Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Comment:

Cryptanalysis of an image encryption scheme based on the Hill cipher[*]

Cheng-qing LI[†1], Dan ZHANG[2], Guan-rong CHEN[1]

([1]*Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong, China*)

([2]*School of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China*)

[†]E-mail: swiftsheep@hotmail.com

Received Dec. 19, 2007; revision accepted Feb. 5, 2008

Abstract: This paper studies the security of an image encryption scheme based on the Hill cipher (Ismail *et al*., 2006) and reports its following problems: (1) There is a simple necessary and sufficient condition that makes a number of secret keys invalid; (2) It is insensitive to the change of the secret key; (3) It is insensitive to the change of the plain-image; (4) It can be broken with only one known/chosen plaintext; (5) It has some other minor defects. The proposed cryptanalysis discourages any use of the scheme in practice.

Key words: Cryptanalysis, Encryption, Hill cipher, Known-plaintext attack, Chosen-plaintext attack
doi:10.1631/jzus.A0720102 **Document code:** A **CLC number:** TP309; TN918

INTRODUCTION

The history of cryptography can be traced back to the secret communication among people thousands of years ago. With the development of human society and industrial technology, theories and methods of cryptography have been changed and improved gradually, and meanwhile cryptanalysis has also been developed. In 1949, Shannon published his seminar paper "Communication theory of secrecy systems" (Shannon, 1949), which marked the beginning of the modern cryptology.

In the past two decades, the security of multimedia data has become more and more important. However, it has been recognized that the traditional text-encryption schemes cannot efficiently protect multimedia data due to such special properties of the multimedia data as strong redundancy and bulk size of the uncompressed data. To meet this challenge, a number of special image encryption schemes based on nonlinear theories were proposed (Li S., 2003; Li S. *et al*., 2004; Li C., 2005). Yet, many of them are found to be insecure from the viewpoint of cryptography (Li C. *et al*., 2004; 2005a; 2005b; 2006; 2007a; 2007b; Li S. *et al*., 2006; 2007; 2008a; 2008b; Alvarez and Li, 2006; Alvarez *et al*., 2007; Zhou *et al*., 2007).

Ismail *et al*.(2006) tried to encrypt images efficiently by modifying the classical Hill cipher (Hill, 1929). Their scheme was commented in (Rangel-Romero *et al*., 2008), and its following problems were found: (1) When m=2, one sub-key can be derived from another sub-key and m pairs of plaintext; (2) The scheme fails to encrypt the plaintext block of a fixed value zero; (3) Some invalid keys may exist (the condition is not discussed); (4) The period of sequence $\{\boldsymbol{K}_l\}$ may be very short (only the period corresponding to one set of secret keys was presented). This paper restudies the security of the scheme proposed by Ismail *et al*.(2006) and reports the following findings: (1) There exist a number of invalid secret keys; (2) The scheme is insensitive to the change of the secret key; (3) The scheme is insensitive to the change of the

[*] Project supported by the National Basic Research Program of China (No. 2006CB303104) and the City University of Hong Kong under the SRG Project, China (No. 7002134)

plain-image; (4) The scheme can be broken with only one known/chosen plain-image; (5) The scheme has some other minor performance defects.

The rest of this paper is organized as follows. The next section briefly introduces the encryption scheme to be studied. Section 3 presents some defects of the scheme. Section 4 discusses how to break the scheme with a known/chosen-plaintext attack. The last section concludes the paper.

IMAGE ENCRYPTION SCHEME TO BE STUDIED

The scheme proposed in (Ismail *et al.*, 2006) scans the gray scales of a plain-image $\boldsymbol{P}$ (or one channel of a color image) of size $M\times N$ in a raster order and divides it into $\lceil MN/m\rceil$ vectors of size m: $\{\boldsymbol{P}_l\}_{l=1}^{\lceil MN/m\rceil}$, where $\boldsymbol{P}_l=\{\boldsymbol{P}((l-1)m+1), \boldsymbol{P}((l-1)m+2), \ldots, \boldsymbol{P}((l-1)m+m)\}$ (the last vector is padded with some zero bytes if MN cannot be divided by m). Then, the vectors $\{\boldsymbol{P}_l\}_{l=1}^{\lceil MN/m\rceil}$ are encrypted in increasing order with the following function:

$$\boldsymbol{C}_l=(\boldsymbol{P}_l\boldsymbol{K}_l) \bmod 256, \tag{1}$$

where $\boldsymbol{K}_l=(\boldsymbol{K}_l[i,j])_{m\times m}$, $\boldsymbol{K}_l[i,j]\in\mathbb{Z}_{256}$, and the initial state of $\boldsymbol{K}_{l\geq2}$ is set to be $\boldsymbol{K}_{l-1}$. Then every row of $\boldsymbol{K}_l$ is generated iteratively with the following function:

$$\boldsymbol{K}_l[i,:]=(\boldsymbol{IV}\cdot\boldsymbol{K}_l) \bmod 256,\ i=1,2,\ldots,m, \tag{2}$$

where $\boldsymbol{IV}$ is a vector of size $1\times m$ and $\boldsymbol{IV}[i]\in\mathbb{Z}_{256}$. Finally, the cipher-image is obtained as $\boldsymbol{C}=\{\boldsymbol{C}_l\}_{l=1}^{\lceil MN/m\rceil}$.

The secret key of the encryption scheme includes three parts: m, $\boldsymbol{K}_1$, and $\boldsymbol{IV}$.

The decryption procedure is the same as the above encryption procedure except that Eq.(1) is replaced by the following function:

$$\boldsymbol{P}_l=(\boldsymbol{C}_l\boldsymbol{K}_l^{-1}) \bmod 256, \tag{3}$$

where $(\boldsymbol{K}_l\boldsymbol{K}_l^{-1}) \bmod 256=\boldsymbol{I}$, the identity matrix.

SOME DEFECTS OF THE SCHEME

Invalid keys

An invalid key is a key that fails to ensure the success of the encryption scheme. From the following Fact 1 and Corollary 1, one can see that one secret key in the above-described scheme is invalid if and only if $\gcd(\det(\boldsymbol{K}_1), 256)\neq1$ or $\boldsymbol{IV}[i] \bmod 2=0$ [In (Ismail *et al.*, 2006), it is only mentioned that $\boldsymbol{K}_1$ should satisfy $\gcd(\det(\boldsymbol{K}_1), 256)=1$].

Fact 1 A matrix $\boldsymbol{K}$ is invertible in $\mathbb{Z}_n$ if and only if $\gcd(\det(\boldsymbol{K}), n)=1$.

Proposition 1 $\det(\boldsymbol{K}_l)=\left(\prod_{i=1}^{m}\boldsymbol{IV}[i]\right)\det(\boldsymbol{K}_{l-1})$.

Proof According to Eq.(2), there is a relation between $\boldsymbol{K}_l$ and $\boldsymbol{K}_{l-1}$ as follows:

$$\boldsymbol{K}_l=\begin{pmatrix}\sum_{i=1}^{m}\boldsymbol{IV}[i]\boldsymbol{K}_{l-1}[i,:]\\ \boldsymbol{IV}[1]\boldsymbol{K}_l[1,:]+\sum_{i=2}^{m}\boldsymbol{IV}[i]\boldsymbol{K}_{l-1}[i,:]\\ \vdots\\ \sum_{i=1}^{m-1}\boldsymbol{IV}[i]\boldsymbol{K}_l[i,:]+\boldsymbol{IV}[m]\boldsymbol{K}_{l-1}[m,:]\end{pmatrix}\bmod 256. \tag{4}$$

Subtracting $\sum_{i=1}^{i_0-1}\boldsymbol{IV}[i]\boldsymbol{K}_l[i,:]$ from $\boldsymbol{K}_l[i_0,:]$ for $i_0=m, m-1, \ldots, 2$, one gets

$$\boldsymbol{K}_l'=\begin{pmatrix}\sum_{i=1}^{m}\boldsymbol{IV}[i]\boldsymbol{K}_{l-1}[i,:]\\ \sum_{i=2}^{m}\boldsymbol{IV}[i]\boldsymbol{K}_{l-1}[i,:]\\ \vdots\\ \boldsymbol{IV}[m]\boldsymbol{K}_{l-1}[m,:]\end{pmatrix}\bmod 256. \tag{5}$$

Subtracting $\boldsymbol{K}_l'[i_0,:]$ from $\boldsymbol{K}_l'[i_0-1,:]$ for $i_0=2, 3, \ldots, m$, one has

$$\boldsymbol{K}_l''=\begin{pmatrix}\boldsymbol{IV}[1]\boldsymbol{K}_{l-1}[1,:]\\ \boldsymbol{IV}[2]\boldsymbol{K}_{l-1}[2,:]\\ \vdots\\ \boldsymbol{IV}[m]\boldsymbol{K}_{l-1}[m,:]\end{pmatrix}\bmod 256. \tag{6}$$

Obviously,

$$\det(\boldsymbol{K}_l)=\det(\boldsymbol{K}_l')=\det(\boldsymbol{K}_l'')=\left(\prod_{i=1}^{m}\boldsymbol{IV}[i]\right)\det(\boldsymbol{K}_{l-1}),$$

which completes the proof of Proposition 1.

Corollary 1 $\det(\boldsymbol{K}_l)=\left(\prod_{i=1}^{m}\boldsymbol{IV}[i]\right)^{l-1}\det(\boldsymbol{K}_1)$.

Proof The result directly follows from Proposition 1.

Insensitivity to change of secret key

It is claimed in Section 5 of (Ismail *et al.*, 2006) that the encryption scheme is very sensitive to the change of the sub-keys $\boldsymbol{K}_1$ and $\boldsymbol{IV}$. This is not true.

Let us first study the influence on $\boldsymbol{K}_{l\geq 2}$ if only one bit of $\boldsymbol{K}_1$ is changed. Without loss of generality, assume that the nth bit of $\boldsymbol{K}_l[1,j_0]$ is changed from 0 to 1, where $0\leq n\leq 7$. Let $\tilde{\boldsymbol{K}}_l$ denote the modified version of $\boldsymbol{K}_l$. The change $\boldsymbol{D}_l=\tilde{\boldsymbol{K}}_l-\boldsymbol{K}_l$ can be represented by the following two equations:

$$\boldsymbol{D}_l[:,j]\equiv\boldsymbol{0},\ \text{for}\ j\neq j_0, \tag{7}$$

$$\boldsymbol{D}_l[:,j_0]=\begin{pmatrix}\sum_{i=1}^{m}\boldsymbol{IV}[i]\boldsymbol{D}_{l-1}[i,j_0]\\ \boldsymbol{IV}[1]\boldsymbol{D}_l[1,j_0]+\sum_{i=2}^{m}\boldsymbol{IV}[i]\boldsymbol{D}_{l-1}[i,j_0]\\ \vdots\\ \sum_{i=1}^{m-1}\boldsymbol{IV}[i]\boldsymbol{D}_l[i,j_0]+\boldsymbol{IV}[m]\boldsymbol{D}_{l-1}[m,j_0]\end{pmatrix}\bmod 256, \tag{8}$$

where $\boldsymbol{D}_l[1,j_0]=2^n$, $\boldsymbol{D}_l[i,j_0]=0$, $i=2, 3, ..., m$.

Since $\boldsymbol{IV}[i]$ mod $2\neq 0$, $\boldsymbol{D}_l[i, j_0]\neq 0$ always holds. From Eq.(8), one can see that $\boldsymbol{D}_l[i,j_0]\geq 2^n$ holds, which means that only the n_0th bit of $\boldsymbol{C}_l[j_0]$ may possibly be changed, where $n\geq n_0$. Also note that there is no influence on $\boldsymbol{C}_l$ if

$$(\boldsymbol{P}_l\cdot\boldsymbol{D}_l[:,j_0])\bmod 256=0. \tag{9}$$

To verify the above analysis, an experiment has been carried out using a plain-image "Lenna" with the secret key

$$\begin{cases}m=4,\ \boldsymbol{IV}=[3\quad 9\quad 17\quad 33],\\ \boldsymbol{K}_1=\begin{pmatrix}11 & 2 & 3 & 7\\ 8 & 5 & 19 & 103\\ 201 & 203 & 119 & 150\\ 7 & 9 & 21 & 35\end{pmatrix}.\end{cases} \tag{10}$$

Only the 5th bit of $\boldsymbol{K}_1[1, 2]$ is changed, namely $\tilde{\boldsymbol{K}}_1[1,2]=\boldsymbol{K}_1[1,2]\oplus 2^5$. Let $\tilde{\boldsymbol{C}}$ denote the cipher-image corresponding to $\tilde{\boldsymbol{K}}_1$. The bit-planes of the difference $|\tilde{\boldsymbol{C}}-\boldsymbol{C}|$ are shown in Fig.1, which demonstrates the very weak sensitivity of the encryption scheme with respect to $\boldsymbol{K}_1$.

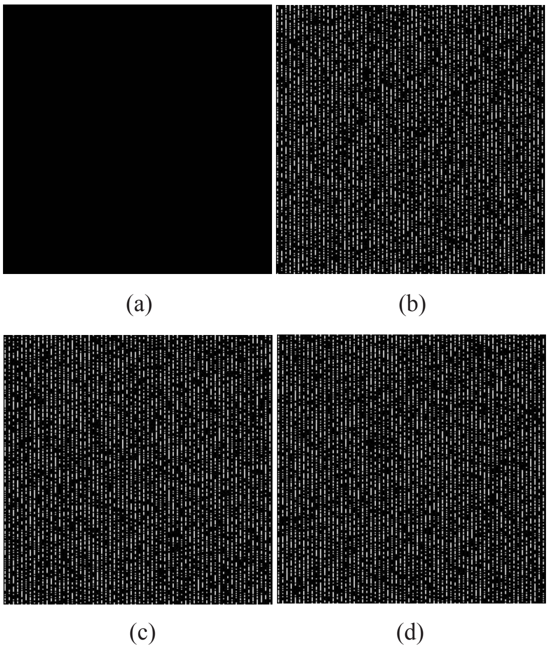

(a) (b)
(c) (d)

Fig.1 Bit-planes of $|\tilde{\boldsymbol{C}}-\boldsymbol{C}|$ when one bit of $\boldsymbol{K}_1$ is changed. (a) 0~4th; (b) 5th; (c) 6th; (d) 7th

Now consider the influence on $\boldsymbol{K}_{l\geq 2}$ if only one bit of $\boldsymbol{IV}$ is changed. Without loss of generality, assume the nth bit of $\boldsymbol{IV}[1]$ is changed from 0 to 1. Similarly, let $\boldsymbol{D}_l$ denote the change of $\boldsymbol{K}_l$. Due to the extremely complex formulation of $\boldsymbol{D}_{l\geq 3}$, only $\boldsymbol{D}_2$ is shown here:

$$\boldsymbol{D}_2[:,j]=\begin{pmatrix}\boldsymbol{K}_1[1,j]2^n\\ \boldsymbol{D}_2[1,j](\boldsymbol{IV}[1]+2^n)+\boldsymbol{K}_2[1,j]2^n\\ \boldsymbol{D}_2[2,j]+\boldsymbol{IV}[2]\boldsymbol{D}_2[2,j]\\ \vdots\\ \boldsymbol{D}_2[2,j]+\sum_{i=2}^{m-1}\boldsymbol{IV}[i]\boldsymbol{D}_2[i,j]\end{pmatrix}\bmod 256, \tag{11}$$

where j=1, 2, …, m.

To see the influence of the change of $\boldsymbol{IV}$, another experiment has been carried out using a plain-image "Lenna" with the same secret key as used above. Only the 5th bit of $\boldsymbol{IV}[1]$ is changed, namely $\boldsymbol{IV}[1]=\boldsymbol{IV}[1]\oplus 2^5$. The bit-planes of the difference between cipher-images corresponding to $\boldsymbol{IV}$ and $\widetilde{\boldsymbol{IV}}$ are shown in Fig.2.

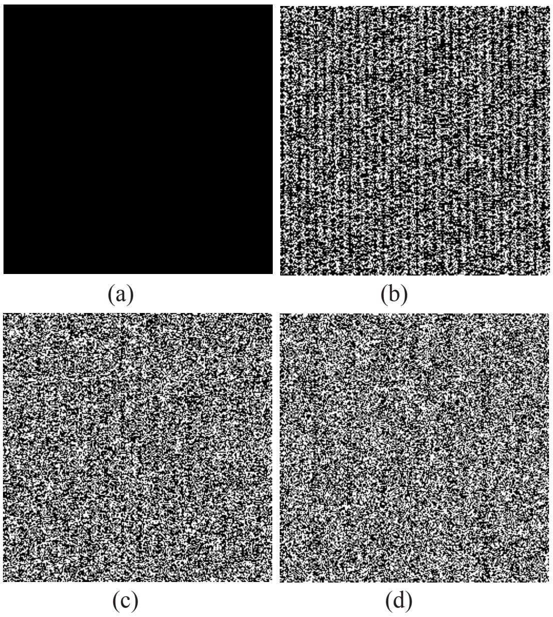

(a) (b) (c) (d)

Fig.2 Bit-planes of $|\tilde{C}-C|$ when one bit of IV is changed. (a) 0~4th; (b) 5th; (c) 6th; (d) 7th

Comparing Fig.1 and Fig.2, one can see that the sensitivity with respect to $\boldsymbol{IV}$ is much stronger than the one with respect to $\boldsymbol{K}_1$, which agrees with the above theoretical analysis. But one bit change of a sub-key of a secure cipher should cause every bit of the ciphertext to be changed with a probability of 1/2. Obviously, the sensitivity of the encryption scheme with respect to sub-keys $\boldsymbol{K}_1$ and $\boldsymbol{IV}$ is very far from this requirement.

Insensitivity to change of plain-image

The property of insensitivity to the change of the plain-image is especially important for image encryption, since an image and its watermarked version may be encrypted simultaneously.

Since the role of $\boldsymbol{P}_l$ in Eq.(1) is exactly the same as that of $\boldsymbol{IV}$ in Eq.(2), the analysis of its insensitivity to the change of the plain-image can be carried out just like the case about the sub-key $\boldsymbol{IV}$ discussed above.

Other problems

The encryption scheme has the following additional problems:

(1) It cannot encrypt the plain-image of a fixed value zero.

(2) The implementation efficiency is low. From Theorem 2.3.3 of (Overbey *et al.*, 2005), one can see that the number of invertible matrices of size m×m in $\mathbb{Z}_{256}$ is

$$|GL(m,\mathbb{Z}_{256})|=2^{7m^2}\prod_{k=0}^{m-1}(2^m-2^k). \tag{12}$$

Thus, the probability that a matrix of size m×m in $\mathbb{Z}_{256}$ is invertible is

$$p_m=\frac{2^{7m^2}\prod_{k=0}^{m-1}(2^m-2^k)}{2^{8m^2}}=\prod_{k=1}^{m}(1-2^{-k}). \tag{13}$$

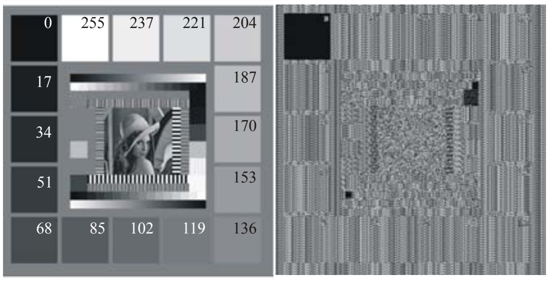
It can be easily verified that $0.288788<p_m\le 1/2$. So, it needs more than $O(2m^3)$ and $O(m^2MN)$ times of computations, respectively, for checking the reversibility of $\boldsymbol{K}_1$ and for calculating $\{\boldsymbol{K}_l^{-1}\}_{l=1}^{\lceil MN/m\rceil}$. Note that these computations only reduce the implementation efficiency of the scheme and make no direct contribution to protecting the plain-image.

(3) The scope of sub-key m is limited. As discussed above, the larger the value m, the higher the computational cost.

(4) The confusion capability is weak. The linearity of the main encryption function makes the scheme unable to assure the cipher-images statistically undistinguishable for different plain-images.

(5) The special properties of the plain-image are not considered. The encryption scheme deals with the plain-image as ordinary text data and does not consider the special properties of the plain-image,

such as the bulky size of uncompressed data and the strong redundancy of adjacent pixels. To demonstrate this defect, the encryption result of one special plain-image with the secret key in Eq.(10) is shown in Fig.3, where Fig.3b also effectively disproves the conclusion about the quality of encryption results given in Section 4 of (Ismail *et al.*, 2006).



(a) (b)

Fig.3 A special test image, "Test_pattern"
(a) Plain-image; (b) Cipher-image

KNOWN/CHOSEN-PLAINTEXT ATTACK

The known/chosen-plaintext attack works by reconstructing the secret key or its equivalent based on some known/chosen plaintexts and their corresponding ciphertexts.

Ismail *et al.*(2006) recognized that the Hill cipher is vulnerable to known/chosen-plaintext attacks and tried to thwart the attack by making the encryption matrix of every block of plain-image $\boldsymbol{K}_l$ change dynamically. However, the equivalent key $\{\boldsymbol{K}_l\}_{l=1}^{\lceil MN/m \rceil}$ can still be reconstructed from some known/chosen plain-images. Furthermore, the equivalent key can even be reconstructed from one known/chosen plain-image due to the short period of the sequence $\{\boldsymbol{K}_l\}_{l=1}^{\lceil MN/m \rceil}$, which is caused by the simple structure of Eq.(2). To study the period of this sequence, 10000 tests have been carried out for a given value of $\boldsymbol{IV}$ of size 1×3, where $\boldsymbol{K}_1$ is selected randomly. The numbers of tests, N_t, with some values of $\boldsymbol{IV}$, are shown in Table 1. Where t is the period of the corresponding sequence $\{\boldsymbol{K}_l[:,1]\}_{l=1}^{\lceil MN/m \rceil}$. Obviously, the period of $\{\boldsymbol{K}_l[:,j]\}_{l=1}^{\lceil MN/m \rceil}$ is very short.

Table 1 Numbers of tests (N_t) with some values of $\boldsymbol{IV}$. $t=2^s$, s=3, 4, ..., 9

$\boldsymbol{IV}$	N_8	N_{16}	N_{32}	N_{64}	N_{128}	N_{256}	N_{512}
(91,63,45)	0	0	0	0	0	1463	8537
(113,25,219)	14	34	127	561	3651	5703	0
(253,115,17)	6	20	72	284	1081	8537	0
(1,3,5)	0	0	98	284	1081	8537	0
(5,121,247)	7	36	132	561	3561	5703	0

Let T denote the period of the sequence $\{\boldsymbol{K}_l\}_{l=1}^{\lceil MN/m \rceil}$. This plaintext attack can be represented by the following function:

$$\boldsymbol{K}_l = \left(\boldsymbol{P}_l^{(B)} \begin{pmatrix} \boldsymbol{C}_l \\ \boldsymbol{C}_{l+T} \\ \vdots \\ \boldsymbol{C}_{l+mT} \end{pmatrix} \right) \bmod 256, \tag{14}$$

where

$$\boldsymbol{P}_l^{(B)} = \begin{pmatrix} \boldsymbol{P}_l \\ \boldsymbol{P}_{l+T} \\ \vdots \\ \boldsymbol{P}_{l+mT} \end{pmatrix}^{-1}. \tag{15}$$

The reversibility of $\boldsymbol{P}_l^{(B)}$ can be ensured by selecting some other blocks from $\{\boldsymbol{P}_{l+iT}\}_{i=m+1}^{\lceil MN/(mT) \rceil}$ or by choosing a special plain-image.

When $MN/(mt)>>m$, the above attack works well; otherwise, m plain-images $\boldsymbol{P}^{(1)}, \boldsymbol{P}^{(2)}, \ldots, \boldsymbol{P}^{(m)}$ and their corresponding cipher-images $\boldsymbol{C}^{(1)}, \boldsymbol{C}^{(2)}, \ldots, \boldsymbol{C}^{(m)}$ are needed for carrying out the attack, which can be represented by

$$\boldsymbol{K}_l = \left(\boldsymbol{P}_l^{(B)} \begin{pmatrix} \boldsymbol{C}_l^{(1)} \\ \boldsymbol{C}_l^{(2)} \\ \vdots \\ \boldsymbol{C}_l^{(m)} \end{pmatrix} \right) \bmod 256, \tag{16}$$

where

$$\boldsymbol{P}_l^{(B)} = \begin{pmatrix} \boldsymbol{P}_l^{(1)} \\ \boldsymbol{P}_l^{(2)} \\ \vdots \\ \boldsymbol{P}_l^{(m)} \end{pmatrix}^{-1}. \tag{17}$$

In this case, the reversibility of $\boldsymbol{P}_l^{(B)}$ can be ensured by utilizing more than *m* plain-images or by choosing *m* special plain-images.

CONCLUSION

In this paper, the security and performance of an image encryption scheme based on the Hill cipher (Ismail *et al*., 2006) have been analyzed in detail. It has been found that the scheme can be broken with only one known/chosen plain-image. There is a simple necessary and sufficient condition that makes a number of secret keys invalid. In addition, the scheme is insensitive to the changes of the secret key/plain-image. Some other performance defects have also been found. In conclusion, the encryption scheme under study actually has much weaker security than the original Hill cipher, which was proposed in the old days when high-speed computers were not available. Therefore, the scheme under question is not recommended for applications.

References

Alvarez, G., Li, S., 2006. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos*, **16**(8):2129-2151. [doi:10.1142/S0218127406015970]

Alvarez, G., Li, S., Hernandez, L., 2007. Analysis of security problems in a medical image encryption system. *Comput. Biol. Med.*, **37**(3):424-427. [doi:10.1016/j.compbiomed.2006.04.002]

Hill, L.S., 1929. Cryptography in an algebraic alphabet. *Am. Math. Month.*, **36**(6):306-312. [doi:10.2307/2298294]

Ismail, I.A., Amin, M., Diab, H., 2006. How to repair the Hill cipher. *J. Zhejiang Univ. Sci. A*, **7**(12):2022-2030. [doi:10.1631/jzus.2006.A2022]

Li, C., 2005. Cryptanalyses of Some Multimedia Encryption Schemes. MS Thesis, Department of Mathematics, Zhejiang University, Hangzhou, China (in Chinese).

Li, C., Li, S., Zhang, D., Chen, G., 2004. Cryptanalysis of a chaotic neural network based multimedia encryption scheme. *LNCS*, **3333**:418-425. [doi:10.1007/b104121]

Li, C., Li, S., Chen, G, Chen, G., Hu, L., 2005a. Cryptanalysis of a new signal security system for multimedia data transmission. *EURASIP J. Appl. Signal Process.*, **2005**(8): 1277-1288. [doi:10.1155/ASP.2005.1277]

Li, C., Li, S., Zhang, D., Chen, G., 2005b. Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher. *LNCS*, **3497**:630-636. [doi:10.1007/11427445_103]

Li, C., Li, S., Lou, D.C., 2006. On the security of the Yen-Guo's domino signal encryption algorithm (DSEA). *J. Syst. Soft.*, **79**(2):253-258. [doi:10.1016/j.jss.2005.04.021]

Li, C., Li, S., Alvarez, G., Chen, G., Lo, K.T., 2007a. Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. *Phys. Lett. A*, **369**(1-2):23-30. [doi:10.1016/j.physleta.2007.04.023]

Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G., 2007b. On the Security Defects of an Image Encryption Scheme. Cryptology ePrint Archive: Report 2007/397. Available at http://eprint.iacr.org/2007/397, Oct. 6, 2007.

Li, S., 2003. Analyses and New Designs of Digital Chaotic Ciphers. Ph.D Thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China (in Chinese).

Li, S., Chen, G., Zheng, X., 2004. Chaos-based Encryption for Digital Images and Videos. *In*: Furht, B., Kirovski, D. (Eds.), Multimedia Security Handbook. CRC Press, LLC, p.133-167.

Li, S., Li, C., Lo, K.T., Chen, G., 2006. Cryptanalysis of an image encryption scheme. *J. Electr. Imag.*, **15**(4). [doi:10.1117/1.2360697]

Li, S., Chen, G., Cheung, A., Bhargava, B., Lo, K.T., 2007. On the design of perceptual MPEG-video encryption algorithms. *IEEE Trans. on Circuits Syst. Video Technol.*, **17**(2):214-223. [doi:10.1109/TCSVT.2006.888840]

Li, S., Li, C., Chen, G., Mou, X., 2008a. Cryptanalysis of the RCES/RSES image encryption scheme. *J. Syst. Soft.*, **81**(7):1130-1143. [doi:10.1016/j.jss.2007.07.037]

Li, S., Li, C., Lo, K.T., Chen, G., 2008b. Cryptanalysis of an image scrambling scheme without bandwidth expansion. *IEEE Trans. on Circuits Syst. Video Technol.*, **18**(3): 338-349. [doi:10.1109/TCSVT.2008.918116]

Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. *Cryptologia*, **29**(1):59-72. [doi:10.1080/0161-110591893771]

Rangel-Romero, Y., Vega-García, R., Menchaca-Méndez, A., Acoltzi-Cervantes, D., Martínez-Ramos, L., Mecate-Zambrano, M., Montalvo-Lezama, F., Barrón-Vidales, J., Cortez-Duarte, N., Rodríguez-Henríquez, F., 2008. Comments on "How to repair the Hill cipher". *J. Zhejiang Univ. Sci. A*, **9**(2):211-214. [doi:10.1631/jzus.A072143]

Shannon, C.E., 1949. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, **28**(4):656-715.

Zhou, J., Liang, Z., Chen, Y., Au, O.C., 2007. Security analysis of multimedia encryption schemes based on multiple Huffman table. *IEEE Signal Process. Lett.*, **14**(3):201-204. [doi:10.1109/LSP.2006.884012]