Cryptanalysis on an Image Scrambling Encryption Scheme Based on Pixel Bit

Liang Zhao *, † Avishek Adhikari ‡ Di Xiao † Kouichi Sakurai *

* Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan

†College of Computer Science, Chongqing University, China

‡ Department of Pure Mathematics, University of Calcutta, India

This research is supported by The Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications with Other Fields Supported by Japan Science and Technology Agency and Department of Science and Technology of the Government of India, and The Governmental Scholarship From China Scholarship Council (CSC).

zhaoliang@itslab.csce.kyushu-u.ac.jp

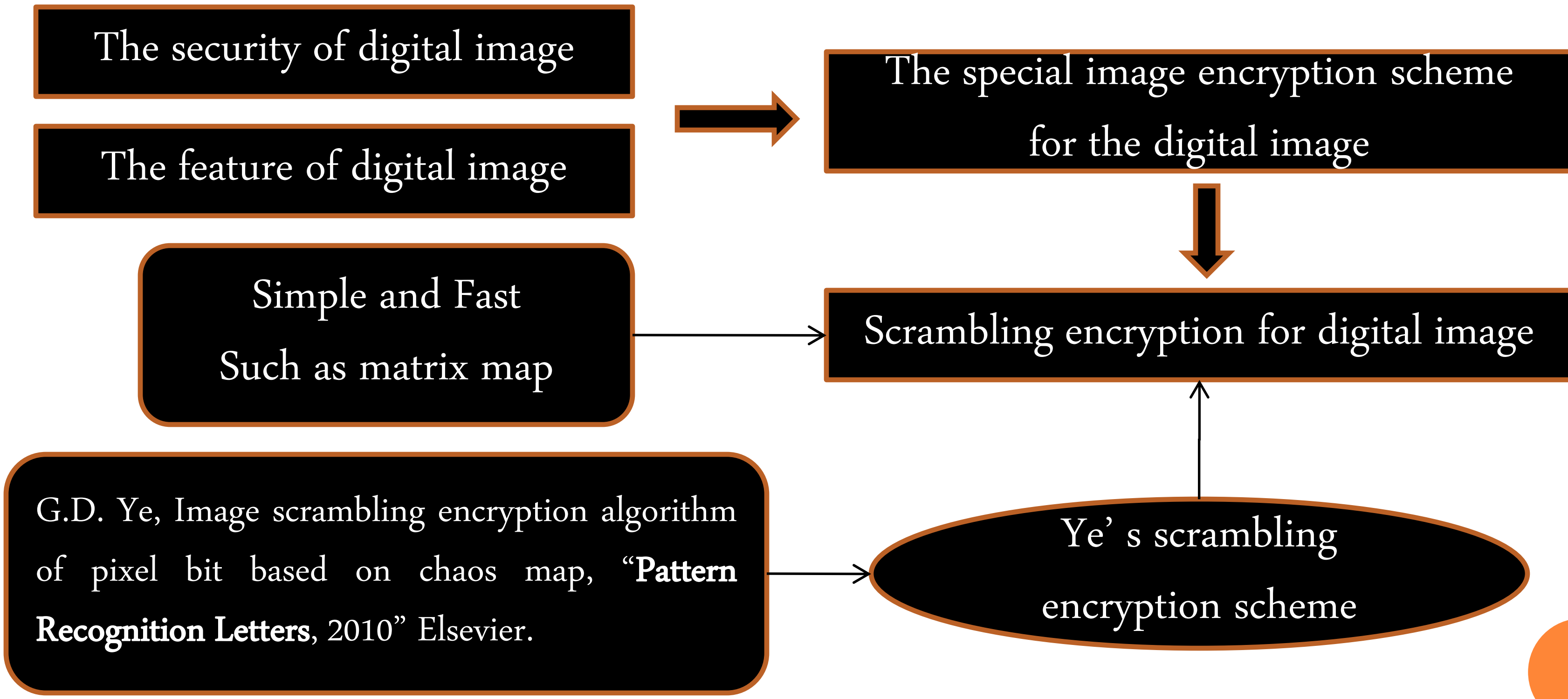
OUTLINE

- Description of Ye' s encryption scheme
- Some research examples about image analysis
- Drawbacks of original image encryption algorithm under study
- Effective attacks to original encryption under study
- Simulation result on proposed attacks
- Two details in proposed attacks
- Conclusions

zhaoliang@itslab.csce.kyushu-u.ac.jp

Description of Ye' s encryption scheme

- The background information about image encryption and Ye's image encryption scheme (2010, Published by Elsevier):



zhaoliang@itslab.csce.kyushu-u.ac.jp

Description of Ye' s encryption scheme

- The main feature of Ye' s image encryption scheme:

1. Based on the scrambling of bit-plane, for every bit (0 or 1), the encryption/decryption process is fast.

2. Ye' s scheme can encrypt the position of pixel and value of pixel at the same time.

This can be seen as the main contribute of Ye' s scheme

zhaoliang@itslab.csce.kyushu-u.ac.jp

Description of Ye' s encryption scheme

Ye's encryption scheme drives from the scrambling of pixels' positions with rows and columns exchange. (*M*× *N image(M* is the height and *N* is the width*),*)

$P^t(i, j)$ is binary number and t∈[0,1,2,3,4,5,6,7]

- One digital image should be presented as a decimal matrix *P*
- decimal pixel ⟶ bits sequence⟶*M*× *8N* binary matrix

$$x_{n+1}=\mu x_n(1\text{-}x_n) \quad P^t(i,j) = \begin{cases} 1 & if\ (P(i,j)/2^t) \bmod 2 = 1 \\ 0 & others \end{cases}$$

- The Logistic chaos system is used for producing the scrambling vectors: *TM and TN*

zhaoliang@itslab.csce.kyushu-u.ac.jp

Description of Ye' s encryption scheme

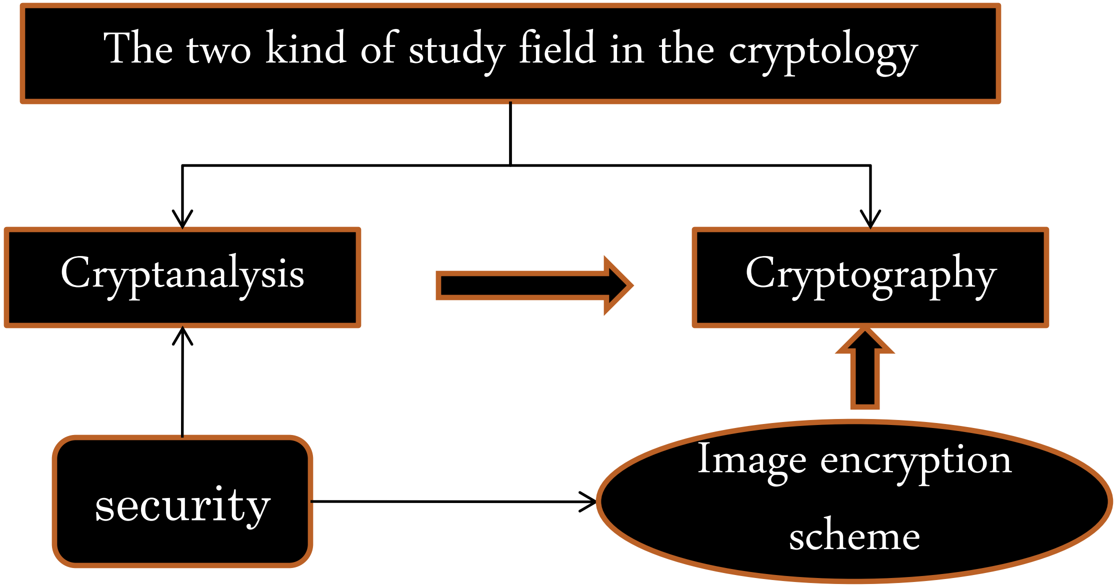
- The binary matrix is encrypted by the scrambling vectors *TM and TN*
- The final decimal cipher matrix *C* can be acquired

$$P(i,j)=\sum_{t=0}^{7}2^{t}\times P^{t}(i,j)$$

- The cipher matrix *C* → Cipher image

zhaoliang@itslab.csce.kyushu-u.ac.jp

Some research examples about image analysis



zhaoliang@itslab.csce.kyushu-u.ac.jp

Some research examples about image analysis

- Four attacks model for image analysis:
  - Cipher-text Only Attack
  - Known Plain-text Attack
  - Chosen Plain-text Attack
  - Chosen Cipher-text Attack

Analysis for image encryption scheme

zhaoliang@itslab.csce.kyushu-u.ac.jp

SOME RESEARCH EXAMPLES ABOUT IMAGE ANALYSIS

- Know plain-text attack-exe[C.C. Chang and T.X. Yu, Cryptanalysis of an encryption scheme for binary images, Pattern Recognition Lett., 2002]

The original binary image encryption scheme can be broken out with some pairs of plain image and cipher image[K.L. Chung and L.C. Chang, 1998]. By acquiring enough number of pairs of plain image and cipher image, the encryption rule can be found out.

- Know plain-text attack-exe[C. Cokal and E. Solak, Cryptanalysis of a chaos-based image encryption algorithm, Phys Lett. A. , 2009]

The chosen-plaintext and known-plaintext attacks are applied to attack the image encryption scheme based on chaos[Z.H. Guan et. al., 2005]. Two plain text–cipher text image($P(1)$, $C(1)$) and ($P(2)$, $C(2)$) are assumed, and the differences of P and C is used in Know plain-text attack.

zhaoliang@itslab.csce.kyushu-u.ac.jp

Some research examples about image analysis

- Chosen plain-text attack-exe[K. Wang et. al., On the security of 3D Cat map based symmetric image encryption scheme, Phys Lett A., 2005]

  A chosen-plain text attack is used for analyzing the 3D cat map based symmetric image encryption scheme[G.R. Chen et. al., 2004].

- Chosen plain-text attack-exe[D. Xiao et. al., Analysis and improvement of a chaos-based image encryption algorithm, Chaos, Solitons, Fract. , 2009]

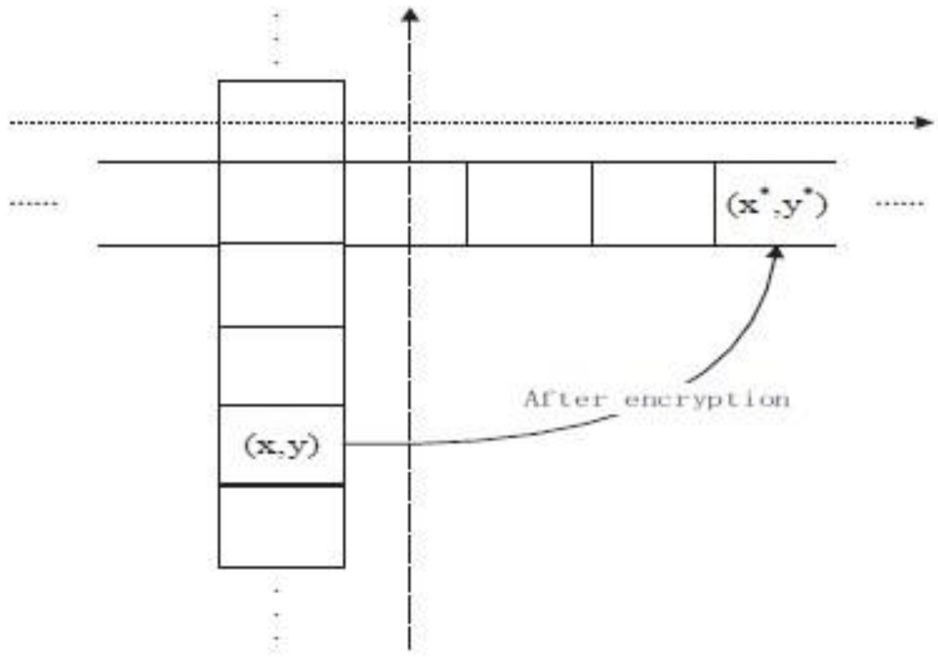
  The chosen-plaintext and known-plaintext attacks are used to recover the true secret keys of an typical image encryption scheme based on chaos[chaos[Z.H. Guan et. al., 2005]. For the chosen plain-text attack, there is no relation between plain-text image and cipher-text image which is utilized by attackers.

zhaoliang@itslab.csce.kyushu-u.ac.jp

Drawbacks of original image encryption algorithm under study

- Only implements the row and column exchange

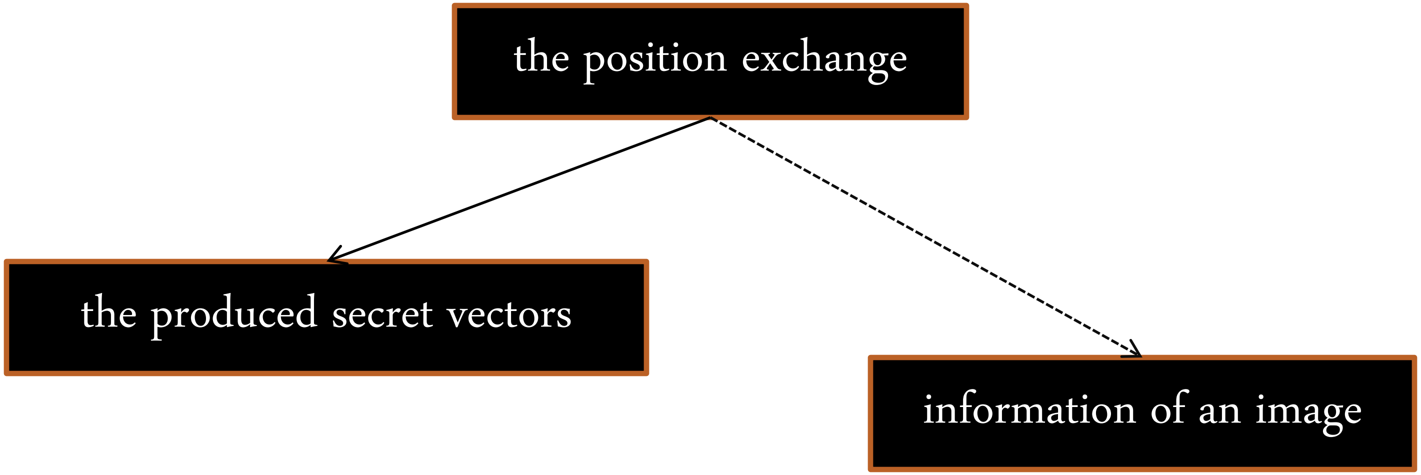
➡ the transformation range is confined into a narrow space



zhaoliang@itslab.csce.kyushu-u.ac.jp

Drawbacks of original image encryption algorithm under study

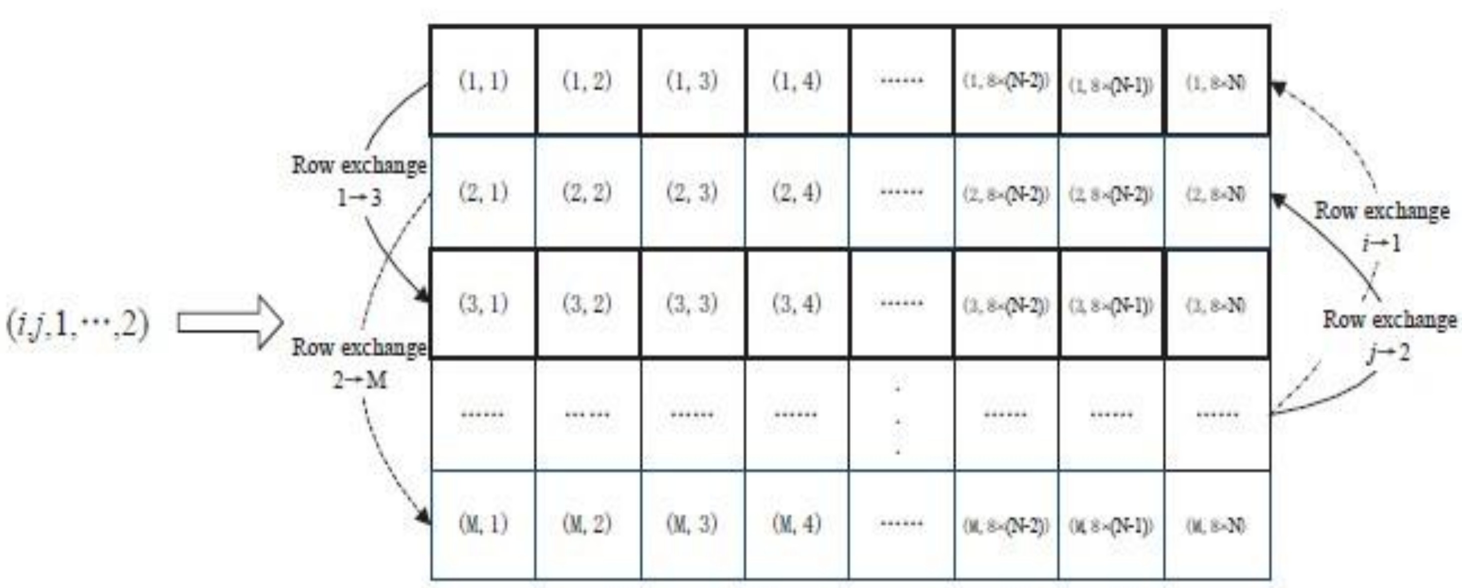
The corresponding relationship about the position exchange of pixel:



zhaoliang@itslab.csce.kyushu-u.ac.jp

Drawbacks of original image encryption algorithm under study

- One row or column has the same transform rule.



zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

- The two main leaks can be taken advantage of by attackers

Chosen plain-text attack

↓

Constructing some image used in the temporary encryption mechanism. After this encryption process, the attackers can get the useful information from the encrypted plain-text image, such as secret keys.

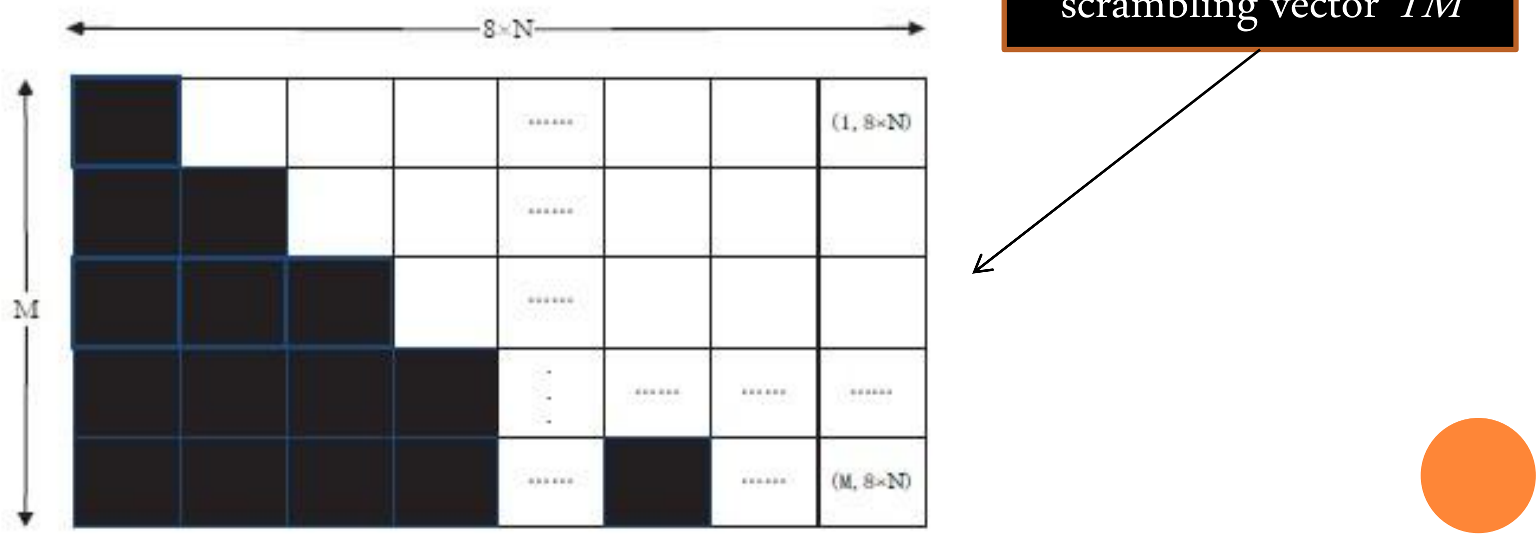
zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

- Two kinds of plain images are chosen for revealing the scrambling vectors: *TM* and *TN*

The RCM is used for revealing the TM.

The RCN is used for revealing the TN.



zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

Algorithm 1 For revealing the row scrambling vector TM

```
Step1
for i = 1 to M do
    for j = 1 to N do
        RCM(i, j) = 255;
    end for
end for
Step2
for i = 1 to M do
    for j = 1 to N do
        for g = 8(j − 1) + 1 to 8j do
            RCM′(i, g) = 1 ⇐ [RCM(i, j) ← Eq.(1)];
        end for
    end for
end for
Step3
for p = 1 to M do
    {e(k)|e(k) ⊆ {1, 2, 3, . . . , 8N}} ←Choose any k many y-coordinate(s) in
    {1, 2, 3, . . . , 8N};
    for u = 1 to k do
        RCM′(p, e(u)) ← 0;
    end for
end for
Step4
for i = 1 to M do
    for j = 1 to N do
        for g = 8(j − 1) + 1 to 8j do
            t ⇐ [RCM′(i, g) ← Eq.(2)];
        end for
        RCM(i, j) ← t;
    end for
end for
```

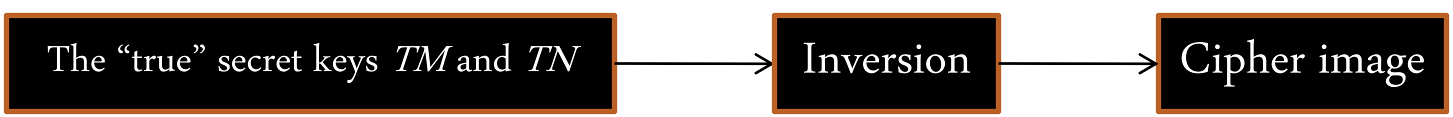

zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

- In order to get the scrambling vector *TN*, there are at least *8 RCN(i)* should be selected for usage.

The reason is that the width of the bit-plain is 8 times of the height

- The *RCM* and *RCN* are all used in the Ye' s image encryption scheme, and after the encryption process, some useful information about *TM* and *TN* can be get.
- *TM* and *TN* are obtained from this process.

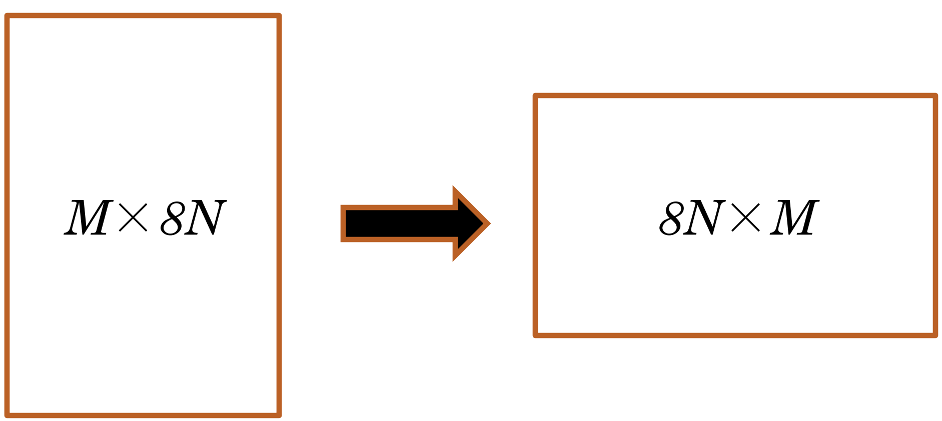


zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

Notice(1)

- The above attack is based on the fact that the height M is less than width $8N$. If M is larger than $8N$, the M and $8N$ should be exchanged firstly.



zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

Notice(2)

- For the *RCN(i)*, the number of i is decided by the size of *M* and *N*. That is to say, if the width *N* is larger than the height *M*, the number of i is more than 8.

Such as: $M \times N = 5 \times 8$, i is 13 for *RCN(i)*

zhaoliang@itslab.csce.kyushu-u.ac.jp

Effective attacks to original encryption under study

Notice(3)

- As the decryption process is the same as the encryption procedure except the "keys" for the decryption, the chosen-ciphertext attack can be also applied for revealing the "true" decryption keys. The crack procedure and the used chosen-ciphertext images are identical with the chosen-plaintext attack.

zhaoliang@itslab.csce.kyushu-u.ac.jp

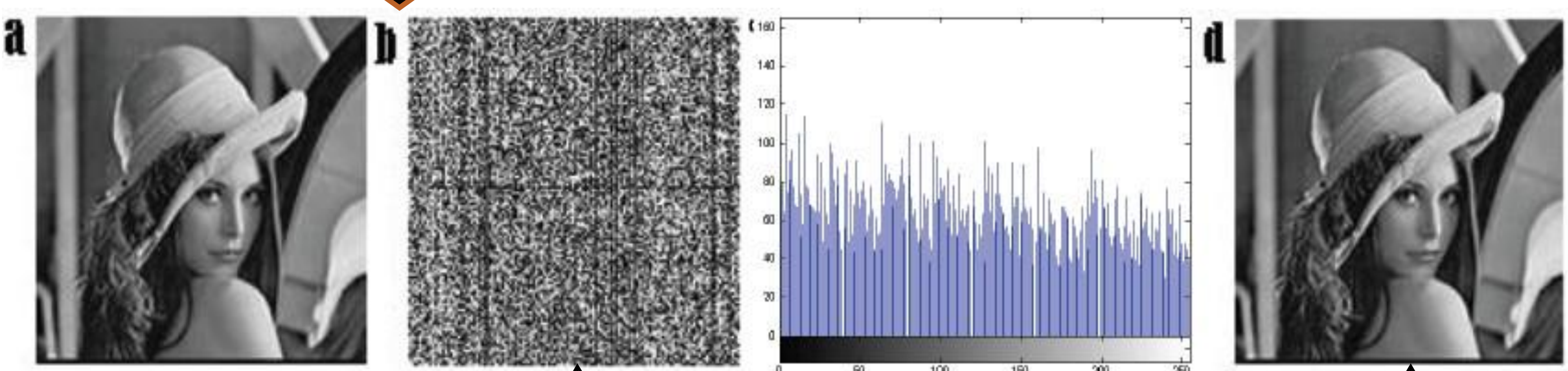
SIMULATION RESULT ON PROPOSED ATTACKS

The secret keys and corresponding parameters are chosen from the original example in original paper.

$x(0)$ and μ are the value of logistic system, m and n are set for getting the TM and TN

Ye' s encryption scheme

$x_0=0.2009$, $\mu=3.98$, $m=20$, $n=51$



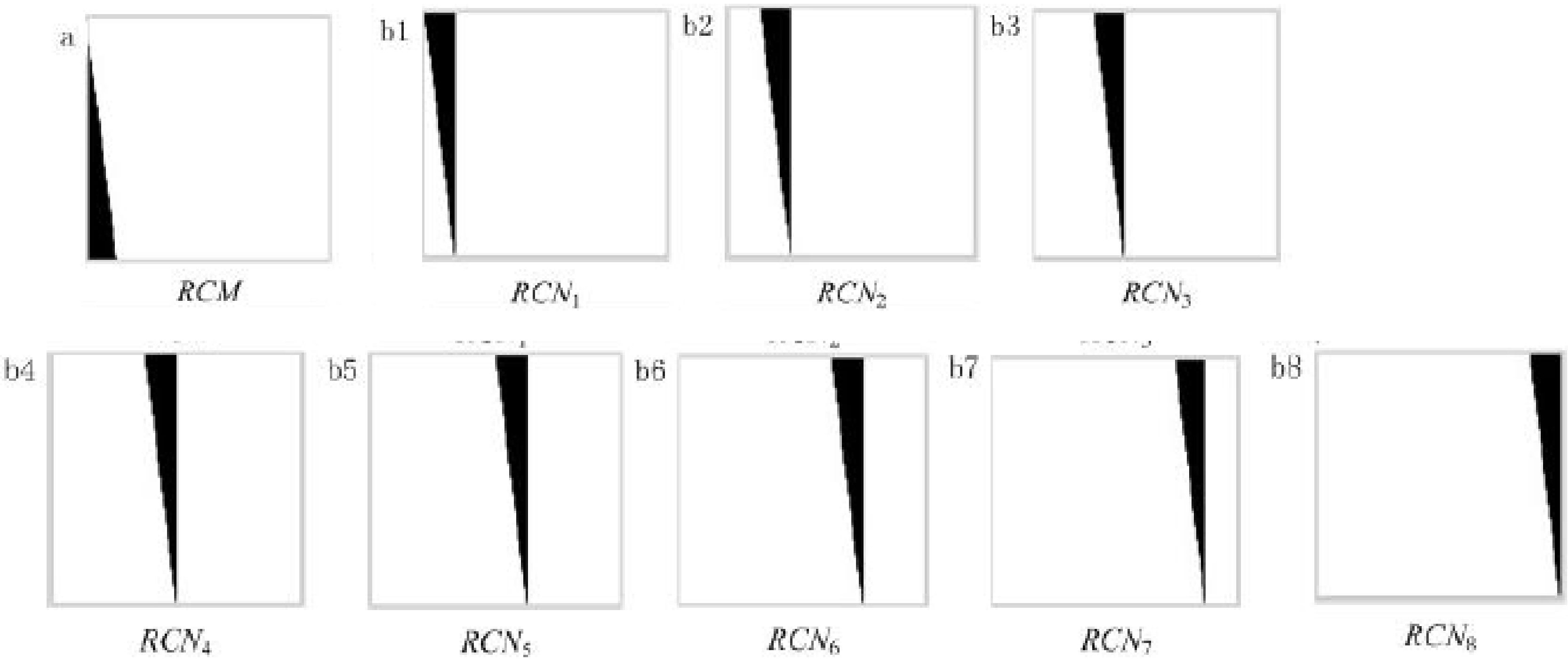
Cipher image

Decrypted image

zhaoliang@itslab.csce.kyushu-u.ac.jp

Simulation result on proposed attacks

- The *RCM* and *RCN*



zhaoliang@itslab.csce.kyushu-u.ac.jp

Simulation result on proposed attacks

c

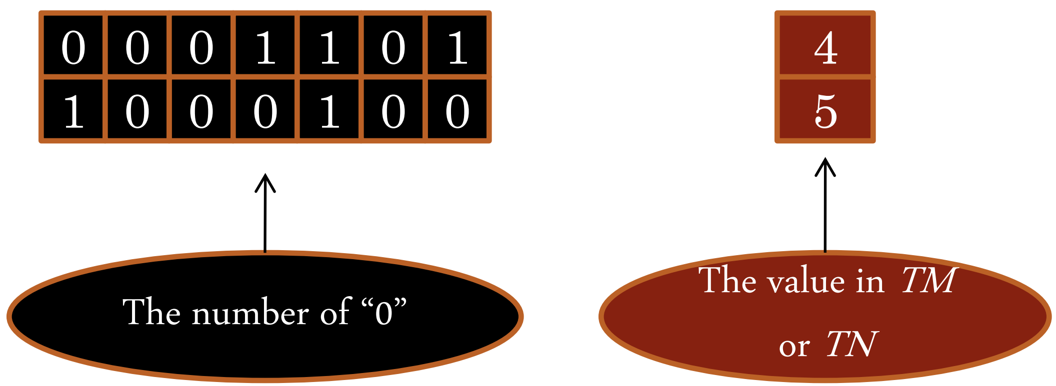
The recovered image

The recovered image

zhaoliang@itslab.csce.kyushu-u.ac.jp

Two details in proposed attacks

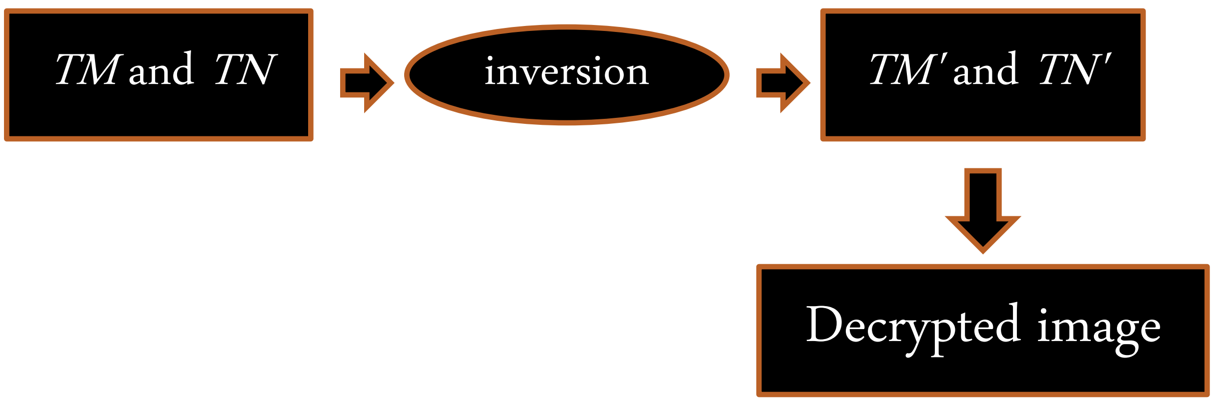
- When the chosen plain-text image is used in Ye' s image encryption scheme, for the $M \times 8N$ bit-plane image, the number of "0" is not changed and can be counted in the end. The number of "0" is the same as the value of TM or TN in one row or one column.



zhaoliang@itslab.csce.kyushu-u.ac.jp

Two details in proposed attacks

- The recovered vectors are not the decryption vectors TM' and TN'. The true decryption vectors are the inversion of TM and TN, and after this process, the corresponding vectors can be used for decryption.



zhaoliang@itslab.csce.kyushu-u.ac.jp

Conclusions

- The leaks of the Ye' s image encryption scheme are found.
- One kind of chosen plain-text attack and chosen cipher-text attack are proposed.
  - *At least 9 chosen plain images (cipher images) are used for obtaining the vectors TM and TN*
  - *For every chosen plain image (cipher image), the number of "0" is the corresponding value in TM and TN*

zhaoliang@itslab.csce.kyushu-u.ac.jp

Thank you very much every researcher

Detailed information:

- The chaos system used in this scheme.

The Logistic chaotic map is only used to produce the random number for constructing the vector *TM* and *TN*. As from our analysis, there is no need to consider which chaos system is used in this scheme. Our attack can directly recover the vector *TM* and *TN*.

Logistic chaotic map: $x_{n+1} = \mu x_n (1 - x_n)$

DETAILED INFORMATION:

- The size of digital image is relative with the chosen plain image.

For an image, if the size is $M \times 8N(M<8N)$, at least 8 *RCN(i)* is used in our attack. For every *RCN(i)*, it can recover part of value of *TN*. When all *RCN(i)* are encrypted, the final *TN* can be gotten.

At the same time, if $M \times 8N(M>8N)$, the *RCN* and *RCM* are constructed according to the exchanged size $M' = 8N$, $(8N)' = M$.

DETAILED INFORMATION:

- How to get the value in *TM* and *TN*.

The number of "0" of one row for the encrypted *RCM* is equal to the corresponding value in *TM*. For the *TN*, it is the same as *TM*. For one column, the number of "0" is equal to the corresponding value in *TN*.

Detailed information:

- Some other thinking about Ye’ s image encryption scheme.

(1) As the 8 bit-planes of one gray-scale image are only pass the scrambling process, the number of “0” and “1” are not changed no matter how many times one image is encrypted. This may be not suitable for image encryption principle since there is no diffusion in whole process.

Detailed information:

- Some other thinking about Ye’ s image encryption scheme.

(2) For some special images, such as an image with only “0” value or with only “255” value, the Ye’ s encryption scheme is ineffective and the cipher-text image is the same as the plain-text image. From this point, we can find that only scrambling for an image is not enough, and it can arrive at the purpose of encryption.