Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping

Rakesh S[1], Ajitkumar A Kaller[2], Shadakshari B C[3] and Annappa B[4]

Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal

[1]rakeshsmysore@gmail.com
[2]ajitkaller@gmail.com
[3]shadsbellekere@gmail.com
[4]annappa@ieee.org

ABSTRACT

With the fast evolution of digital data exchange and increased usage of multi media images, it is essential to protect the confidential image data from unauthorized access. In natural images the values and position of the neighbouring pixels are strongly correlated. The proposed method breaks this correlation increasing entropy of the position and entropy of pixel values using block shuffling and encryption by chaotic sequence respectively. The plain-image into blocks and then performs block based shuffling using Arnold Cat transformation. Further, the image is uniformly scrambled, where all the pixels in the same block of scrambled image come from different blocks of original image, after which the image as a whole is shuffled again by the transform. Finally the shuffled image is encrypted using a chaotic sequence generated using symmetric keys, to produce the ciphered image for transmission. The experimental results show that the proposed algorithm can successfully encrypt/decrypt the images with the secret keys, and the analysis of the algorithm also demonstrates that the encrypted images have good information entropy and low correlation coefficients.

KEYWORDS

Correlation, Image Decryption, Image Encryption, Image Entropy, Image Shuffling

1. Introduction

Encryption is a common technique to uphold multimedia image security in storage and transmission over the network. It has application in various fields include internet communication, medical imaging and military communication. Due to some inherent features of images like high data redundancy and bulk data capacity, the encryption of images differs from that of texts, thus algorithms suitable textual data may not be good for multimedia data.

Many image-protection techniques use vector quantization (VQ) as the main encryption technique (Chang et al., 2001; Chen and Chang, 2001). A symmetric block encryption algorithm creates a chaotic map, used for permuting and diffusing multimedia image data. There have been many more image encryption algorithms based on chaotic maps [1]-[5]. There has been many other image encryption algorithms proposed based concepts such as block cipher[6] and selective encryption[9]. Also few techniques in video encryption has also been proposed[10]. Several cryptosystems similar to data encryption, such as steganography [8] and digital signature [7] have also been proposed to increase security of image storage and transmission.

In this paper, a new uniform scrambling and block based image shuffling is proposed to achieve good shuffling effect and the encryption of the shuffled image is performed using a chaotic map to enforce the security of the proposed encryption process.

2. Proposed Method

In order to improve the security performance of the image encryption algorithm, positions of pixels in the original image is shuffled and gray values of the shuffled image is changed.

2.1. Image Encryption

Step i. The image has to be shuffled and scrambled to decrease correlation between adjacent pixels, to do this, we first divide the whole image I into blocks of size 16x16, B_1, B_2, . . ., B_n.

Step ii. Apply Arnold Cat transformation within block B_i by the following equation:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (1)$$

where (x, y) are original coordinates of I and (x',y') are new shuffled coordinates . After repeating this step for each of the n blocks we get partially shuffled image I' (x, y).

Step iii. Intra-block shuffling would not be sufficient to decrease correlation between pixel positions, the pixels also needs to be uniformly scattered across the image. To measure randomness, we consider image position entropy given by the following equation

$$H(I) = \sum_{i=1}^{n} H_i(P) \quad (2)$$

where, n is the total number of image blocks, $H_i(P)$ is the entropy of the ith block and denotes the average information capacity in this block and it is defined as follows

$$H_i(P) = \sum P(x,y) \log \left(\frac{1}{P(x,y)}\right) \quad (3)$$

where, P(x,y) is the probability of pixel which coordinates (x,y) in original image appears at the ith block in the scrambled image. We known that $H_i(P)$ will reach the maximum when all the P(x,y) are equal and thus H(I) attains the maximum value. So the perfect state of image scrambling is the random pixel in respective block of the scrambled image has the equal probability of coming from the random situation in plain original image. One can also conclude that average information content will get the maximum when the probability that pixels in a block of original image is distribute into different blocks. Thus we perform uniform scrambling where the pixels in the same block of the image I' is distributed into all the blocks and the every block has one pixel at least, without regarding to the order of the pixels, accordingly all the pixels in the same block of scrambled image come from different blocks of the plain image.

Figure(1) below shows that all the pixels in the first block of the original image are distributed into all the blocks of the scrambled image, irrespective of the order. Thus, ideal block numbers is N for an original image of size NxN. After this uniform scrambling, we get new image I''.

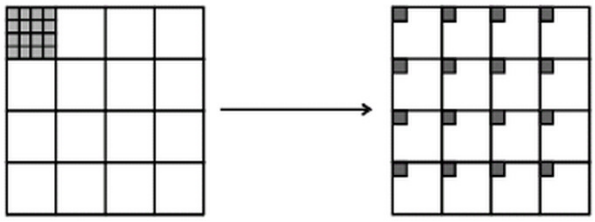


Figure 1. Uniform Image Scrambling

Step iv. Apply Cat transformation again, but this time to the whole image to I''. After the above steps, correlation of pixel positions will be reduced, but to decrease this value further and bring it to the ideal value 0, we repeat steps i to iv iteratively to get the final shuffled and scrambled image IS. In our algorithm we performed 3 iterations were performed to get the shuffled image, which proved to be sufficient by the experimental results.

Step v: The essence of image encryption or image scrambling is to reduce the correlation of pixel positions and the correlation of pixel values until they are irrelevant to each other. Image shuffled by above three steps will result low correlation, but the pixels will still be having same values, entropy and histogram will be same as that of the original image, making the system vulnerable for statistical attacks. So pixel values have to be encrypted to increase entropy. This is done by using the symmetric secret keys A and K to generate chaotic sequence, which is used to encrypt pixel values with a combination of add and XOR operations as shown below-

```
A=K*A*(1-A)
KB1=mod(10^14*A,256)
IE(x,y)= mod(IS(x,y)+KB1,256)

A=K*A*(1-A)
KB2=mod(10^14*A,256)
IE(x,y)= xor(IE(x,y),KB2)
```

where, (x,y) are pixel co-ordinates of the intermediate shuffled image IS. The resultant will be an encrypted image IE, with entropy close to ideal value of 8. And in our case, the keys A and K were taken to be 0.3905 and 3.9885 respectively. Also the above method restricts encrypted values less than 256, by modulus operation and thus making the resultant also an 8 bit image. By experimental results, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the plain image, thus not providing any indication to employ statistical attacks on the encrypted image.

2.2 Image Decryption

The encrypted image IE can be easily decrypted by reversing the effect and retracing the encryption steps backwards -

Step i: The image IE is decrypted by generating the same chaotic sequence using same symmetric key pair A and K. A combination of XOR and subtract operation is used to decrypt individual pixel values of the image. The resultant would be an image ID, having the pixel values same as that of original image, but correlation between adjacent pixel still not being the same due shuffling.

Step ii. Apply inverse the transformation matrix used in embedding process to shuffle the pixels of the whole image. During watermark embedding, Arnold Cat transformation used $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ as mapping matrix, thus here its inverse $\begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$ is used as transformation matrix to get the partially de-shuffled image ID'.

Step iii : Now the block wise shuffling and scrambling effect on the pixels performed during process has to nullified . For this we divide the whole image ID' into 16x16 sized blocks, B1, B2, . . ., Bn. And the pixels uniformly scattered across the image amongst different blocks has to be brought back to their respective block, getting back the original positional entropy. Say the resultant of this step is an intermediate de-shuffled image ID''.

Step iv. The transformation matrix used in step ii, is applied once again on each of the blocks B_1, B_2,.., B_n to de-shuffle the image block wise. Steps ii to iv are repeated the same number of

iterations performed during encryption process to finally remove all the shuffling and scrambling, fetching image ID'''. Also by experimental results, the normalized correlation coefficient between the original image and decrypted image is very close to the ideal value unity, proving the robustness and correctness of the proposed encryption algorithm.

3. Experimental Results

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical, differential and brute-force attacks. Thus the histogram of the ciphered image must be uniform to avoid statistical attacks, and the key space must be large enough to avoid brute force attacks. Below performance analysis of the proposed approach shows that it is indeed robust against possible attacks and also flexible enough to extend the same to binary and RGB images as well.

3.1. Histogram Analysis

In the experiments, the plain image, its corresponding cipher image and their histograms are shown in fig (2). It is clear that the histogram of the cipher image is nearly uniformly distributed, and significantly different from the respective histograms of the plain original image. So the encrypted image does not provide any clue to employ any statistical attack on the proposed procedure, which makes statistical attacks difficult.

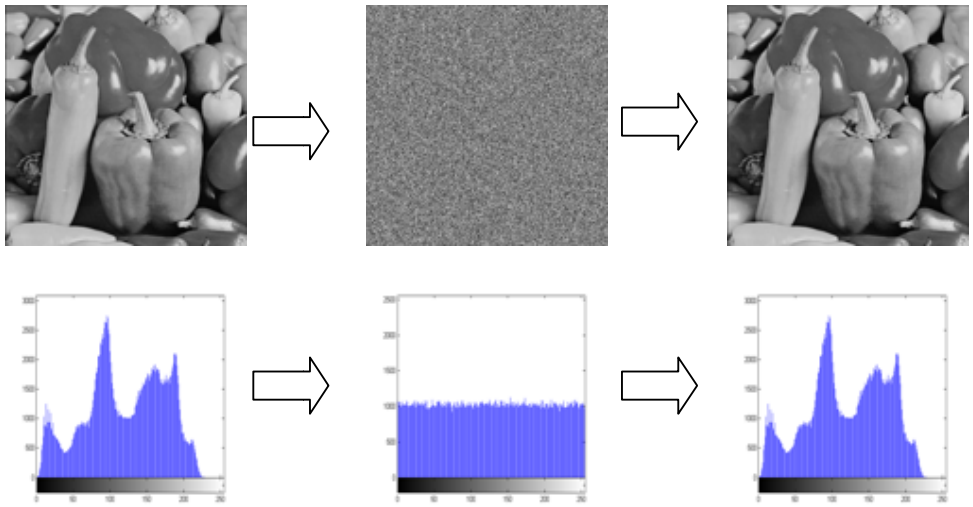


Figure 2. Original, Encrypted and Decrypted Images and their corresponding Histograms

3.2. Correlation of two adjacent Pixels

Here, we test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in the encrypted image. Correlation coefficient of each pair is calculated by the formula below-

$$\mathrm{cov}(p,q) = E(p - E(p))(q - E(q)) \tag{4}$$

where p and q are pixel values of two adjacent pixels in the image. Fig. (3) (a) shows the distribution of two horizontally adjacent pixels of the plain image, (b) the distribution of two horizontally adjacent pixels of the cipher image, similarly figure (c) shows the distribution of two

vertically adjacent pixels of the original image and (d) distribution of two vertically adjacent pixels of the encrypted image.

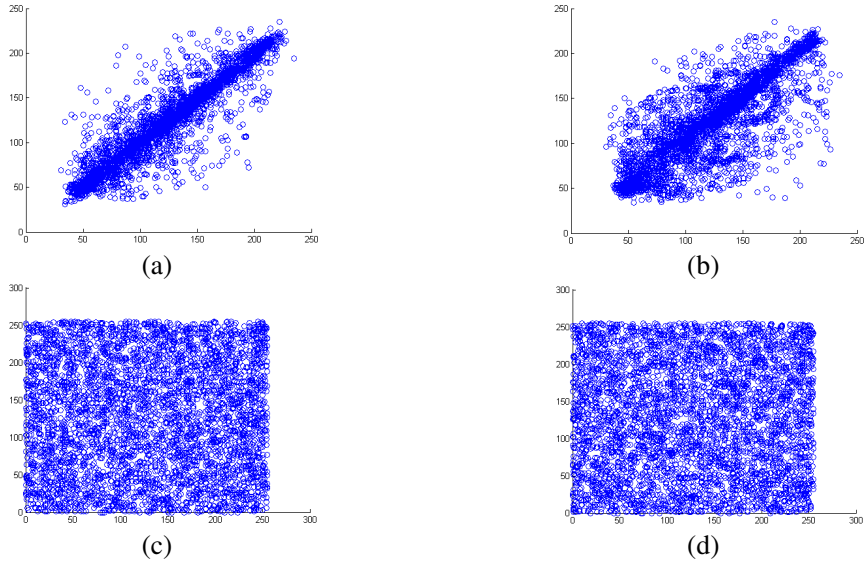


Figure 3. Correlation comparison of two adjacent pixels

3.3. Image Entropy

Entropy is a measure uncertainty association with random variable. As for an image, the encryption decreases the mutual information among encrypted image variables and thus increases the entropy value. A secure system should satisfy a condition on the information entropy that is the cipher image should not provide any information about the original image. The information entropy is calculated using equation

$$\text{Entropy} = \sum(p(i) * \log(1/p(i))) \tag{5}$$

where p(i) is the probability of occurrence of a pixel with gray scale value i. If each symbol has an equal probability then entropy of 8 would correspond to complete randomness, which is expected in encrypted image.

Different images have been tested by the proposed image encryption procedure and the results of entropy, horizontal and vertical correlation coefficients are shown in the Table(1) below.

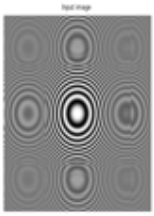
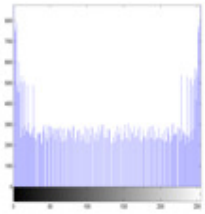
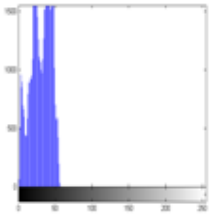
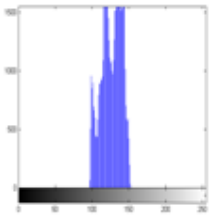
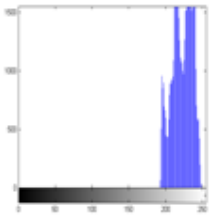
Table 1. Tested Images and their corresponding entropy, horizontal and vertical correlation.

Image	Entropy Horizontal Correlation Vertical Correlation	Image	Entropy Horizontal Correlation Vertical Correlation
	7.999207 0.000962 -0.001922		7.999253 0.000893 -0.001703
	7.999227 -0.001827 0.001319		7.999342 -0.002541 0.001462
	7.999308 0.000106 0.001632		7.999951 0.000308 0.000312

3.4. Key Space Analysis

For secure cryptosystem, the key space should be large enough to make sure that brute force attack is infeasible. The proposed algorithm has 2^{256} different combinations of the secret keys. A cipher with such as a long key space is sufficient for practical use. Furthermore, if we consider the shuffling and scrambling as part of the key, the key space size will be even larger. Hence, the key space of the proposed algorithm is sufficiently large enough to resist the exhaustive of brute-force attacks.

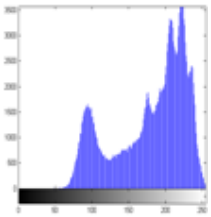
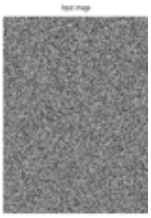
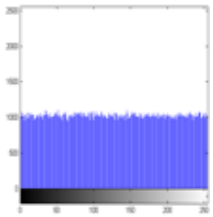
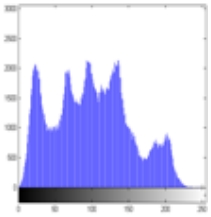
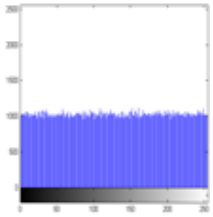
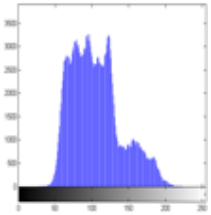
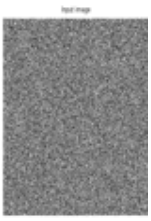
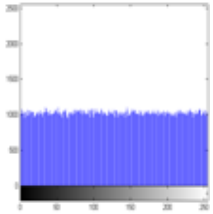
Table 2. Testing for special cases.

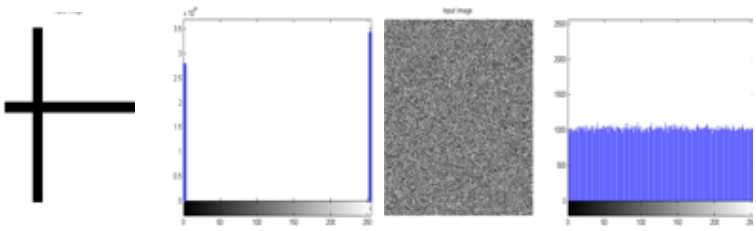
Case	Image	Histogram	Entropy Horizontal Correlation Vertical Correlation
1			7.997100 0.004073 0.002616
2			7.997435 0.000713 -0.002101
3			7.997684 0.001263 -0.000059
4			7.997348 -0.000500 -0.000701

3.5. Testing for Special Cases

Table(2) above shows that the proposed algorithm works for some special cases also, as in case 1, where the original image already has high entropy and pixels evenly scattered, and in case 2-4 where the histogram is squeezed within a small range and is mean shifted in the wide gray scale range available. Also the table(3) below shown application of the same on red, green and blue channels of lena, shown in cases 1-3 respectively and on a binary image case 4. The correlation and entropy values in tables (2)-(3) prove the effectiveness of the proposed approach.

Table 3. Algorithm Tested for RGB and Binary Images.

Case	**Image**	**Histogram**	**Encrypted**	**Histogram**	**Entropy** **Horizontal Correlation** **Vertical Correlation**
1					7.999372 0.000521 -0.002127
2					7.999316 -0.000348 0.002087
3					7.999418 0.002986 -0,000743

4		7.999365 -0.002221 0.001245

4. Conclusion

In this paper, a new improved for image security using a combination of image transformation and encryption techniques is proposed. The approach first does uniform scrambling and block based image shuffling is proposed to achieve good shuffling effect and later encrypt the shuffled image using a chaotic map to enforce security. The experimental analysis shows that the proposed image encryption system has a very large key space, has information entropy close to the ideal value 8 and has low correlation coefficients close to the ideal value 0. Thus the analysis proves the security, effectiveness and robustness of the proposed image encryption algorithm. Further work will be concentrated on extending proposed algorithm for video and audio encryption.

5. References

[1] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, “Encryption and decryption of images with chaotic map lattices.” CHAOS Journal, American Institute of Physics, vol. 16, no. 3, pp. 033118-033118-6, 2006.

[2] S. E. Borujeni, M. Eshghi1, ―Chaotic Image Encryption Design Using Tompkins-Paige Algorithm, Hindawi Publishing Corporation, Mathematical Problems in Engineering, Article ID 762652, 22 pages, 2009.

[3] Abir Awad, Abdelhakim Saadane, ―Efficient Chaotic Permutations for Image Encryption Algorithms, Proceedings of the World Congress on Engineering Vol I, 2010.

[4] Ai-hongZhu, Lia Li, ―Improving for Chaotic Image Encryption Algorithm Based on Logistic Map, 2nd Conference on Environmental Science and Information Application Technology, 2010.

[5] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavand, “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps.” Physics Letter A, vol. 366, no. 4-5, pp. 391-396, 2007.

[6] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images," Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt, 2006

[7] Aloha Sinha, Kehar Singh, “A technique for image encryption using digital signature”, Optics communications, ARTICLE IN PRESS, 2003.

[8] X.Y. Wang, and Q. J Shi, “New Type Crisis, Hysteresisand Fractal in Coupled Logistic Map.” Chinese Journal of Applied Mechanics, pp. 501-506, 2005.

[9] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS’02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[10] S. Changgui, B. Bharat, "An efficient MPEG video encryption algorithm," Proceed in g s of the symposium on reliable distributed systems, IEEE computer society Press, 1998, pp. 381-386.