Cryptanalysis of an image encryption scheme based on the Hill cipher

Chengqing Li\textsuperscript{a,*}, Dan Zhang\textsuperscript{b}, and Guanrong Chen\textsuperscript{a}

\textsuperscript{a}Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong SAR, China
\textsuperscript{b}College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, Zhejiang, China

Abstract

This paper studies the security of an image encryption scheme based on the Hill cipher 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.

Key words: cryptanalysis, encryption, Hill cipher, known-plaintext attack.

CLC: TN918, TP393.08.

1 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” \cite{1}, 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 some special properties of the multimedia data, such as strong redundancy.

* Corresponding author: Chengqing Li (swiftsheep@hotmail.com).
and bulk size of the uncompressed data. To meet this challenge, a number of special image encryption schemes based on some nonlinear theories were proposed [2–4]. Yet, many of them are found to be insecure from the viewpoint of cryptography [5–17].

In [18], Ismail et al. tried to encrypt images efficiently by modifying the classical Hill cipher [19]. This paper studies the security of the scheme proposed in [18] 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 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 detailed cryptanalysis of the scheme. The last section concludes the paper.

2 The image encryption scheme to be studied

The scheme proposed in [18] scans the gray scales of a plain-image \( P \) (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 \( m \): \( \{P_l\}_{l=1}^{\lceil MN/m \rceil} \), where \( P_l = \{P((l-1) \cdot m + 1), \ldots, P((l-1) \cdot m + m)\} \) (the last vector is padded with some zero bytes if \( MN \) can not be divided by \( m \)). Then, the vectors \( \{P_l\}_{l=1}^{\lceil MN/m \rceil} \) are encrypted in increasing order with the following function:

\[
C_l = (P_l \cdot K_l) \mod 256, \quad (1)
\]

where \( K_1 = (K_1[i,j])_{m \times m} \), \( K_1[i,j] \in \mathbb{Z}_{256} \), the initial state of \( K_{l \geq 2} \) is set to be \( K_{l-1} \), and then every row of \( K_l \) is generated iteratively with the following function, for \( i = 1 \sim m \):

\[
K_l[i,:]= (IV \cdot K_i) \mod 256, \quad (2)
\]

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

The secret key of the encryption scheme includes three parts: \( m \), \( K_0 \), and \( IV \).

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

\[
P_l = (C_l \cdot K_l^{-1}) \mod 256, \quad (3)
\]
where \((K_l \cdot K_l^{-1}) \mod 256 = I\), the identity matrix.

3 Cryptanalysis

3.1 Some Defects of the Scheme

3.1.1 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 \(\gcd(K_1, 256) \neq 1\) or \(IV[i] \mod 2 = 0\).

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

Proposition 1 \(\det(K_l) = \left(\prod_{i=1}^{m} IV[i]\right) \det(K_{l-1})\).

Proof: According to Eq. (2), there is a relation between \(K_l\) and \(K_{l-1}\), as follows:

\[
K_l = \begin{pmatrix}
\sum_{i=1}^{m} IV[i]K_{l-1}[i,:] \\
IV[1]K_l[1,:] + \sum_{i=2}^{m} IV[i]K_{l-1}[i,:] \\
\vdots \\
\sum_{i=1}^{m-1} IV[i]K_l[i,:] + IV[m]K_{l-1}[m,:]
\end{pmatrix} \mod 256. \tag{4}
\]

Subtracting \(\sum_{i=1}^{i_0-1} IV[i]K_l[i,:]\) from \(K_l[i_0,:]\) for \(i_0 = m \sim 2\), one gets

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

Subtracting \(K'_l[i_0,:]\) from \(K'_l[i_0 - 1,:]\) for \(i_0 = 2 \sim m\), one has
Obviously, \( \det(K_l) = \det(K'_l) = \det(K''_l) = \left( \prod_{i=1}^{m} IV[i] \right) \det(K_{l-1}) \), which completes the proof of the proposition. \( \blacksquare \)

**Corollary 1** \( \det(K_l) = \left( \prod_{i=1}^{m} IV[i] \right) l^{-1} \det(K_1). \)

**Proof:** The result directly follows from Proposition 1. \( \blacksquare \)

### 3.1.2 Insensitivity to the change of the secret key

Although it is claimed in [18, Sec. 5] that the encryption scheme is very sensitive to the change of the sub-keys \( K_1, IV \), this is not true.

Let’s first study the influence on \( K_{l \geq 2} \) if only one bit of \( K_1 \) is changed. Without loss of generality, assume that the \( n \)-th significant bit of \( K_1(1, j_0) \) is changed from zero to one, where \( 0 \leq n \leq 7 \). Let \( \widetilde{K}_l \) denote the modified version of \( K_l \).

The change \( D_l = \widetilde{K}_l - K_l \) can be presented by the following two equations:

\[
D_l[;, j] \equiv 0, \text{ for } j \neq j_0, \quad (7)
\]

\[
D_l[; j_0] = \begin{pmatrix}
IV[1]D_{l-1}[1, j_0] + \sum_{i=2}^{m} IV[i]D_{l-1}[i, j_0] \\
\vdots \\
\sum_{i=1}^{m} IV[i]D_{l-1}[i, j_0] + IV[m]D_{l-1}[m, j_0]
\end{pmatrix} \mod 256, \quad (8)
\]

where \( D_1[1, j_0] = 2^n, D_1[i, j_0] = 0, i = 2 \sim m. \)

Since \( IV[i] \mod 2 \neq 0, D_l[i, j_0] \neq 0 \) always exist. From Eq. (8), one can see that \( D_l[i, j_0] \geq 2^n \) exists, which means that only the \( n_0 \)-th bit of \( C_l[j_0] \) may possibly be changed, where \( n_0 \geq n \). Note also that there is no influence on \( C_l \) if

\[
(P_lD_l[; j_0]) \mod 256 = 0.
\]
To verify the above analysis, an experiment has been carried out using a plain-image “Lenna” with the secret key

\[
m = 4, \ IV = (3 \ 9 \ 17 \ 33), \ K_1 = \begin{pmatrix}
11 & 2 & 3 & 7 \\
8 & 5 & 19 & 103 \\
201 & 203 & 119 & 150 \\
7 & 9 & 21 & 35 \\
\end{pmatrix}.
\]

Only the 5-th significant bit of \(K_1[1, 2]\) is changed, namely \(\hat{K}_1[1, 2] = (K_1[1, 2] + 5525) \mod 256\). Let \(\hat{C}\) denote the cipher-image corresponding to \(\hat{K}_1\). The bit-planes of difference \(|\hat{C} - C|\) are shown in Fig. 1, which demonstrates the very weak sensitivity of the encryption scheme with respect to \(K_1\).

![Fig. 1. The bit-planes of \(|\hat{C} - C|\) when one bit of \(K_1\) is changed.](image)

Now, consider the influence on \(K_{l \geq 2}\) if only one bit of \(IV\) is changed. Without loss of generality, assume the \(n\)-th significant bit of \(IV[1]\) is changed from zero to one. Similarly, let \(D_l\) denote the change of \(K_l\). Due to the extremely complex formulation of \(D_{l \geq 3}\), only \(D_2\) is shown here.

\[
D_2[,] = \begin{pmatrix}
K_1[1, j]2^n \\
D_2[1, j](IV[1] + 2^n) + K_2[1, j]2^n \\
D_2[2, j] + IV[2]D_2[2, j] \\
\vdots \\
D_2[2, j] + \sum_{i=2}^{m-1} IV[i]D_2[i, j]
\end{pmatrix} \mod 256,
\]

where \(j = 1 \sim m\).

To see the influence of the change of \(IV\), an experiment has been carried out using plain-image “Lenna”, with the same secret key shown in Eq. (9) above. Only the 5-th significant bit of \(IV[1]\) is changed, namely \(\hat{IV}[1] = (IV[1] + 2^5) \mod 256\). The bit-planes of difference between cipher-images corresponding to \(IV\) and \(\hat{IV}\), respectively, are shown in Fig. 2.
Comparing Fig. 1 and Fig. 2, one can see that the sensitivity with respect to $IV$ is much stronger than the one with respect to $K_1$, 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 changed with a probability of $\frac{1}{2}$. Obviously, the sensitivity of the encryption scheme with respect to sub-keys $K_1, IV$ is very far from this requirement.

Fig. 2. The bit-planes of $|\tilde{C} - C|$ when one bit of $IV$ is changed.

### 3.1.3 Insensitivity to the change of the plain-image

This property is especially important for image encryption since an image and its watermarked version may be encrypted simultaneously.

Since the role of $P_1$ in Eq. (1) is exactly the same as that of $IV$ in Eq. (2), the analysis about its insensitivity to the change of the plain-image can be carried out just like the case about the sub-key $IV$ discussed above.

### 3.1.4 Some other problems

The encryption scheme has the following additional problems:

(1) cannot encrypt plain-image of a fixed value zero;
(2) efficiency of implementation is low: From [20, Thorem 2.3.3], one can see that the number of invertible matrices of size $m \times m$ in $\mathbb{Z}_{256}$ is

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

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

$$p_m = \frac{2^{7m^2} \prod_{k=0}^{m-1} (2^m - 2^k)}{2^{8m^2}} = \prod_{k=1}^{m} (1 - 2^{-k}) \approx \frac{1}{3}. $$

So, it needs $O(3m^2)$ and $O(m^2 \cdot MN)$ times of computations, respectively, for checking the reversibility of $K_1$ and for calculating $\{K_1^{-1}\}_{i=1}^{[MN/m]}$. 
Note that these computations have no direct contributions 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: This problem is caused by the linearity of the main encryption function. To demonstrate this defect, the encryption result of one special plain-image is shown in Fig. 3, where Figure 3b) also effectively disproves the conclusion about the quality of encryption results given in [18, Sec. 4].

![Fig. 3. A special test image, “Test_pattern”.](image)

3.2 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.

For this encryption scheme, the equivalent key $\{K_l\}_{l=1}^{[MN/m]}$ can be reconstructed from $m$ plain-images $P^{(1)} \sim P^{(m)}$ and their corresponding cipher-images $C^{(1)} \sim C^{(m)}$ by using

$$K_l = \left(P_l^{(B)} \cdot \begin{pmatrix} C_l^{(1)} \\ C_l^{(2)} \\ \vdots \\ C_l^{(m)} \end{pmatrix} \right) \mod 256,$$

(13)
where

$$P_l^{(B)} = \left( \begin{array}{c}
P_l^{(1)} \\
P_l^{(2)} \\
\vdots \\
P_l^{(m)}
\end{array} \right)^{-1}. \quad (14)$$

The reversibility of $P_l^{(B)}$ can be ensured by utilizing more than $m$ plain-images or by choosing $m$ special plain-images. Note that the above known/chosen-plaintext attack can be carried out with only one known/chosen plain-image due to the very short period of sequence $\{K_l[:, j]\}^{[MN/m]}$ for $j = 1 \sim m$. To study the period of this sequence, 10,000 tests have been done for a given value of $IV$ of size $1 \times 3$, where $K_1$ is selected randomly. The numbers of tests where the corresponding sequence $\{K_l(:, 1)\}^{[MN/m]}$ has period $p$, $N_p$, with some values of $IV$, is shown in Table 1, which shows that the period of $\{K_l[:, j]\}^{[MN/m]}$ is indeed very short.

### Table 1

Values of $N_p$ with some values of $IV$, $p = 2^s$, $s = 3 \sim 9$.

| IV          | $N_8$ | $N_{16}$ | $N_{32}$ | $N_{64}$ | $N_{128}$ | $N_{256}$ | $N_{512}$ |
|-------------|-------|----------|----------|----------|-----------|-----------|-----------|
| (91, 63, 45)| 0     | 0        | 0        | 0        | 1463      | 8537      |
| (113, 25, 219)| 14   | 34       | 127      | 561      | 3561      | 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         |

### 4 Conclusion

In this paper, the security and performance of an image encryption scheme based on the Hill cipher 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 change 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, therefore is not recommended for applications.
5 Acknowledgement

This research was supported by the City University of Hong Kong under the SRG project 7002134.

References

[1] C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28 (4) (1949) 656–715.

[2] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), Multimedia Security Handbook, CRC Press, LLC, 2004, Ch. 4, pp. 133–167, preprint available online at http://www.hooklee.com/pub.html.

[3] S. Li, Analyses and new designs of digital chaotic ciphers, Ph.D. thesis, School of Electronic and Information Engineering, Xi’an Jiaotong University, Xi’an, China, available online at http://www.hooklee.com/pub.html (2003).

[4] C. Li, Cryptanalyses of some multimedia encryption schemes, Master’s thesis, Department of Mathematics, Zhejiang University, Hangzhou, China, available online at http://eprint.iacr.org/2006/340 (May 2005).

[5] C. Li, S. Li, D. Zhang, G. Chen, Cryptanalysis of a chaotic neural network based multimedia encryption scheme, Lecture Notes in Computer Science 3333 (2004) 418–425.

[6] C. Li, S. Li, G. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission, EURASIP Journal on Applied Signal Processing 2005 (8) (2005) 1277–1288.

[7] C. Li, S. Li, D. Zhang, G. Chen, Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher, Lecture Notes in Computer Science 3497 (2005) 630–636.

[8] C. Li, S. Li, D.-C. Lou, On the security of the Yen-Guo’s domino signal encryption algorithm (DSEA), Elsevier Journal of Systems and Software 79 (2) (2006) 253–258.

[9] S. Li, C. Li, K.-T. Lo, G. Chen, Cryptanalysis of an image encryption scheme, Journal of Electronic Imaging 15 (4) (2006) article number 043012.

[10] C. Li, S. Li, G. Álvarez, G. Chen, K.-T. Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and xor operations, Physics Letters A 369 (1-2) (2007) 23–30.

[11] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.
[12] D. Arroyo, C. Li, S. Li, G. Alvarez, Cryptanalysis of a computer cryptography scheme based on a filter bank, available online at http://arxiv.org/abs/0710.5471 (2007).

[13] C. Li, S. Li, M. Asim, J. Nunez, G. Álvarez, G. Chen, On the security defects of an image encryption scheme, Cryptology ePrint Archive: Report 2007/397, available online at http://eprint.iacr.org/2007/397 (2007).

[14] S. Li, C. Li, K.-T. Lo, G. Chen, Cryptanalysis of an image scrambling scheme without bandwidth expansion, accepted by IEEE Transactions on Circuits and Systems for Video Technology, available online at http://eprint.iacr.org/2006/215 (2007).

[15] J. Zhou, Z. Liang, Y. Chen, A. O. C., Security analysis of multimedia encryption schemes based on multiple huffman table, IEEE Signal Processing Letters 14 (3) (2007) 201–204.

[16] S. Li, G. Chen, A. Cheung, B. Bhargava, K.-T. Lo, On the design of perceptual MPEG-video encryption algorithms, IEEE Transactions on Circuits and Systems for Video Technology 17 (2) (2007) 214–223.

[17] G. Alvarez, S. Li, L. Hernandez, Analysis of security problems in a medical image encryption system, Computers in Biology and Medicine 37 (3) (2007) 424–427.

[18] I. A. Ismail, M. Amin, H. Diab, How to repair the hill cipher, Journal of Zhejiang University SCIENCE A 7 (12) (2006) 2022–2030.

[19] L. S. Hill, Cryptography in an algebraic alphabet, The American Mathematical Monthly 36 (1929) 306–312.

[20] J. Overbey, W. Traves, J. Wojdylo, On the keyspace of the hill cipher, Cryptologia 29 (1) (2005) 59–72.