Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Block Based Image Encryption Using Iterative Arnold Transformation

Pavan Kumar Goswami, Namita Tiwari, Meenu Chawla
Dept of CSE, MANIT BHOPAL
India

Abstract*— Encryption process prevents the image data from unauthorized user. The primary goal of this paper is security management. This will provide integrity, accuracy and safety of image which is travelling over Internet. Researchers have proposed incompatible method to encrypt image but correlation between pixels play desperate roll for original image. So, here we introduce new architecture for image encryption and decryption using block based image encryption using iterative Arnold transformation. The proposed method in this paper increases the entropy and reduces the correlation by using block shuffling and encryption using iterative Arnold transformation. First the plain image divides into blocks. All these blocks are then shuffled using proposed technique which work on the row wise block shuffling and column wise block shuffling then shuffled image is then encrypted using transformation .It provides the keyless framework for image encryption.

Keywords*— Image encryption, Shuffling, Security, Accuracy, Transformation, Encryption, Arnold transformation, Block shuffled image, Keyless encryption.

I. INTRODUCTION

Technology has changed the world dramatically. Last few decades have witnessed, some great events, especially in the field of digital communication Internet has shrunk the world. Whole world has becomes a global village. It's very easy to access the information as well as data. Need of the communication network usage has increased, sharing the data over open network is also rising. To prevent the data from unauthorized access, encryption technique is widely used. Encryption the data inform of images is currently on of the hot research area. Now day's images are widely used for authorization purpose. There are several approaches to encrypt the images .In this paper we have characterized the different image encryption algorithms based on their properties. We have also discussed the advantages of these algorithms and their demerits. Image encryption algorithms are generally evaluated on performance measure such as contrast, security, accuracy, computational complexity etc. Good encryption algorithms should be able to regenerate the original image, in terms of colors and contrast. It should also have to be secure and computationally less expensive.

Image encryption algorithms can be characterized on the basis of key they used or amount of information they lost while retrieving the original image from encrypted one. On basis of Key image encryption algorithms are characterized as image encryption using key approach is traditional.

(a) Encryption is done using a key and algorithms example of their approaches.
(1) Digital signature (2) Chaos theory (3) Vector quantization etc

(b)Image encryption without using key (keyless encryption) – It's involve the splitting of image at pixel level such that individual share doesn't convey any information about image. There is no need of key management.

II. RELATED WORKS

Image Encryption Using Affine Transform and XOR Operation

In image encryption using affine transformation and XOR operation [1] author has proposed a location transformation based encryption technique. They redistribute the pixel value to different location using affine transformation technique. The transformed image has been divided into pixel block then they encrypt each block using XOR operation. Author has used a 64 bits symmetric key. This key has been further divided into 8 sub keys. The key is chosen in such a way that the first sub key is relatively prime to width of the image fourth sub key is relatively prime, to height of image. They have used 2 level of computation. In the first level the first four sub key are used for location transformation of pixel value. They have used affine transformation cipher algorithms for this. In second level next four sub keys is used for encryption and the blocks are XORed with the keys .This result in reduction of correlation between pixel values.

Image Encryption Using Block-Based Transformation Algorithm

In this image encryption algorithm, images are divided into number of blocks [2]. This will help us to reduction in correlation and also increase the entropy of image. The image are divided into blocks are random process and the block size are also chose randomly. Information regarding each blocks and its size are stored in transformation table. For better transformation block size should be small. Transformed image are then encrypted using blowfish algorithm.

A New Scrambling Method Based on Arnold and Fermat Number Transformation

It can be concluded that the statistical character of the whole image is unchanged although the partial relativity of pixels are destroyed [7]. That is the histogram of originally image and the histogram of scrambled image are the same. The statistical character of secret images pre-processed with Arnold easily can be attacked, so it is necessary to study a new

information hiding method, which not only can change the texture information of image, but also can change the statistical character of image. Arnold transformation is simply known as cat map transformation. Suppose the coordinate (x, y) in 2-D plain. The Arnold transformation that change the coordinate (x, y) to the (x', y') by using formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ n \qquad (1)$$

This should transform the image iteratively.

III. PROPOSED WORK

A block based image encryption using iterative Arnold transformation. First of all image are divided into n*n blocks. Where n is number of rows and columns, to reduce the correlation among the pixels. Blocks have been shuffled using the algorithm1 discussed next. After divide the image into block each block treats as the cell and each cell position change according to algorithms row wise and column wise. After that Arnold transformation applied on shuffled blocks of image iteratively. The transform is a process of clipping and splicing that realign the pixel matrix of digital image. Arnold transformation has been discussed in algorithm2.

Algorithm1 for block shuffling

Input: gray image;
Output: block shuffled image;
Step1: read the image from disk;
Step2: divide the image n*n blocks;
Step3: Initialize the variables;
Image = rows* col;
BlocksizeR =n;
BlocksizeC =n;
wholeBlockRows = rows / blockSizeR;
wholeBlockCols = columns / blockSizeC;
Step4: display all the blocks;
plotIndex = 1;
numPlotsR = size(cell array);
numPlotsC = size(cell array);
for r = 1 : numPlotsR
for c = 1 : numPlotsC
subplot (numPlotsR, numPlotsC, plotIndex);
grayblock = ca{r,c};
Show gray block;
plotIndex = plotIndex + 1;
Increment c;
Increment r;
Step5: Shuffled the blocks within
Image;

- Initialize l =1
- For every numplotsR till l is less than numplotR do
  (a) Initialize i=1;
  (b) do,until numplotC greater than i
    1. initialize temp
    2. j= numplotC
    3. swap ca(l,j)& ca(l,i)
    4. increment I by 1
    5. decrement j by -2
- increment l by 1
- initialize l=1
- for every numplotC until l is less than numplotC do
  (a) Initialize i=1
  (b) do,until numplotC is greater than i
    1. initialize temp
    2. j=numplotsR
    3. swap ca(j,l)& ca(I,l)
    4. increment i by 1
    5. decrement j by -2

- increment l by 1

Step5: arrange shuffled block into an image

Algorithm2 for Arnold transformation

Input: block shuffled image;

Output: encrypted image;

- Define the number of iteration;
- j=1;
- do, until the j is less than number of iteration

```
for x=1ton
 for y=1ton
x1=mod ((1*x+1*y),n);
    y1=mod ((1*x+2*y), n);
    temp=image(x,y);
    image(x,y)=image(x1,y1);
    image(x1, y1) =Temp;
```

IV. RESULT ANALYSIS

Results are evaluated on the following parameters. Here discussion of results is based on different size of blocks. Block size are 30*30, 50*50 and 100*100.

(1)MEAN SQUARE ERROR-

The **Mean Squared Error (MSE)** of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated.

$$MSE = \frac{1}{n2}\sum_{i,j=0}^{N-1} \| C(i,j) - \hat{C}(i,j) \|^2$$

Calculated mean square error on different image is less as compared to previous technique it will help to make image more secure.

(2) NORMALISED CROSS CORELATION-

Normalized Cross Correlation (NCC) has been commonly used as a metric evaluate the degree of similarity or dissimilarity between two compared images. The main advantage of the normalized cross correlation over the cross correlation is

That it is less sensitive to linear changes in the amplitude of illumination in the two compared images.

$$C_{AB} = \frac{\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{i,j}-\bar{A})(B_{i,j}-\bar{B})}{\sqrt{\frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(A_{i,j}-\bar{A})^2 \frac{1}{r*c}\sum_{i}^{r}\sum_{j}^{c}(B_{i,j}-\bar{B})^2}}$$

$A_{i,j}$ and $B_{i,j}$ are the pixels in the i^{th} row and j^{th} column of A and B respectively and r, c represent the no. of rows and columns in the image.

(3)PSNR (Peak Signal to Noise Ratio)-

PSNR is defined as ratio of amount of significant signal information to noise. This parameter shows quality measure of an encryption technique. Lower the value of PSNR, more the encryption is stronger because it shows resultant cipher image is noise like and it contains very less amount of significant information.

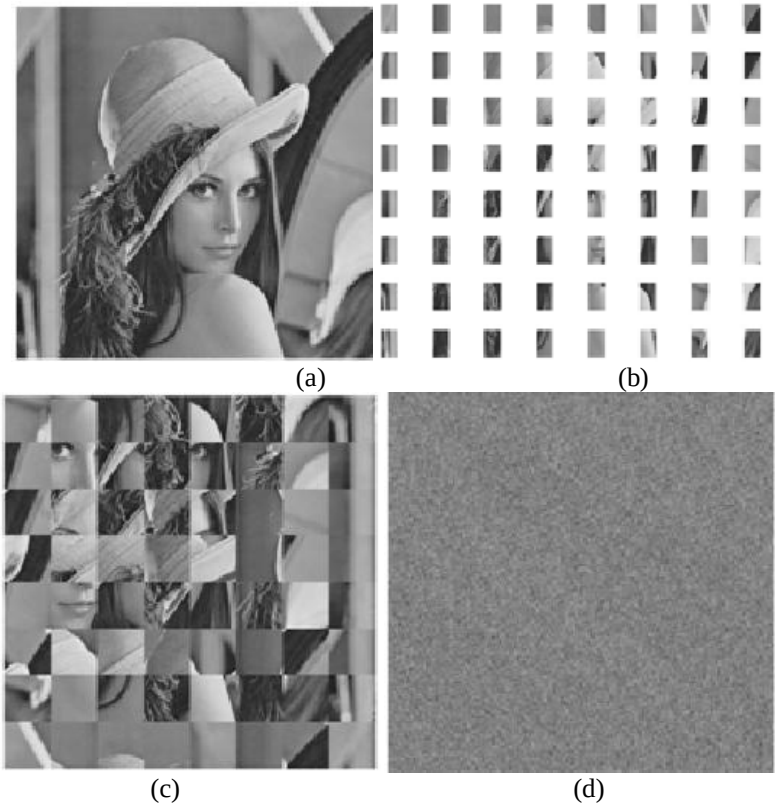
$$PSNR = 10log\frac{(2^N-1)^2}{MSE}$$

(4)ENTROPY-

In information theory, entropy is a measure of the uncertainty in a random variable. In this context, the term usually refers to the entropy, which quantifies the expected value of the information contained in a message. Entropy is typically measured in bits, nats or bans. Shannon entropy is the average unpredictability in a random variable, which is equivalent to its information content.

$$h = -\Sigma(p_i log_2 p_i)$$

Where p_i is the frequency of intensity level i in the image. The maximum h an 8–bit image can attain is 8.



(a) (b)

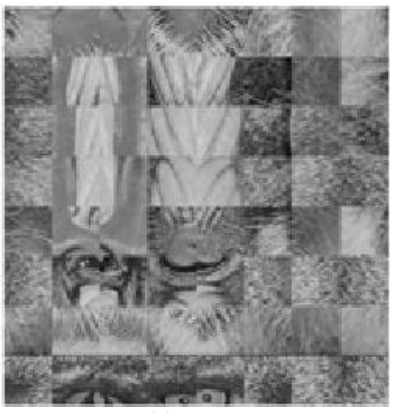
(c) (d)

Figure 1(a) Original image of Lena.tiff (b) Blocked image of Lena.tiff (c) Shuffled image of Lena.tiff (d) Encrypted image of lena.tiff

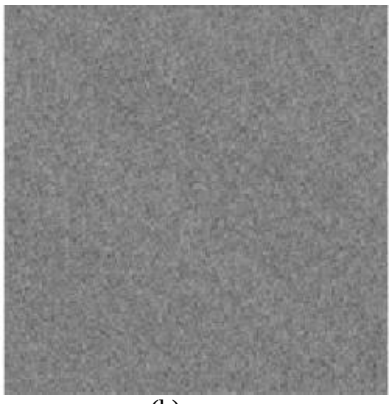
Table 1 Result for image-Lena.tiff

Block size	**MSE**	**Normalized correlation**	**PSNR**	**Entropy**
100*100	4.5711e+003	0.0020	11.5306	7.4451
50*50	4.5695e+003	0.0024	11.5321	7.4451
30*30	4.5958e+003	-0.0034	11.5072	7.4451

(a) (b)



(c)

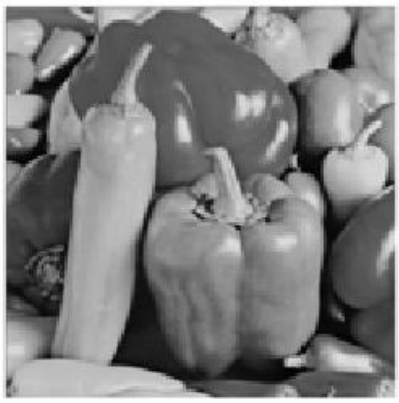


(b)

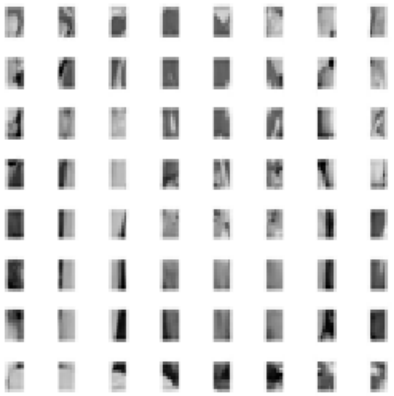
Figure2 (a) Original image of baboon.tiff (b) Blocked image of baboon.tiff (c) Shuffled image of baboon.tiff (d) Encrypted image of baboon.tiff

Table 1 Result for image-baboon.tiff

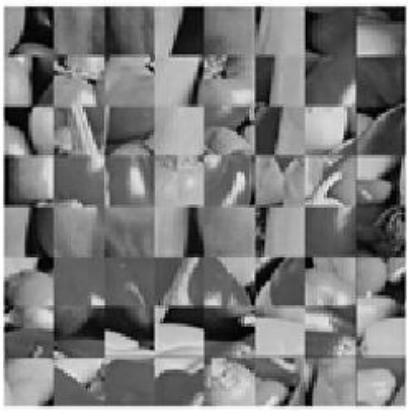
Block size	MSE	Normalized correlation	PSNR	Entropy
100*100	3.5929e+003	-0.0034	12.5763	7.3583
50*50	3.5969e+003	-0.0045	12.5715	7.3583
30*30	3.5928e+003	-0.0033	12.5765	7.3583



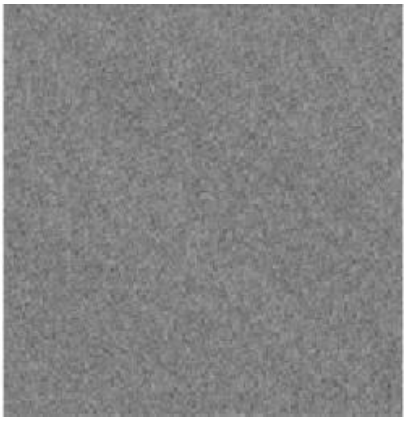
(a)



(b)



(c)



(d)

Figure3 (a) Original image of pepper.tiff (b) Blocked image of peppers.tiff (c) Shuffled image of pepper.tiff (d) Encrypted image of pepper.tiff

Table 2 Result for image-peppers.tiff

Block size	MSE	Normalized correlation	PSNR	Entropy
100*100	5.8795e+oo3	-0.0127	10.4374	7.5937
50*50	5.7686e+003	0.0064	10.5201	7.5937
30*30	5.8347e+003	-0.0050	10.4706	7.5937

V. CONCLUSION

The proposed encryption algorithm uses two different algorithms. One algorithm is for divide the image into blocks after that each block is shuffled within image and another for Arnold transformation which will apply on the shuffled image iteratively. This approach provides us to encrypt the image two times. First the images are scrambled using algorithm and then transformation with using key. High key sensitivity is required by secure image cryptosystems, which means that the cipher image cannot be decrypted correctly. This guarantees the security of the proposed technique against brute-force attacks to some extent.

REFERENCES

[1] A. Nag, J.P. Singh, S. Khan, S. Biswas, and D. Sarkar, "Image Encryption Using Affine Transform andXOROperation", in *Proc. international conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN),* , pp.309-312,2011.

[2] Mohammad Ali Bani Younes and Arnan Jantan ," Image Encryption Using Block-Based transformation Algorithm", *IAENG International Journal of Computer Science*, vol. 35:1, IJCS_35_1_03,2008.

[3] S Malik, A Sardana, J Jaya,."A Keyless Approach to Image Encryption", *in International conference on Communication Systems and Network Technologies (CSNT)*, pp. 879 - 883, 2012.

[4] A Goel and N Chandra. "A Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel". *In Internation conference on Communication Systems and Network Technologies (CSNT)*, pp.884-888, 2012 .

[5] Jayantkushwaha;Bolanath Roy "Secure Image Data by Double encryption*" International Journal of Computer Applications (0975 – 8887) Volume 5– No.10*, August 2010.

[6] Zhenwei Shang, Honge Ren and Jian Zhang" A Block Location Scrambling Algorithm of Digital Image Based on ArnoldTransformation*" The 9th International Conference for Young Computer Scientists, ICYCS*, 2008.

[7] Zhang Yanqun; WangQianping;"A New Scrambling Method Based on Arnold and Fermat NumberTransformation"*International conference on Environmental science and information application technology*,2009.

[8] Lingling Wu, Jianwei Zhang and Weitao Deng and Dongyan He "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm" *1st International confrece on Information Science and Engineering (ICISE*), 2009 .

[9] LiuFang, and WangYuKai;"Restoring of the Watermarking Image in Arnold Scrambling*",2nd International conference on Signal Processing Systems (ICSPS)*, 2010.

