnold Map

Nilesh Y. Choudhary
M-TECH (CSE)
RKDF IST, Bhopal India

Ravindra K. Gupta
RKDF IST, Bhopal India

ABSTRACT
To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .The Fully image encryption techniques is very complex in nature and takes a lot of computational time. But, certain applications do not require total encryption; it requires a part of the multimedia data to be transparent to all users, like Pay-TV or Payable Internet Imaging Albums which involves encrypting the most meaningful parts of an image. In this paper we focus on a partial image encryption technique based on block wise shuffling with the help of Arnold map .Firstly image is divided into blocks then Blocks within the image are permuted by using Arnold map and final permuted block are combined that yields partial encrypted images . This process is repeated for different block size. The PSNR and NPCR obtained by our technique shows that the proposed technique gives better result than the existing techniques.

General Terms
Partial Image Encryption, Arnold map, NPCR MSE Logistic map

1. INTRODUCTION
Due to low cost and high availability of digital data, the communication network usage has increased and because of the rapid growth of the internet, the security of digital images has become more important and attracted much attention in the digital world today. The generality of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of user's privacy for all applications. A digital image is defined as a two dimensional rectangle array. and the elements of that array are denoted as pixels So We can say that Images are the collection of pixels. And image Encryption is a technique to convert the image into unreadable format [1].

Many digital services require reliable security in storage and transmission of digital images .To prevent image from unauthorized access, Encryption techniques of digital images play a very important role .Since Digital images are exchanged over various types of networks and a large part of this digital information is either confidential or private. So Encryption is the preferred technique for protecting the transmitting information. But, the huge size, complex structure and statistical properties of digital images make the computational overhead and processing time involved during encryption and decryption a major bottleneck, especially for real time applications [2].

Several encryption schemes have been proposed with respect to the approach in construction for both storage and transmission domains, which are generally categorized into full encryption and selective (or partial) encryption schemes. Encryption operation involves implementing encryption methods to entire or partial image information using either standard block ciphers like AES, DES, etc., or using stream ciphers. Furthermore, several random position per- mutation algorithms and chaotic based cryptosystems have been used to encrypt entire or partial image data [3].

Selective image encryption is a current research trend being investigated to minimize the encryption time of digital images. It does not strive for maximum security, but trades off security for computational complexity. It involves representing the most meaningful parts of an image. Consequently, the encryption process is carried out on the most significant bits, pixels or blocks using three major encryption techniques: value substitution, scrambling positions, or a combination.

In 2002, Marc Van Droogenbroeck and Raphal Benedett, [4] proposed a selective encryption for compressed image that utilized JPEG compression. In JPEG, the Huffman coder aggregates zero coefficients into runs of zeros. In order to approach the entropy, it also 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.

In 2005, Roman Pfarrhofer and Andreas Uhl [5] explained the concept partial encryption for the gray scale image. In this technique first of all gray scale image is decomposed into its 8 bit planes and then the most significant bit planes are encrypted. Simulation result of this technique shows that the encryption of the 4 most significant bit plane is not secure enough.however selectively encrypting 2 bit planes is sufficient if severe alienation of the image data is acceptable, if encryption is done for 4 bit planes then provides high confidentiality.

Tao Xiang et.al [6] proposed a universal selective gray level image encryption algorithm in 2007, where the spatiotemporal chaotic system is utilized. the effectiveness of selective encryption is analyzed based on simulation result that resolve the tradeoff between security and performance. This scheme is then extended to encrypt RGB color images. Result analyses for both scenarios show that the proposed schemes achieve high security and efficiency.

In 2008, Nidhi et.al [7], proposed a selective encryption technique in wavelet domain for conditional access systems. In this technique encryption is applied only to a subset of multimedia data stream rather than the multimedia data in its entirety .it save the computational time and computational resources because of partial encryption. So it controls the transparency of the multimedia data at the time of encryption.

In 2008, Zahia Brahimi et.al [8] presented novel selective encryption image schemes based on JPEG2000. In this technique first encrypts only that codeblocks which corresponds to some sensitive precincts. And then to improve the security level codeblocks are permuted contributing in the selected precincts. To minimize the amount of processed encrypted data while

ensuring the best possible degradation through the permutation, the idea of combining permutation and selective encryption is used. This method doesn't introduce superfluous JPEG2000 markers in the protected code stream.

In 2012 Priyanka Agrawal and Manisha Rajpoot [9] explained a concept where some part of the image are efficiently encrypted by selecting the part of the image which is further used in its normal mode of operation for encryption. After the encryption, the encrypted data is sent along with remaining original part of the message .The main concept behind this work is to select the part of the image by the arranging the bit stream in grid form and choosing the diagonal of the grid. This technique deals with a partial image encryption algorithm of images to reduce energy consumption for encryption of the large volume visual data in many different areas such as mobile phone services, wireless networking, and applications in homeland security .

In same year Gaurav Bhatnagar et.al. [10] Also proposed efficient and simple selective encryption technique that is based on pixels of interest and singular value decomposition. In this technique pixel position is scrambled with the help of Saw-Tooth space filling curve followed by the selection of significant pixels using pixels of interest method. After that the diffusion process is applied on the significant pixels using a secret image key obtained from non-linear chaotic map and singular value decomposition. At last reliable decryption process is used to construct original image from the encrypted image. Simulation results show that the proposed scheme can achieve various purposes of selective encryption and is computationally secure.

In 2013 H T Panduranga et.al. [11] Presents a partial image encryption based on block wise shuffling with the help of chaotic map. Pixels positions are permuted within the block by using chaotic map. Partial encrypted images are obtained by selecting the different block size. The MSE and NPCR comparison of proposed technique with the existing encryption techniques shows that the proposed technique gives better security than the existing techniques..

Selective encryption can also be applied to the DCT coefficients during the vector quantization phase .Moreover, encryption can also be combined with the entropy-coding phase into a single step ,and hence reduce the computational time, and maintain format compliance and compression rates.

We have proposed an hybrid approach that involves permutation of blocks within the image according to Arnold map.in this technique firstly image is divided into blocks then Blocks within the image are permuted by using Arnold map and and then permuted block are combined that yields Permuted images

. This process is repeated for different block size. And finally get the partially encrypted image. The rest of this paper is organized as follows. Section II briefly explains the concept of Arnold map. Section III describes the proposed partial encryption algorithms. The evaluation parameter is described in Section IV. Experimental results described in section V. Section VI conclude the paper.

2. ARNOLD TRANSFORM

Arnold transform is used widely in information hiding technology. However it can also be used for image encryption. Arnold transform has periodicity and periodicity depends on image size. Arnold transform is simple. Arnold transform, also called cat map transform, is only suitable for encrypting N×N images. It is defined as [12].

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N$$

Some conditions for the map is that p and q are positive integers and

$$\det \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} = 1$$

This makes the map area-preserving. Here N is the size of the image. In our system we choose the value of p and q is equal to 1.so our cat map would be

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \qquad (1)$$

Where (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image, respectively. Let A denote the left matrix in the right part of equation (1), I(x, y)k and I(x', y')k represent pixels in the original image and the encrypted image obtained by performing Arnold transform k times, respectively. Thus, image encryption using k times Arnold transforms [12] can be written as.

$$I(x', y')^K = AI(x, y)^{k-1} (\mathrm{mod}\, N)$$

Where k = 1, 2, … , n, and $I(x', y')^0 = I(x, y)$. Obviously, one can multiply the inverse matrix of A at each side of equation (2) to obtain $I(x, y)^{k-1}$. In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times.

$$J(x, y)^k = A^{-1} J(x', y')^{k-1} (\mathrm{mod}\, N)$$

Where $J(x', y')^0$ is a pixel of the encrypted image, and $J(x, y)^k$ is a decrypted pixel by performing k iterations. We can rewrite equation above as

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \mod N \qquad (2)$$

3. PROPOSED IMAGE ENCRYPTION SCHEME

3.1 Encryption Algorithm

Image Encryption process of a given image is divided in to the following steps.

I. Firstly we select a gray scale image X of N×N pixel size with L bit per pixel.

II. Next step of proposed image encryption method based on decomposition of the input gray image X into blocks of B*B; initially the size of B is 4 and next time it is multiply by 2 and increased up to N/2*N/2.

III. Next step is to applying Arnold Transformation on every block of decomposed image with the help of equation 1 up to Arnold key which is calculate on the basis of Block size. Equation 1 is used to transform each and every block coordinates of the image. When all the coordinates are transformed, the image we obtain is a encrypted image. At a certain step of iterations, if the image we achieve reaches our anticipated target (i.e. up to secret key), we have achieved the scrambled image we wanted to. The decryption of image relies on the transformation periods (i.e. the number of iteration to be followed = Arnold's period – secret key).

IV. Combined all the permuted blocks to make an image that referred as permuted image. And this permuted image works as input image for next time.
V. Repeat steps from II to IV for next block size until block size reached up to N/2 *N/2 .
VI. Finally we get the partial encrypted image. And this image is ready to transmit.

3.2 DecryptionAlgorithm

A Reverse process of encrypted image is called as image decryption. Decryption is also systematic or step-by-step procedure to convert cipher image into original image (encrypted image). The decryption process is divided into different steps.

I. The input is a gray scale encrypted image Y of N×N pixel size with L bit per pixel.
II. Second step of proposed image encryption method based on decomposed of the input gray image Encrypted image Y into blocks of B*B; initially the size of B is n/2 and next time it is divided by 2 and decreased up to 4*4.
III. The Next step is to applying anti scrambling on each and every encrypted image Blocks. The decryption is achieved by applying Inverse Arnold transformation to the encrypted image block. The corresponding two dimensional Inverse Arnold transformation matrix is define in equation 2.
IV. Combined all the blocks into an image .And this intermediate image works as input for next time.
V. Repeat steps from II to IV for next block size until block size reached down to 4*4 .
VI. After antiscrambling has been done by using Anti-Arnold's Transformation, the resultant image is the original decrypted image.

Figure 1 shows block diagram of proposed method.

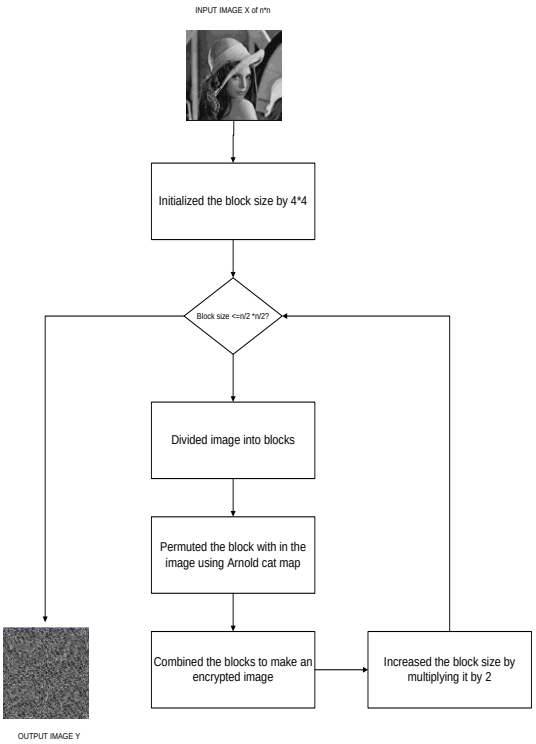


Fig. 1. **Block Diagram of proposed method**

Fig. 2.

4. EVALUATION METRICS

In this investigation, the set of criteria for comparing the selected algorithms are: the MSE, PSNR, UAIC NPCR and IQI.

4.1 Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [13] can be defined as the measure of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-C'(i,j))^2$$

Where C(i, j) is the original image and C' (i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

4.2 Peak signal to noise ratio (PSNR)

The PSNR depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR = 20\log 255^2 / MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

4.3 UAIC and NPCR

Attacker tries to find out a relationship between the plain image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Trying to make a slight change such as modifying one pixel of the encrypted image, attacker observes the change of the plain-image. To test the influence of one pixel change on the whole encrypted image by the proposed algorithm, two common measures are used [14]:

Number of Pixel Change Rate (NPCR)

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

Unified Average Change Intensity (UACI)

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times 100\%$$

C1 and C2: two ciphered images, whose corresponding original images have only one-pixel difference. C1 and C2 have the same size.

C1(i, j) and C2(i, j): grey-scale values of the pixels at grid (i,j).

D(i, j): determined by C1(i, j) and C2(i, j), if C1(i, j) = C2(i,j), then, D(i, j) = 1; otherwise, D(i, j) = 0.W and H: columns and rows of the image.

4.4 Universal Image Quality Index (UIQ)

The UIQ indicates the structural similarity between two images. The UIQ lies between [-1, 1] and the value closer to 1, the greater similarity in the images. Mathematically, UIQ is defined as in [15].

$$Q = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \cdot \frac{2\mu_x \mu_y}{\mu_x^2 + \mu_y^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2}$$

Where μ_x , μ_y , σ_x , σ_y and σ_{xy} are the mean of x & y, variance x & y and the covariance of x and y respectively.

5. SIMULATION RESULT

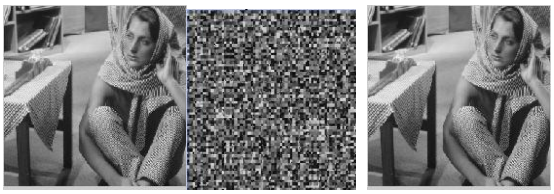
In the experiment, we do partial image encryption using Arnold cat map and we are taken different images of size 512× 512 shown in Figure 2.

(a) (b) (c)

Fig. 3. Test Images (a)Lena (b)Baby in womb(c)Plane

To demonstrate our method we used the gray image Lena as Shown in Figure 3(a), the results are shown as in Figure 3(b). The block shuffling effect is very good and the encrypted image is very like the salt and paper noise. Figure 3(c) is the result of decryption, comparing with original image as shown in Figure 3(a), there is nothing to be lost.

Figure 4(a) is the histogram of original image Lena. Figure 4(b)is the histogram of the encrypted image permuted by the proposed method .fig 4 shows that the histogram of the both image are same so we can say that in encrypted image all the gray value remain same only it permuted within the image.



(a) (b) (c)

Fig. 4. **Results after image encryption and Decryption system for Lena**.

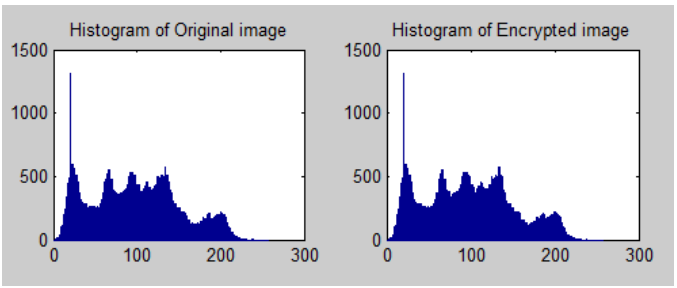


Fig. 5. **Histograms of the image Encryption and Decryption system for Lena**

TABLE I. Shows average Correlation between pixel values and compare different image Encryption Methods.

	Method[11]					Proposed Method				
Parameter Image	MSE	PSNR	NPCR	UACI	UIQ	MSE	PSNR	NPCR	UACI	UIQ
Leena	**5575.067**	**21.3366**	**99.2805**	4.3091	0.7497	106.5086	27.8570	99.1535	19.7049	0.0857
Baby in Womb	**5946.1824**	**20.7768**	**99.6302**	6.9813	0.69863	47.1727	31.3939	99.6265	29.2180	0.0626
Plane	**1943.6871**	30.4891	98.2216	0.64049	0.9526	130.9438	26.9600	99.2329	19.1658	0.1054

The Average quality parameters between the corresponding pixels values of the three encrypted images Lena, Baby in Womb and plane are tabulated in Table I, from which it can be said that the PSNR and NPCR are better than that obtained using the method [11]. Results of MSE and NPCR values are greatly increased compared to existing method results in Table II

6. CONCLUSION

In this paper we proposed a partial image encryption technique based on block wise shuffling with the help of Arnold map. Periodicity of Arnold map depends on image size. Images are permuted by using Arnold map and permuted block are combined that yields partial encrypted images. This process is repeated for different block size. The encryption and decryption process are simple enough to be carried out on any large sized image, but provides enough security. We have designed our image Encryption and Decryption System using Matlab 7.8.0 to accomplish this research work. We have evaluated our proposed image Encryption and Decryption System on gray Scale image of 512*512. The experimental result proved that Correlation between pixel values are significantly decreased. The PSNR and NPCR obtained by our technique shows that the proposed technique gives better result than the existing techniques. We will future investigate in our proposed algorithm also can be applying to color image.

7. REFERENCES

[1] I. Öztürk and I. Sogukpınar, "Analysis and comparison of image encryption algorithms", Transactions on Engineering, Computing and Technology, vol. 3, pp. 1305-5313, 2004.

[2] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[3] Osama A. KHASHAN, Abdullah M. ZIN, Elankovan SUNDARARAJAN," Performance study of selective encryption in comparison to full encryption for still visual images" Journal of Zhejiang University-SCIENCE C (Computers & Electronics),2014.

[4] Marc Van Droogenbroeck and Raphal 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

[5] Roman Pfarrhofer and Andreas Uhl, Selective Image Encryption Using JBIG, IFIP International Federation for Information Processing 2005.

[6] Tao Xiang, Kwok-wo Wong, and Xiaofeng Liao, Selective image en- cryption using a spatiotemporal chaotic system, American Institute of Physics 2007.

[7] Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, Selective encryption of multimedia images, NSC 2008, December 17-19, 2008.

[8] Zahia Brahimi, Hamid Bessalah, A. Tarabet, M. K. Kholladi, Selective Encryption Techniques of JPEG2000 Codestream for Medical Images Transmission, WSEAS Transactions on Circuits and Systems Issue 7, Volume 7, July 2008 .

[9] Priyanka Agrawal and Manisha Rajpoot, A Fast and Secure Selective Encryption Scheme using Grid Division Method, IJCA vol.51 no.4,pp29-33, Aug -2012.

[10] Gaurav Bhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648663.

[11] Panduranga H T, Dr.Naveenkumar S K, Kiran," Partial Image Encryption using block wise shuffling and chaotic map", Proceedings of International Conference on Optical Imaging Sensor and Security, Coimbatore, Tamil Nadu, India, July 2-3, 2013.

[12] W. Ding, W. Q. Yan, D. X. Qi, "Digital Image Scrambling Technology Based on Arnold Transformation " .

[13] 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.

[14] 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 Telecommunications (JSAT), April Edition, 2011.

[15] Zhou Wang, Alan C. Bovik, A universal image quality index, IEEE signal processing Letters, Vol. xx, No, Y, March 2002.