Breaking Row-Column Shuffle Based Image Cipher

Weihai Li, Yupeng Yan, Nenghai Yu
Department of Electronic Engineering and Information Science
University of Science and Technology of China
96, Jinzhai Road, Hefei Anhui Province, P. R. China
whli@ustc.edu.cn

ABSTRACT
In this paper, a redundancy based cipher-only attack is proposed to break row-column shuffle based image encryption algorithms, which are considered to be safe under cipher-only attack before although it is well known that they are fragile under known-plaintext attack. This attack is carried out on the shuffle operations itself by analyzing the redundancy remained in cipher image, and doesn't care how the shuffle tables are generated. So, no matter how the shuffling tables are generated, this attack is valid. Experimental results show high quality deciphered images from one single cipher image, and that demonstrate the validity of our attack method. This attack method is also a potential threat to shuffle-scramble combined encryptions.

Categories and Subject Descriptors
I.4.9 [**Image Processing and Computer Vision**]: Applications.

E.3 [**Data Encryption**]: – *code breaking.*

General Terms
Algorithms, Reliability, Security.

Keywords
Cryptanalysis, Image encryption, Row-column shuffle, Redundancy.

1. INTRODUCTION
In the digital world today, the security of digital images becomes more necessitous since more images are transmitted through the open network. Furthermore, special and reliable security in digital images storage and transmission is needed in many applications, especially in the circumstance of cloud storage and cloud computing. Image encryption technology is an effective measure to ensure the information security of private images. With this technology, only the legal users can decrypt encrypted images correctly with the secret key [1,2].

Fundamental data encryption techniques of scramble and shuffle [2,3] are also basic techniques in image encryption algorithms. Row-column shuffle, which shuffles the rows and columns of an image respectively and successively, is sometimes used directly as encryption when high-speed is required, or adopted as a stage in many encryption algorithms. To rule the shuffles of rows and columns, researchers have presented many ways to generate the shuffle tables from pseudo-random sequences of discrete chaotic sequence [4] or linear feedback shift register, etc.

MM'12, October 29-November 2, 2012, Nara, Japan.

However, it is very hard to evaluate the security of a given image encryption algorithm. Although it has been reported that permutation-only encryptions are fragile to known/chosen-plaintext attack [5,6], it is still considered safe by a properly designed key usage policy. For example, Figure 1 shows an example which ensures that the session key (key to encrypt/decrypt images) varies each time.

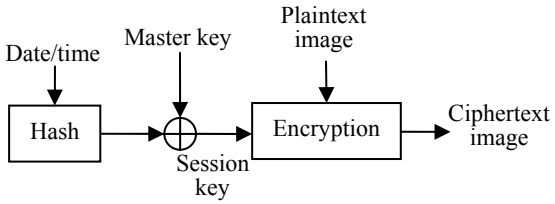


Figure 1. A key usage scheme example.

In this paper, a cipher-only attack is reported to break row-column shuffle based encryption algorithms by one single cipher image. This attack does not analyze encrypted image from the data level, but from the low semantic level. In another word, it takes advantage of the high redundancy remained in encrypted image. It is worth mentioning that this attack is valid for all kinds of row-column shuffle encryption algorithms, and is also a potential threat to shuffle-scramble combined encryptions since it has nothing to do with how the shuffle tables are generated.

The following of this paper is organized as follows. In Section 2, a brief introduction of row-column shuffle encryption algorithm is made, and some statistical security analyses are discussed. Then our attack method is presented in Section 3. In Section 4, we gave some experimental results, and discussed the probability of applying this attack to shuffle-scramble combined encryption. Finally, a short conclusion is made in Section 5.

2. ROW-COLUMN SHUFFLE BASED ENCRYPTION ALGORITHM
As we did in general data encryption, scramble and shuffle are two basic and primary techniques in image encryption. Up to date, researchers have developed many encryption algorithms of scramble, shuffle, or their combinations. The row-column shuffle is among the simplest and fastest ones and thus is adopted when computing cost is a key factor of a system.

When performing row-column shuffle, an image is regarded as a matrix of h rows and w columns. The procedure of row-column shuffle is very simple [4]. First, two tables, one for row shuffle and the other for column shuffle, are generated from the secret key. Then the rows and columns are shuffled successively

according to their shuffle tables. The procedure of shuffling rows followed by shuffling columns is equivalent to the procedure of shuffling columns followed by shuffling rows.

Since our attack is irrespective to the shuffling tables, we just using a simple pseudo-random number generator (PRNG) as an example to explain the algorithm. The PRNG is

$$x_{i+1} = x_i^2 + x_i + s \pmod{n}, \text{for } i = 0,1,2,\cdots, \quad (1)$$

in which, s is the random initial seed, and n is a large number. The row shuffle table T_R is defined as:

$$a = x_i \pmod{h}, \quad (2)$$

$$T_R(i) = a + b\ . \quad (3)$$

Here b is minimum non-negative integer, which ensures $a+b$ does not appear before. According to table T_R, row i is shuffled to row $T_R(i)$ for i=0,1,2,…,h-1. The column shuffle table $T_C(i)$ is defined similarly.

Figure 2 gives an example of row-column shuffle. For human sight, no information can be seen from the encrypted image.

(a) Original image. **(b) Encrypted image.**

Figure 2. A row-column shuffle encryption.

There are still no trustable criterions to evaluate the security of an image encryption algorithm. Instead, the following statistical measures are often used as reference indexes.

Histogram is a measure about image content [2,3]. An algorithm maybe secure if it flat the histogram. But for a shuffle-only encryption, the histogram of encrypted image is the same with the original one since shuffling does not change the value of pixels. So we overleap this analysis. A corresponding measure is entropy index, which is calculated from histogram [7]. Therefore the entropies of original image and shuffled image are also the same.

Correlation of two adjacent pixels is a widely used statistical criterion [2,3,7,8]. Since nature image contains large redundancy, the correlations of neighbor pixels are very large; whereas encrypted image is noise-like, and the correlation tends to be very small. Here we calculate correlation coefficients C_r with

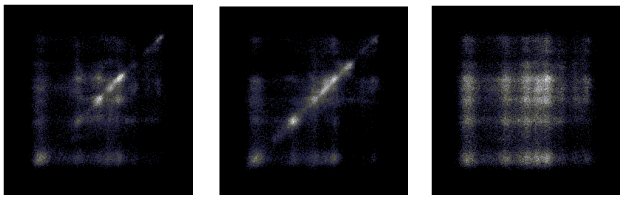
$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}, \quad (4)$$

where x_j and y_j are gray values of two adjacent pixels in original and encrypted image respectively, and N is the total number of pixels. The defect of this criterion is that it only describes correlations of neighbor pixels, but not considers long distance correlation.

Gray level dependence matrix (GLDM) is a measure of adjacent pixel correlations, and it can help us to make a visual intuitive judgment. Figure 3 shows the GLDMs among two horizontally, vertically, and diagonally adjacent pixels of Figure 2 respectively. The corresponding correlation coefficients C_r are given in Table 1. The values are acceptable but not very good because the example PRNG is just a simple one.

Horizontally **Vertically** **Diagonally**

(a) GLDM for Figure 2(a).



Horizontally **Vertically** **Diagonally**

(b) GLDM for Figure 2(b).

Figure 3. GLDM among adjacent pixels.

Another statistical analysis is the peak signal-to-noise ratio (PSNR) [8], which can be calculated with

$$PSNR = 20\log_{10}\frac{255}{\left(\frac{1}{N}\sum_{j=1}^{N}\left(x_j - y_j\right)^2\right)^{1/2}}, \quad (5)$$

in which the x_j, y_j and N have the same definitions as in formula (4). Unfortunately, the PSNR only describes the difference between two images, but has no necessary relation to security. The *PSNR* between the encrypted image and original image of Figure 2 is given in Table 1. The low *PSNR* shows that the two images have little relation.

Table 1. Measures of Correlation coefficients and PSNR

	Original image Figure 2(a)	**Encrypted image Figure 2(b)**
Horizontal *Cr*	0.9722	0.1761
Vertical *Cr*	0.9852	0.3049
Diagonal *Cr*	0.9603	0.0711
PSNR	-	11.5522

However, no matter how good these values appear, they have no necessary relation with security. In the next section, a redundancy based attack was proposed to break this encryption algorithm.

3. REDUNDANCY BASED ATTACK

3.1 Cryptanalysis with redundancy

Suppose $S(i)$ is the inverse shuffle table, which satisfies

$$S\left(T\left(i\right)\right)=i\ . \tag{6}$$

For an original image $I(y,x)$, its encrypted version can be written as $I_E(T_R(y),T_R(x))=I(y,x)$, here y and x are pixel coordinates, then the decrypted image is $I_D(S_R(y),S_C(x))=I_E(y,x)$. Therefore, to break an encrypted image is to find two tables S'_R and S'_C which are similar to S_R and S_C, viz,

$$\arg\min_{S'_R,S'_C}\left\|I_D\left(S_R\left(y\right),S_C\left(x\right)\right)-I'_D\left(S'_R\left(y\right),S'_C\left(x\right)\right)\right\|. \tag{7}$$

Unlike ordinary cryptanalysis of general data encryption, there are more tricks we can use on image data. It is well known that image contains large redundancy, which means adjacent pixels are likely to be similar, so are adjacent lines. Therefore, we can estimate S'_R and S'_C by rearranging rows and columns to get large similarity between adjacent lines. According to this idea, we form a new objective function

$$\max_{S'_R,S'_C}\left\{\sum_{y=1}^{h-1}Corr^{x}_{I'_D}\left(y,y+1\right)\times\sum_{x=1}^{w-1}Corr^{y}_{I'_D}\left(x,x+1\right)\right\} \tag{8}$$

with the correlation functions defined between two rows or two columns:

$$Corr^{x}_{I(y,x)}\left(y_1,y_2\right)=\frac{\sum_{x=1}^{w}\left[I\left(y_1,x\right)I\left(y_2,x\right)\right]}{\left(\sum_{x=1}^{w}I\left(y_1,x\right)^2\sum_{x=1}^{w}I\left(y_2,x\right)^2\right)^{\frac{1}{2}}}, \tag{9}$$

$$Corr^{y}_{I(y,x)}\left(x_1,x_2\right)=\frac{\sum_{y=1}^{h}\left[I\left(y,x_1\right)I\left(y,x_2\right)\right]}{\left(\sum_{y=1}^{h}I\left(y,x_1\right)^2\sum_{y=1}^{h}I\left(y,x_2\right)^2\right)^{\frac{1}{2}}}, \tag{10}$$

Then, we make use of the variable separation approach to estimate the inverse row and column shuffle tables separately with equations (11), since the row and column shuffle operations can be separated.

$$\begin{cases}S'_R\left(y\right)=\arg\max_{S'_R}\sum_{y=1}^{h-1}Corr^{x}_{I_D\left(S'_R\left(y\right),x\right)}\left(y,y+1\right)\\ S'_C\left(x\right)=\arg\max_{S'_R}\sum_{x=1}^{w-1}Corr^{y}_{I_D\left(y,S'_C\left(x\right)\right)}\left(x,x+1\right)\end{cases}. \tag{11}$$

3.2 Cryptanalysis process

To find the optimal solution of problems in (11) is a hard work, particularly for large scale image. However, we noticed that a suboptimal solution is good enough for us to understand the content, since human visual system has a strong adaptive ability.

To break a given encrypted image $I(y,x)$ of size $h\times w$, our cryptanalysis process includes two similar stages: row rearrange and column rearrange. During the row rearrange stage, rows are shuffled to get a suboptimal solution of S'_R:

Step 1: A correlation matrix **C** is calculated for each pair of rows.

$$C\left(i,j\right)=\begin{cases}Corr^{x}_{I_E(y,x)}\left(i,j\right) & for\ j>i\\ -1 & for\ j\le i\end{cases}\quad 1\le i,j\le h \tag{12}$$

Step 2: Construct a graph ***G***, in which node i corresponds to the row i in image I_E. if $C(i,j)>0$, then add an edge between node i and j.

Step 3: Construct a graph ***H***, which has the same nodes as ***G***, but no edges.

Step 4: Find the maximum edge in ***G***. Add this edge into ***H*** if it does not produce any loop in ***H*** and no node has more than two edges connected. Remove this edge from ***G***.

Step 5: Repeat step 4, until (h-1) edges are added into ***H***. Obviously, this edges will link all nodes in ***H*** into a chain.

Step 6: Set S'_R according to the node numbers along the link.

Step 7: Rearrange rows according to S'_R.

For the column rearrange stage, just replacing all rows with columns. The order of the two stages is free.

After the rows and columns are all rearranged, the encrypted image is deciphered.

4. EXPERIMENTAL RESULTS

Several experiments are made to demonstrate the validity of our redundancy based attack method.

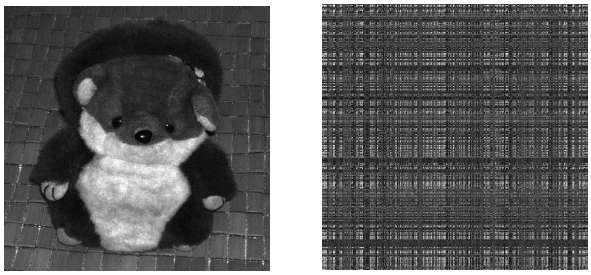
Apply the redundancy based attack to Figure 2(b), the deciphered result is shown in Figure 4. We can see that the deciphered image is perfectly the same with the original image, not concerning its 180 degree rotation. Since we just randomly choose a head of the link in step 6, the decrypted image is possible to be upside-down or left-right-swap. Anyway, human sight has no trouble to understand the image content.

(a) Original image. **(b) Deciphered image.**

Figure 4. Deciphered image of Figure 2(b).

Figure 5 gives another experiment example. In Figure 5(c), we can see the attack is carried out with some disordered stripes. This is not surprising since our solution is not the optimal solution. However, we can still understand its content, or manually adjust these stripes easily since the number is not large.

We established a dataset of 143 row-column shuffle encrypted images. The original images are downloaded from the Internet. Each cipher image is then attacked separately, and all main objects can be recognized clearly. Among them, 43 deciphered images are perfect without disordered stripes.



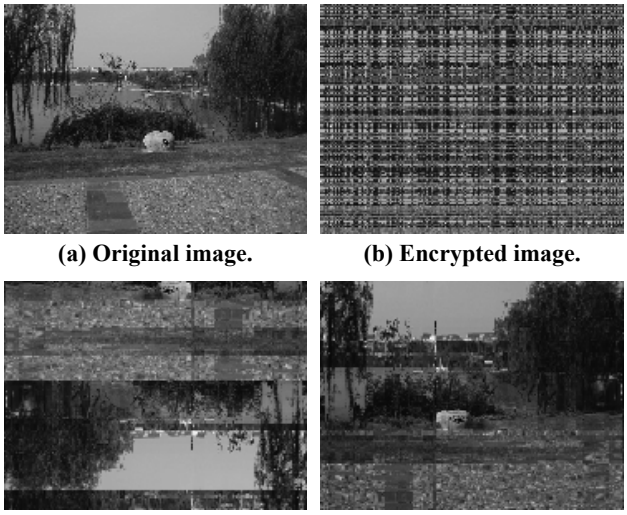
(a) Original image. (b) Encrypted image.

(c) Deciphered image. (d) Modified result.

Figure 5. An attack example on a toy image.

A more strong experiment was conducted on the following example. The original image and encrypted image are both manually copied from the PDF version of [4]. The sizes of images given by [4] are 568×426, but the copied version is only 183×138 because they are zoomed in PDF format.

Again, we got good result as shown in Figure 6. From Figure 6(c), all main objects can be recognized. When we manually rotated the deciphered image 180 degree, and adjust 6 mainly disordered horizontal stripes, a better result is obtained as Figure 6(d).



(a) Original image. (b) Encrypted image.

(c) Deciphered image. (d) Modified result.

Figure 6. An attack example on image from [4].

Summarily, this redundancy based attack can break all row-column shuffle based image encryptions, no matter how their shuffle tables are generated, and even if the cipher image are resized and compressed.

In addition, there are more encryption algorithms which combined the row-column shuffle with pixel scramble. Theoretically, a perfect scramble operation can cover image redundancy. But in practical, some new flaws, related to non-ideal scramble numbers, may be introduced. If some relations between two scrambled lines are found, then this attack can be performed by changing correlations to these new relations.

5. CONCLUSION

This paper presents a cipher-only attack method on row-column shuffle based image encryptions, by means of the spread high redundancy remained in cipher image. With this method, one single encrypted image by any such kind encryption can be deciphered. Although this attack is carried out for shuffle-only encryption, it is also a potential threat to shuffle-scramble combined encryption algorithms for those imperfect scramble.

6. REFERENCES

[1] Bianchi, T., Piva, A. and Barni, M. 2008. Discrete cosine transform of encrypted images. In *Proceedings of the 2008 International Conference on Image Processing* (San Diego, USA, Oct. 12- 15, 2008), 1668-1671. DOI= http://dx.doi.org/10.1109/ICIP.2008.4712093.

[2] Patidar, V., Pareek, N.K., Purohit, G. and Sud, K.K. 2011. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics Communications.* 284, 19 (Sep. 2011), 4331-4339. DOI=http://dx.doi.org/10.1016/j.optcom.2011.05.028.

[3] Bigdeli, N., Farid, Y. and Afshar, K. 2012. A robust hybrid method for image encryption based on Hopfield neural network. *Computers and Electrical Engineering.* 38, 2 (Mar. 2012), 356-369. DOI= doi:10.1016/j.compeleceng.2011.11.019.

[4] Zhang, D., Gu, Q., Pan, Y. and Zhang, X. 2008. Discrete chaotic encryption and decryption of digital images. In *Proceedings of the 2008 International Conference on Computer Science and Software Engineering* (Wuhan, China, Dec. 12 - 14, 2008), 849-852. DOI= http://doi.ieeecomputersociety.org/10.1109/CSSE.2008.1165 .

[5] Li, C.Q., Lo, K.T. 2011. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plain text attacks. *Signal Processing*. 91, 4 (Apr. 2011), 949-954. DOI= http://dx.doi.org/10.1016/j.sigpro.2010.09.014.

[6] Li, S.J., Li, C.Q., Chen, G.R., Bourbakisc, N.G. and Lo, K.T. 2008. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing : Image Communication*. 23, 3 (Mar. 2008), 212-223. DOI= http://dx.doi.org/10.1016/j.image.2008.01.003.

[7] Sam, I.S., Devaraj, P. and Bhuvaneswaran, R.S. 2011. Chaos based image encryption scheme based on enhanced logistic map. *Lecture Notes in Computer Science*. 6536 (2011), 290-300. DOI= http://dx.doi.org/10.1007/978-3-642-19056-8_22.

[8] Patidar, V., Purohit, G., Sud, K.K. and Pareek, N.K. 2010. Image encryption through a novel permutation-substitution scheme based on chaotic standard map. In *Proceedings of 2010 International Workshop on Chaos-Fractal Theories and Applications* (Dalian, China, Oct. 29 – 31, 2010), 164-169. DOI=http://dx.doi.org/10.1109/IWCFTA.2010.58.