On the Security of an Image Encryption Method

Shujun Li[1] *and Xuan Zheng*[2]

[1] Institute of Image Processing, School of Electronics and Information Engineering
Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China
[2] Department of Electrical Engineering, Polytechnic University
5 MetroTech Center, Brooklyn, NY 11201

ABSTRACT

The security of digital images attracts much attention recently, and many different image encryption methods have been proposed. In 1999, J.-C. Yen and J.-I. Guo proposed a novel image encryption algorithm called BRIE (Bit Recirculation Image Encryption). This paper points out that BRIE is not secure enough from strict cryptographic viewpoint. It has been found that some defects exist in BRIE, and a known/chosen-plaintext attack can break BRIE with only one known/chosen plain-image. Experiments are made to verify the defects of BRIE and the feasibility of the attack.

1. INTRODUCTION

In the digital world nowadays, the security of digital images becomes more and more important since the communications of digital products over open network occur more and more frequently. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications and confidential video conferencing, etc. In order to fulfill such a task, many image encryption methods have been proposed [1–7], but some of them [2, 6, 7] have been known to be insecure [3, 8, 9].

In [1], a novel image encryption method called BRIE (Bit Recirculation Image Encryption) is proposed, which is a pixel transformation cipher. This paper points out some security defects in BRIE, and presents a known/chose-plaintext attack to break BRIE with only one known/chosen plain-image. Generally speaking, BRIE is not secure from strongly cryptographic viewpoint and should not be used in any strict applications.

This paper is organized as follows. In Sect. 2, we firstly give a brief introduction of BRIE. The detailed analyses about the security defects of BRIE are made in Sect. 3. The know/chosen-plaintext attack is proposed in Sect. 4. Experimental results are also included in Sect. 3 and 4. Section 5 briefly discusses how to improve BRIE, and the last section concludes this paper.

2. BRIE ALGORITHM

The basic idea of BRIE is the bit recirculation of the pixels, which is controlled by a chaotic pseudo-random binary sequence. The secret keys of BRIE are two integers α, β and the initial condition $x(0)$ of a one-dimensional chaotic system. Assume the size of the plain-image is $M \times N$. Run the chaotic system to make a chaotic orbit $\{x(i)\}_{i=0}^{\lceil (MN+1)/8\rceil -1}$. Then generate a pseudo-random binary sequence (PRBS) $\{b(i)\}_{i=0}^{MN}$ from the 8-bit binary representation of $x(i) = 0.b(8i+0)b(8i+1)\cdots b(8i+7)$. For the plain-pixel $f(x,y)(0 \leq x \leq M-1, 0 \leq y \leq N-1)$, the cipher-pixel $f'(x,y)$ is determined by the following equation:

$$f'(x,y) = ROLR_p^q(f(x,y)), \tag{1}$$

where $p = b(N \times x + y), q = \alpha + \beta \times b(N \times x + y + 1)$ and $ROLR_p^q$ is a cyclical shift by q bits in a direction controlled by p:

$$ROLR_p^q(x = b_7 b_6 \cdots b_0) = \begin{cases} \sum\limits_{i=0}^{7} b_i \cdot 2^{(i-q+8) \bmod 8}, & p = 0 \\ \sum\limits_{i=0}^{7} b_i \cdot 2^{(i+q) \bmod 8}, & p = 1 \end{cases}. \tag{2}$$

The decryption procedure can be denoted by

$$f(x,y) = ROLR_{1-p}^q(f'(x,y)) = ROLR_p^{8-q}(f'(x,y)). \tag{3}$$

Apparently, BRIE is a pixel transformation cipher, i.e., the cipher-pixel at (x,y) is uniquely determined by the plain-pixel at the same position. The authors of [1] claim that BRIE needs very low computation complexity, and has high security since $\{b(i)\}$ contains $MN+1$ secure bits generated by the chaotic iterations. However, we will point out that some serious defects exist in BRIE, and that a known/chosen-plaintext attack can break it. The BRIE encrypts the plain-image column by column, which is somewhat inconvenient in practice. In this paper, we modify BRIE to work in line mode, which will not essentially influence the security of BRIE.

3. SOME DEFECTS OF BRIE

3.1. Essential Defects of $ROLR$ Operations

The $ROLR$ operations controlled by pseudo-random chaotic sequence $\{b(i)\}$ are the kernel of BRIE. But $ROLR$ have two essential defects when it is used in BRIE, which both lower the security of BRIE and limit its applications in practice.

1) Some plain-pixels may keep unchanged ($f'(x,y) = f(x,y)$) after encryption. If there are too many such pixels, the plain-image will roughly emerge from the cipher-image. The plain-pixels can be divided into the following four classes[1]. **C1**) 0, 255: $f'(x,y) \equiv f(x,y), \forall \alpha, \beta$. **C2**) 85, 170: If $\alpha \bmod 2 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha$; if $\alpha + \beta \bmod 2 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha + \beta$; and if $\alpha \bmod 2 = (\alpha + \beta) \bmod 2 = 0$,

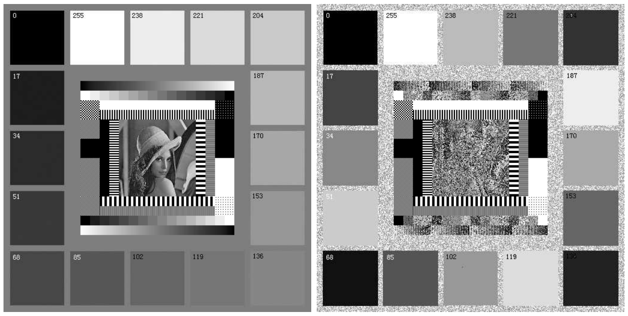
This paper has been published in *Proceedings of the 2002 IEEE International Conference on Image Processing* (ICIP 2002), vol. 2, pp. 925-928, 2002, IEEE.

Please contact us via `http://www.hooklee.com`.

[1] Different repeated patterns exist in the binary representation of different pixels: C1) eight repeated bits – 0 (00000000), 1 (11111111); C2) four repeated 2-bit segments – 85 (01010101), 170 (10101010); C3) two repeated 4-bit segments – 17 (00010001), etc.; C4 – no repeated pattern.

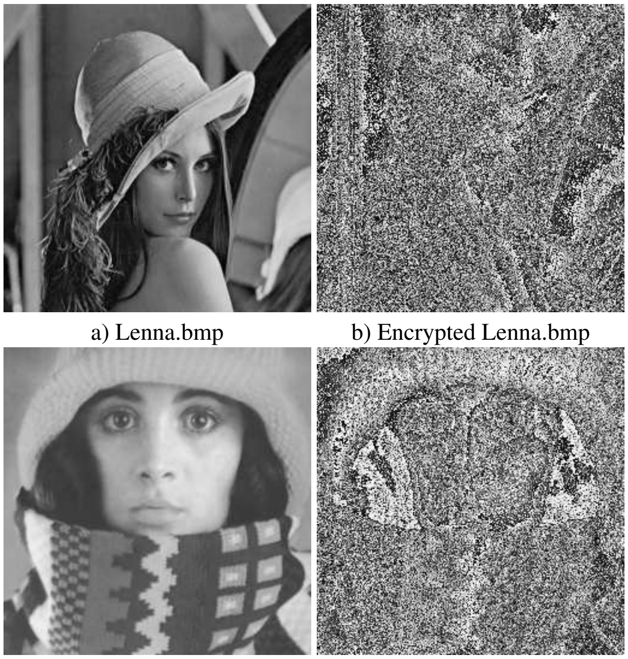
$f'(x,y) \equiv f(x,y)$. **C3)** 17, 34, 51, 68, 102, 119, 136, 153, 187, 204, 221, 238: If $\alpha \bmod 4 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha$; if $\alpha + \beta \bmod 4 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha + \beta$; and if $\alpha \bmod 4 = (\alpha+\beta) \bmod 4 = 0$, $f'(x,y) \equiv f(x,y)$. **C4)** All other gray values: If $\alpha \bmod 8 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha$; if $\alpha+\beta \bmod 8 = 0$, $f'(x,y) = f(x,y)$ when $q = \alpha+\beta$; and if $\alpha \bmod 8 = (\alpha+\beta) \bmod 8 = 0$, $f'(x,y) \equiv f(x,y)$.

2) For a sub-region in the plain-image with fixed gray value, at most eight[2] gray values will be contained in the corresponding sub-region of the cipher-image. Such a fact will make the edge of this sub-region appear in the cipher-image.



a) Test_Pattern.bmp b) Encrypted Test_Pattern.bmp

Fig. 1. A special image encrypted with BRIE



a) Lenna.bmp b) Encrypted Lenna.bmp

c) Miss.bmp d) Encrypted Miss.bmp

Fig. 2. Lenna.bmp and Miss.bmp encrypted by BRIE, $\alpha = 5, \beta = 1, x(0) = 0.75$

Apparently, if the cipher-image have many unchanged pixels and/or the plain-image have many sub-regions with fixed gray values, it will be possible to obtain some useful information about the plain-image by only observing the cipher-image. In Fig. 1, we give the experimental result about a specially designed image, which contains pixels in all four classes (The gray values of the 16 squares are respectively 0, 17, 34, ..., 221, 238, 255). The related parameters are $\alpha = 2, \beta = 4, x(0) = 0.75$ and the chaotic system is selected as logistic map with control parameter 3.9.

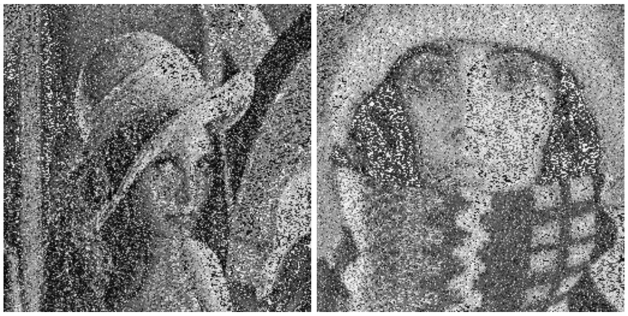
In fact, the second fact can be extended to more general case. For a given sub-region, if all gray values are close and only a few LSBs of the values are different, there will be enough similar pixels in the sub-cipher-region to cause the edge to emerge in the cipher-image. Generally speaking, the larger the sub-region is and the closer the gray values are, the more clear the edge will be. In Fig. 2, Lenna.bmp and Miss.bmp are shown as examples. In the cipher-images, we can find many important edges of the plain-images.

3.2. Security Problem about α, β

The selection of α, β is not mentioned in [1]. We find α, β must yield the following three restrictions to avoid possible insecurity, the number of such values is only $7 \times 7 - 7 - 2 = 40$, which is dramatically small and will be useful for cryptanalysis.

R1) $\boldsymbol{1 \le \alpha \le 7, 1 \le \beta \le 7}$. Consider $ROLR_p^q = ROLR_p^{q+8}$, this restriction is natural.

R2) $\boldsymbol{\alpha + \beta \neq 8}$. If $\alpha + \beta = 8$, beyond half pixels will obey $f'(x,y) = f(x,y)$ (recall the discussion in the last subsection). Such a fact will cause the plain-image is roughly leaked from the cipher-image. In Fig. 3, we give the results about Lenna.bmp and Miss.bmp when $\alpha = 6, \beta = 2, x(0) = 0.75$.



a) Encrypted Lenna.bmp b) Encrypted Miss.bmp

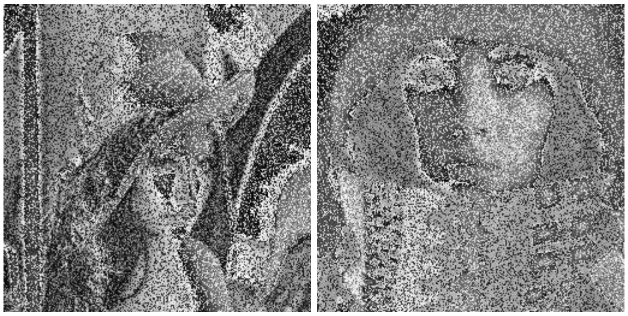
Fig. 3. Lenna.bmp and Miss.bmp encrypted by BRIE, $\alpha = 6, \beta = 2, x(0) = 0.75$ (compare them with Fig. 2)

R3) $\boldsymbol{\alpha \bmod 8 \neq 1, 7}$ or $\boldsymbol{(\alpha+\beta) \bmod 8 \neq 1, 7}$. If the restriction is not satisfied (when $\alpha = 1, \beta = 6$ or $\alpha = 7, \beta = 2$), all plain-pixels will be encrypted by one-bit $ROLR$ operation since $ROLR_p^7 = ROLR_{1-p}^1$ and $ROLR_p^9 = ROLR_p^1$. Consequently, rather larger visual information of the plain-image will leak from the cipher-image. When $\alpha = 1, \beta = 6, x(0) = 0.75$, the results about Lenna.bmp and Miss.bmp are given in Fig. 4. We can see the cipher-images contain so many strong edges that one eavesdropper can guess the plain-image.

3.3. Low Practical Security to Brute-Force Attack

In [1], the authors claimed that there are 2^{MN+1} possible encryption results since the cipher-image is determined by $\{b(i)\}_{i=0}^{MN}$. Because all $\{b(i)\}$ keep secret to illegal users and the reconstruction of the chaotic orbit $\{x(i)\}_{i=0}^{\lceil (MN+1)/8 \rceil - 1}$ is rather difficult, BRIE is secure enough. However, the above statement is not true because of the following fact: total $MN + 1$ bits are uniquely determined by the chaotic system and its initial condition $x(0)$. Once one gets $x(0)$, he can easily reconstruct $\{b(i)\}_{i=0}^{MN}$ to decrypt the cipher-image. $x(0)$ can be determined by brute-force

[2] The number is determined by the fixed gray value: C1 – 1, C2 – 1 or 2, C3 – 1 $\sim$ 4, C4 – 1 $\sim$ 8.



a) Encrypted Lenna.bmp b) Encrypted Miss.bmp

Fig. 4. Lenna.bmp and Miss.bmp encrypted by BRIE, $\alpha = 1, \beta = 6, x(0) = 0.75$ (compare them with Fig. 2)

searching. Of course, to break BRIE, we also should know α, β besides $x(0)$.

Now let us calculate the total number of available secret keys. Assume the chaotic systems is iterated with floating-point arithmetic of double precision, then $x(0)$ will have 63 meaningful bits (the sign bit must be zero since $x(0) \geq 0$). Consider the number of available α, β is 40, the total number of keys is 40×2^{63}.

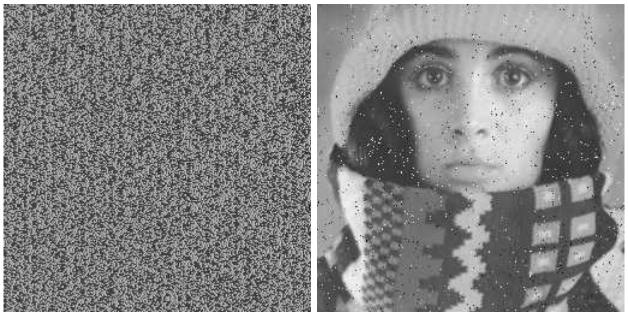
The exact computation complexity of the brute-force attack is estimated as follows. For each key, $\lfloor (MN+1)/8 \rfloor$ chaotic iterations are needed to generate $\{b(i)\}_{i=0}^{MN}$, and MN $ROLR$ operations are needed to decrypt the cipher-image. Assume one chaotic iteration and one $ROLR$ operation consume same time, the average attack complexity of BRIE to brute-force attack will be $(40 \times 2^{63}/2) \times 9(MN+1)/8 \approx 2^{67.5} \times MN$, which is much smaller than 2^{MN} when M, N are not too small. Assume $M = N = 512 = 2^9$, which is the typical size of a "large" digital image, the attack complexity will be only $2^{67.5} \times MN = 2^{85.5} \ll 2^{MN} = 2^{262144}$. Consider the rapid progress of digital computers and distributed arithmetic, the complexity is required to be not lower than 2^{128} for a strict cipher [10]. Apparently, BRIE can not provide enough security. As a result, the security of BRIE is overestimated by the authors of [1], even under brute-force attack.

4. KNOWN/CHOSEN-PLAINTEXT ATTACK

If one can get only one plain-image, he can break BRIE easily and fast, which corresponds to the known/chosen-plaintext attack in cryptanalysis. As we know, the known-plaintext and chosen-plaintext attacks will be very meaningful if a same key is used to encrypt more than one plaintexts, especially in the case that a larger number of plaintexts are all encrypted with a same key. For a "good" cipher, the capability to resist known-plaintext attack is very important and generally needed. It is because of the following fact: the key management will be very complex, inconvenient and inefficient in many applications, if any key must not be used to encrypt more than one plaintexts [10].

4.1. Breaking BRIE with Mask Array Q

Assume the known/chosen plain-image is f and its cipher-image is f' (both $M \times N$). For the plain-pixel $f(x,y)$, the cipher-pixel $f'(x,y)$ must be one of the 8 values: $ROLR_0^1(f(x,y)) \sim ROLR_0^7(f(x,y))$. By comparing $f(x,y)$ and $f'(x,y)$, we can easily find at least one integer [3] $q(x,y)$, which satisfies $f'(x,y) = ROLR_0^{q(x,y)}(f(x,y))$. Repeat this procedure, we can get a mask array $Q = [q(x,y)]_{M \times N}$. If $f(x,y)$ is a gray value in class C4 (recall Sect. 3.1), $q(x,y)$ can be used to decrypt any cipher-pixels at (x,y). If $f(x,y)$ is a gray value in class $C1 \sim C3$, generally $q(x,y)$ cannot be used to decrypt cipher-pixels at (x,y). Fortunately, for most digital images, the number of $C1 \sim C3$ pixels is much smaller than C4 pixels. Consequently, the mask array Q can be employed to decrypt other cipher-images encrypted by BRIE with same keys. If the size of the cipher-images is not larger than the size of Q, the plain-images can be entirely recovered except a few plain-pixels. Select Lenna.bmp as the known/chosen plain-image, we obtain a mask array Q and then successfully cryptanalyze the cipher-image of Miss.bmp. The mask array Q and decrypted Miss.bmp are given in Fig. 5, where Q is transformed to a pseudo-random image f_Q as follows: $F_Q(x,y) = q(x,y) \times 32$. We can see a few pixels in Miss.bmp cannot be correctly cryptanalyzed because of the corresponding pixels in Lenna.bmp are $C1 \sim C3$ pixels.



a) Mask array Q b) Decrypted Miss.bmp by Q

Fig. 5. Cryptanalyze Miss.bmp using mask array Q generated from known/chosen Lenna.bmp, $\alpha = 5, \beta = 1, x(0) = 0.75$

Using Q as the cryptanalytic tool has two problems: a) For a cipher-image whose size is larger than $M \times N$, only $M \times N$ pixels can be recovered. If the image is much larger than $M \times N$, the recovered part cannot reflect the whole scene of the plain-image. See Fig. 6 for the cryptanalytic result of a larger image Peppers.bmp, whose size is 384×384 (larger than 256×256). b) If the known/chosen image contains too less C4 pixels, there will not be enough efficient $q(x,y)$ to decrypt cipher-pixels. The second problem can be overcome by increasing the number of known/chosen plain-images.

4.2. Finding the Secret Keys from Q

Obviously, the best solution to the problems of Q is to get the secret keys of BRIE α, β and $x(0)$. Once Q is obtained, we can deduce α, β and equivalent $x(0)$ by the following steps.

Step 1: Divide the known/chosen plain-image into 8-pixel blocks, and find a C4 pixel $f(x^*, y^*)$ followed by 2 consecutive C4 blocks[4] (generally it is easy for most images).

Step 2: Assume $\alpha' = 1 \sim 7$ and $\beta' = 1 \sim 7$.

Step 3: If α' and/or β' disobey the restrictions **R1**, **R2** and **R3** described in Sect. 3.2, go to **Step 2**;

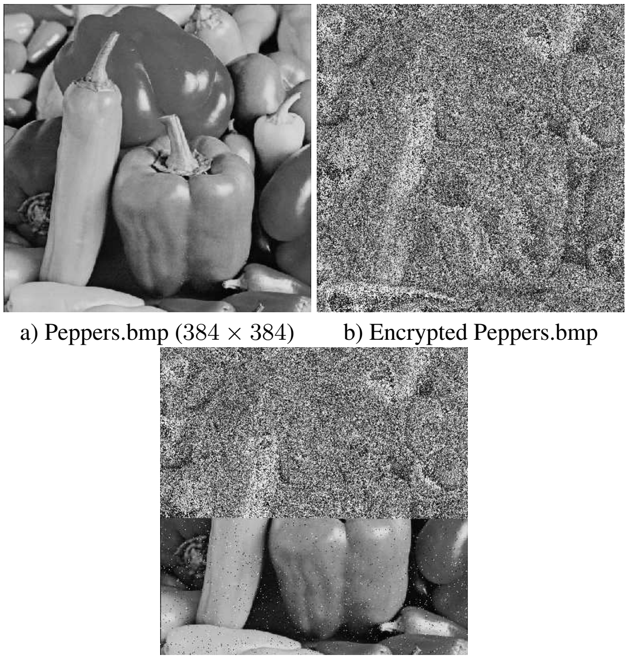
Step 4: Calculate the following four values: $q(1) = \alpha', q(2) = (\alpha' + \beta') \bmod 8, q(3) = 8 - q(1), q(4) = (8 - q(2)) \bmod 8$.

Step 5: Get 16 bits $\{b(1), \cdots, b(i), \cdots, b(16)\}$ from the mask values $q(x,y)$ corresponding to the 16 C4 plain-pixels starting from $f(x^*, y^*)$ as follows[5]:

[3] If $f(x,y)$ belongs to class C4, only unique such integer exists. For class C1, the number of such integers are 8; for C2, the number is 4; for C3, the number is 2.

[4] Here, "C4 block" means that all pixels in this block are C4 pixels.

[5] Note that $\{q(1), q(3)\} \cap \{q(2), q(4)\} = \varnothing$ for any α, β.



a) Peppers.bmp (384 × 384) b) Encrypted Peppers.bmp

c) Decrypted Peppers.bmp by Q

Fig. 6. Cryptanalyze Peppers.bmp using mask array Q generated from known/chosen Lenna.bmp, $\alpha = 5, \beta = 1, x(0) = 0.75$

- if $q(x,y) \notin \{q(1), q(2), q(3), q(4)\}$, go to **Step 2**;
- if $q(x,y) \in \{q(1), q(3)\}$, $b(i) = 0$;
- if $q(x,y) \in \{q(2), q(4)\}$, $b(i) = 1$.

Step 6: Generate two binary decimals using $b(1) \sim b(16)$: $x1 = \sum_{i=1}^{8} b(i) \times 2^{-i}$ and $x2 = \sum_{i=1}^{8} b(i+8) \times 2^{-i}$.
Step 7: If $x2$ and $x1$ yield the equation of the employed chaotic system, mark the current α' and β' as a candidate for the right α and β. Go to **Step 2** until $\alpha' = 7$ and $\beta' = 7$.
Step 8: Search the right α and β in all marked candidates.
Step 9: Brute-forcedly search the other $n - 8$ bits of $x1$, where n is the meaningful bit number of the chaotic orbit.

In the above procedure, if the 16 continuous C4 pixels are the first 16 pixels of plain-images, then $x1 = x(0)$; otherwise $x1$ is a equivalent key of $x(0)$ since $x1$ also can be used to generate chaotic sequence after $x1$. The search complexity of the above procedure is chiefly determined by **Step 9**. When $n = 63$ (double precision floating-point arithmetic), it is 2^{55}, which is still rather large. But compared with the complexity of simple brute-force attack (see Sect. 3.3), the key entropy decreases by at least $\log_2(40 \times 2^8) \approx 13.3$ bits.

5. IMPROVING BRIE

To improve the security of BRIE to brute-force attack and the attack of getting the secret keys from Q, some simple modifications will be efficient, such as increasing the bit number of $x(0)$, adding control parameters of the chaotic system to the secret keys. But neither of them can improve the security to the known/chosen-plaintext attack with Q.

To escape from the known/chosen-plaintext attack based on Q, some complicated modifications should be made, such as cascading an extra cipher to perturb the cipher-image after BRIE [10], or using pseudo-randomly generated α and β by cipher-pixels or added secret keys [11,12]. Here, the security of the modified BRIE will be ensured by the new parts, not the BRIE itself.

6. CONCLUSION

In this paper, we point out the insecurity of a novel image encryption method proposed in [1]. Detailed cryptanalytic investigations are given and a known/chosen-plaintext attack is presented to break this image encryption method. We suggest not using it in strict applications, except it can be ensured that any secret key will never been used repeatedly to encrypt more than one plain-images.

7. ACKNOWLEDGEMENT

The authors would like to thank Dr. Xuanqin Mou and Prof. Yuanlong Cai at Xi'an Jiaotong University for their supports on this paper, Miss Yanghui Cao and Luhua Gong at Xi'an Jiaotong University for their helps in the preparation of this paper. Also, we thank one anonymous reviewer for his/her useful comments to enhance the clarity of this paper.

8. REFERENCES

[1] Jui-Cheng Yen and Jiun-In Guo, "A new image encryption algorithm and its VLSI architecture," in *Proc. IEEE Workshop Signal Processing Systems*, 1999, pp. 430–437.

[2] Jui-Cheng Yen and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," in *Proc. IEEE ISCAS*, 2000, vol. 4, pp. 49–52.

[3] Howard Cheng and Xiaobo Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[4] Jiri Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[5] Josef Scharinger, "Fast encryption of image data using chaotic kolmogrov flows," *J. Electronic Imaging*, vol. 7, no. 2, pp. 318–325, 1998.

[6] Henry Ker-Chang Chang and Jiang-Long Liu, "A linear quadtree compression scheme for image encryption," *Signal Processing: Image Communication*, vol. 10, pp. 279–290, 1997.

[7] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou, "Image encrytion method using a class of fractals," *J. Electronic Imaging*, vol. 4, no. 3, pp. 251–259, 1995.

[8] Jinn-Ke Jan and Yuh-Min Tseng, "On the security of image encryption method," *Information Processing Letters*, vol. 60, pp. 261–265, 1996.

[9] Shujun Li and Xuan Zheng, "Cryptanalysis of a chaotic image encryption method," *Proc. IEEE ISCAS 2002*, to be published.

[10] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., New York, second edition, 1996.

[11] Tohru Kohda and Akio Tsuneda, "Statistics of chaotic binary sequences," *IEEE Trans. Information Technology*, vol. 43, no. 1, pp. 104–112, 1997.

[12] Li Shujun, Mou Xuanqin, and Cai Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *Progress in Cryptology - INDOCRYPT 2001*. 2001, Lectuer Notes in Computer Science, vol. 2247, pp. 316–329, Springer-Verlag, Berlin.