Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

How to repair the Hill cipher

ISMAIL I.A.[1], AMIN Mohammed[2], DIAB Hossam[2]

([1]*Faculty of Computers and Information, Zagazig University, Zagazig, 44511, Egypt*)

([2]*Computer Science Department, Faculty of Science, Menoufiya University, Shebeen El-kom, 32511, Egypt*)

E-mail: amr4442@hotmail.com; mamin04@yahoo.com; hossamdiab_86@yahoo.com

Received Mar. 20, 2006; revision accepted Aug. 25, 2006

Abstract: The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. However, a main drawback of this algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. This paper presents a variant of the Hill cipher that overcomes these disadvantages. The proposed technique adjusts the encryption key to form a different key for each block encryption. Visually and computationally, experimental results demonstrate that the proposed variant yields higher security and significantly superior encryption quality compared to the original one.

Key words: Hill cipher, Image encryption, Modified Hill cipher, Quality of encryption
doi:10.1631/jzus.2006.A2022 **Document code:** A **CLC number:** TP393

INTRODUCTION

Owing to the advance in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information directly and clearly through images. Hence, data security has become a critical and imperative issue.

Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput (Overbey *et al*., 2005; Saeednia, 2000). However, Hill cipher succumbs to a known plaintext attack and can be easily broken with such attacks. To overcome the weak security of the Hill algorithm, we present a method for adjusting the key matrix for achieving higher security and better image encryption.

The paper is organized as follows. Section 2 gives a brief introduction of the Hill cipher. Section 3 is devoted to the proposed algorithm. Encryption quality factors are presented in Section 4. Experimental results are presented in Section 5. Experimental analysis is discussed in Section 6. Section 7 gives the conclusion.

THE HILL CIPHER

The Hill cipher algorithm takes m successive plaintext letters and substitutes m ciphertext letters for them. The substitution is determined by m linear equations in which each character is assigned a numerical value (a=0, b=1, …, z=25). Let m be a positive integer, the idea is to take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one ciphertext element. Then, an $m\times m$ matrix $\boldsymbol{A}$ is used as a key of the system such that $\boldsymbol{A}$ is invertible modulo 26 (Peterson, 2000; Lerma, 2005). Let a_{ij} be the entry of $\boldsymbol{A}$. For the plaintext block $x=(x_1, x_2, \ldots, x_m)$ (the numerical equivalents of m letters) and a key matrix $\boldsymbol{A}$, the corresponding ciphertext block $y=(y_1, y_2, \ldots, y_m)$ can be computed as

Encryption:

$$(y_1, y_2, \cdots, y_m) = (x_1, x_2, \cdots, x_m)\boldsymbol{A} \pmod{26}, \quad (1)$$

where

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & & a_{mm} \end{bmatrix}.$$

The ciphertext is obtained from the plaintext by means of a linear transformation.

Decryption:

The reverse process, deciphering, is computed by

$$(x_1, x_2, \cdots, x_m) = (y_1, y_2, \cdots, y_m)\boldsymbol{A}^{-1} \pmod{26}, \quad (2)$$

where

$$\boldsymbol{A}^{-1} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & & a_{mm} \end{bmatrix}^{-1} \pmod{26}. \quad (3)$$

Since the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m-letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet (Barr, 2002).

We note that Hill cipher can be adopted to encrypt grayscale and color images. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image (Li and Zheng, 2002).

METHODOLOGY OF KEY ADJUSTMENT

Despite Hill cipher being difficult to break with a ciphertext-only attack, it succumbs to a known plaintext attack assuming that the opponent has determined the value of the m being used. Let m be distinct plaintext-ciphertext pairs, say, $\boldsymbol{x}_j=(x_{1j}, x_{2j}, \ldots, x_{mj})$ and $\boldsymbol{y}_j=(y_{1j}, y_{2j}, \ldots, y_{mj})$, $1\leq j\leq m$, such that $\boldsymbol{y}_j=e_k(\boldsymbol{x}_j)$, $1\leq j\leq m$ (e_k is the encryption process by the key k). Define two $m\times m$ matrices $\boldsymbol{X}=(x_{ij})$ and $\boldsymbol{Y}=(y_{ij})$. Whenever $\boldsymbol{X}$ is invertible in the encryption equation $\boldsymbol{Y}=\boldsymbol{XK}$, the opponent can compute the unknown key of ciphering as $\boldsymbol{K}=\boldsymbol{X}^{-1}\boldsymbol{Y}$ and thereby break the cipher (Barr, 2002). If $\boldsymbol{X}$ is not invertible, then it will be necessary to try other sets of m plaintext-ciphertext pairs. When m is unknown, assuming that m is not too large, the opponent could simply try m=2, 3, …, until the key is found. If the guessed value of m was incorrect, the obtained key matrix would be not agree with further plaintext-ciphertext pairs (Stinson, 2002).

Using a linear transformation by one key matrix for all blocks ciphering leads to blocks linear dependency which obviously results in weak security. To overcome this weakness, we use one-time-one-key matrix for each block ciphering, with each key matrix being derived from the key matrix preceding it. That is, each block is encrypted by its own key.

The proposed methodology is based on adjusting the encryption key from one block to another. The scheme is to modify each row of the matrix key by multiplying the current key by an initial vector $\boldsymbol{IV}$. This procedure can be thought of as a process of encrypting each row of the key depending on a secret initial vector $\boldsymbol{IV}$.

More specifically, let the encryption key be an $m\times m$ matrix $\boldsymbol{k}$,

$$\boldsymbol{k} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix},$$

and let the $(i-1)$th block be encrypted by the key $\boldsymbol{k}_{i-1}$. To get the new key, we first randomly select an initial vector $\boldsymbol{IV}$ of length m, say $\boldsymbol{IV}=[v_1, v_2, \ldots, v_m]$. Second, we adjust the rows of $\boldsymbol{k}_{i-1}$ one at a time as:

For the first row of $\boldsymbol{k}_{i-1}$, $\boldsymbol{k}_{i-1}(1,:)$

$$\boldsymbol{k}_{i-1}(1,:) = \boldsymbol{k}\cdot\boldsymbol{IV} \bmod n, \quad (4)$$

where n is the number of the alphabet (26 for text and 256 for images).

Now, the first row is changed (encrypted) and the key becomes,

$$\boldsymbol{k}'=\begin{bmatrix} k'_{11} & k'_{12} & \cdots & k'_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}, \tag{5}$$

where $\boldsymbol{k}'_{1j}$ $(j=1, \ ..., \ m)$ is computed from Eq.(4).

Similarly, the ith row of $\boldsymbol{k}_{i-1}$ can be encrypted by

$$\boldsymbol{k}_{i-1}(i,:)=\boldsymbol{k}'\cdot\boldsymbol{IV} \bmod n, \tag{6}$$

where all rows of the matrix key preceding i have been adjusted with the key at this point being

$$\boldsymbol{k}'=\begin{bmatrix} k'_{11} & k'_{12} & \cdots & k'_{1m} \\ k'_{21} & k'_{22} & \cdots & k'_{2m} \\ \vdots & & \cdots & \vdots \\ k'_{i1} & k'_{i2} & \cdots & k'_{im} \\ \vdots & & \cdots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}. \tag{7}$$

After modifying all rows of $\boldsymbol{k}_{i-1}$, the matrix $\boldsymbol{k}'$ gives the new encryption key $\boldsymbol{k}_i$ for the ith block. That is, for each block, we compute its own encryption key which is obtained by adjusting all rows of the prior block key according to Eq.(6).

Now, the obtained modified key is used to encrypt the ith block of the message as,

$$(y_{i1}, y_{i2}, \cdots, y_{im})=(x_{i1}, x_{i2}, \cdots, x_{im})\boldsymbol{k}_i \bmod n,$$

where $\boldsymbol{k}_i$ is adjusted

$$\boldsymbol{k}_i=\begin{cases} k \text{ of original Hill}, & i=1; \\ \text{Adjustment of } \boldsymbol{k}_{i-1}, & i\geq 2. \end{cases} \tag{8}$$

When Eq.(8) is used in adjusting the encryption key, we refer to the algorithm HillMRIV (Abbreviation for Hill multiplying rows by initial vector).

QUALITY OF ENCRYPTION MEASURING FACTORS

One of the most important factors in examining the encrypted image is the visual inspection where the higher the disappearance of the main features is, the better the encryption algorithm will be. But, depending on the visual inspection only is not enough in judging the complete hiding of the data image content. So, other measuring techniques are considered to evaluate the degree of encryption quantitatively.

With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently, this means that the higher the change in pixel values, the more effective the image encryption will be and hence the quality of encryption. So, the quality of encryption may be expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one (Ziedan *et al*., 2003).

In addition to the visual inspection, three measuring quality factors will be considered to evaluate and compare between encryption algorithms. These factors are, the maximum deviation, the correlation coefficient and irregular deviation (Elkamchouchi and Makar, 2005).

The maximum deviation factor

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images (Ziedan *et al*., 2003). The steps of this measure are as follows:

(1) Count the number of pixels of each grayscale value in the range from 0 to 255 and present the results graphically (in the form of curves) for both original and encrypted images (i.e. get their histogram distributions).

(2) Compute the absolute difference or deviation between the two curves and present it graphically.

(3) Count the area under the absolute difference curve, which is the sum of deviations (D) with this representing the encryption quality. D is given by the trapezoidal rule:

$$D=\frac{h_0+h_{255}}{2}+\sum_{i=1}^{254}h_i, \tag{9}$$

where h_i is the amplitude of the absolute difference curve at value i. Of course, the higher the value of D, the more is the encrypted image deviated from the original image.

The correlation coefficient factor

Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, then they are in perfect correlation (i.e. the correlation coefficient equals one) if they are highly dependent (identical). In that case the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different, i.e., the encrypted image has no distinct features and is highly independent of the original image. So, success of the encryption process means smaller values of the correlation coefficient (*C.C*), which is measured by the following equation

$$C.C=\frac{cov(x,y)}{\sigma_x\sigma_y}=\frac{\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{\sum_{i=1}^{N}(x_i-E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i-E(y))^2}}, \tag{10}$$

where $E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$, x and y are greyscale pixel values of the original and encrypted images.

The irregular deviation factor

This quality measuring factor is based on how much the deviation caused by encryption (on the encrypted image) is irregular (Elkamchouchi and Makar, 2005). It gives attention to each individual pixel value and the deviation caused at every location of the input image before getting the histogram as described in (Ziedan *et al*., 2003) which does not bear any information about the location of the pixels. This method can be summarized in the following steps:

(1) Calculate the ***D*** matrix which represents the absolute values of the difference between each pixel values before and after encryption. So, ***D*** can be represented as:

$$\boldsymbol{D}=|\boldsymbol{I}-\boldsymbol{J}|, \tag{11}$$

where ***I*** is the input image, and ***J*** is the encrypted image.

(2) Construct the histogram distribution *H* of the absolute deviation between the input image and the encrypted image. So, *H*=*histogram*(***D***).

(3) Get the average value of how many pixels are deviated at every deviation value (i.e., the number of pixels at the histogram if the statistical distribution of the deviation matrix is a uniform distribution). This average value (*DC*) can be calculated as:

$$DC=\frac{1}{256}\sum_{i=0}^{255}h_i, \tag{12}$$

where h_i is the amplitude of the absolute difference histogram at the value i.

(4) Subtract this average from the deviation histogram, and then take the absolute value of the result:

$$AC(i)=|H(i)-DC|. \tag{13}$$

(5) Count the area under the absolute *AC* value curve, which is the sum of variations of the deviation histogram from the uniformly distributed histogram:

$$ID=\sum_{i=0}^{255}AC(i). \tag{14}$$

The lower the *ID* value, the better the encryption algorithm is.

RESULTS

In our experimental results, several images are evaluated. These images are Lena as it is the reference image used in image processing research (it does not contain many high frequency components), Nike and Micky as examples of an image containing very large areas of a single color, and, Girls as example of an image containing many high frequency components. We illustrate the numerical evaluations for encryption quality of the original Hill cipher and HillMRIV, respectively (Table 1).

The results of the three measuring factors are given in Table 1 where *M*1 indicates the maximum deviation measure, *M*2 indicates the correlation coefficient measure, and *M*3 indicates the irregular deviation measure. The greater *M*1 is, the better; while for *M*2 the closer to zero the better, while for *M*3 the smaller the better. Based on the discussion presented in (Elkamchouchi and Makar, 2005), *M*3 does not

Table 1 The numerical evaluations for encryption quality of the original Hill cipher and HillMRIV, respectively

Cipher	*M*1		*M*2		*M*3	
	Original Hill	HillMRIV	Original Hill	HillMRIV	Original Hill	HillMRIV
Girls	8585	9001	0.0217	0.0062	9693.2	9261.2
Lena	6505.5	6888	0.0072	0.0051	8851.1	8486.9
Nike	23217	22209	0.7240	0.0061	28096	4423
Micky	18568	16998	0.4651	0.0027	15122	3939.5

give any misleading results and can be used alone to test the quality of encryption in the field of image encryption. So, if *M*3 agrees with other measuring factors, it will be good judging, otherwise the final decision on measuring the quality of the encryption algorithms will be based on *M*3 which is based on the irregular deviation on each pixel value. For Girls image as an example, with the smallest *M*3, the proposed algorithm yields the better encryption.

A striking example of the degree to which original Hill cipher can reveal patterns in the plaintext is shown in Fig.1. Obviously, as shown in Fig.1, the proposed method, HillMRIV, can encrypt identical plaintext blocks to totally different ciphertext blocks, whereas the original Hill cipher cannot. That is, the proposed method has advantage in hiding data patterns over the original Hill. Another example is shown in Fig.2.

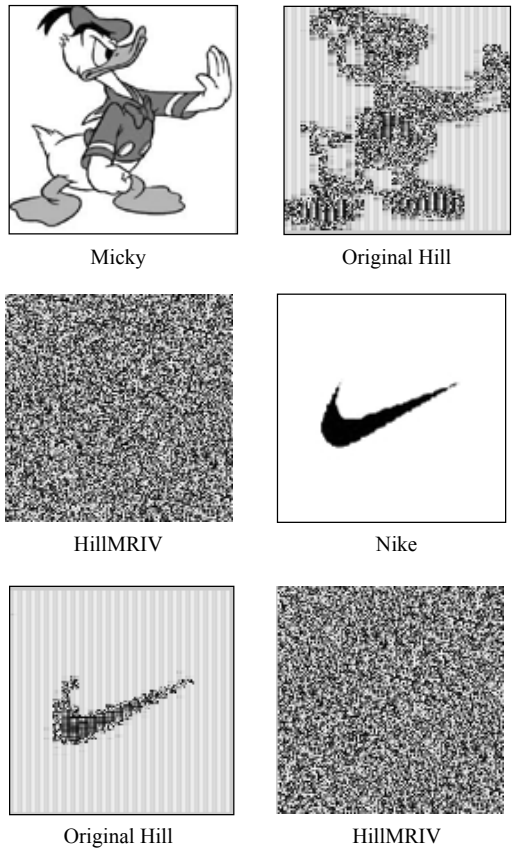


Fig.1 A striking example of the degree to which original Hill cipher can reveal patterns in the plaintext

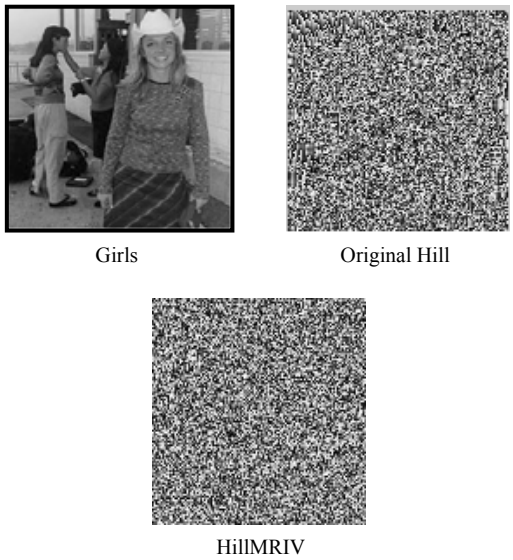


Fig.2 Encryption of Girls image by original Hill and HillMRIV

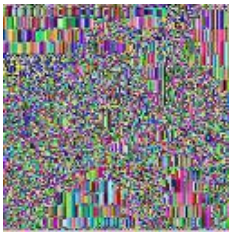
Visually, HillMRIV is better than the original Hill cipher in hiding all features of the image, specially the image that contains large areas of a single color.

An example of color image encryption by the original Hill cipher and HillMRIV is given in Fig3.

EXPERIMENTAL ANALYSIS

A good encryption scheme should resist all kinds


Man


Original Hill


HillMRIV

Fig.3 An example of color image encryption by the original Hill cipher and HillMRIV

of known attacks, such as known-plain-text attack, ciphertext only attack, statistical attack, and various-brute force attacks (Chen *et al*., 2004). Some security analysis on the proposed image encryption scheme, including the most important ones like key space analysis and statistical analysis, which demonstrated the satisfactory security of the proposed scheme, are described as follows.

Key space analysis

A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute force attacks infeasible. Key space analysis and testing of the proposed image encryption were completely carried out, with results summarized as follows:

Key space: In general, the Hill cipher key space consists of all matrices of a given dimension that are invertible modulo n. Based on (Overbey *et al*., 2005; Saeednia, 2000), the Hill cipher key space is very large. The 3×3 matrices over a 26-letter alphabet, 1634038189056 can serve as key matrices. So, the proposed algorithm will also have a large key space, and so, it resists all kinds of brute force attacks.

Key sensitivity test: Assume that two ciphering keys $\boldsymbol{k}$ and $\boldsymbol{k}'$, which have only one bit difference in between, are used for encryption. A typical key sensitivity test was conducted, according to the following steps:

(1) First, an image $\boldsymbol{F}$ is encrypted by using the test key $\boldsymbol{k}$.

(2) Then, change only one bit of $\boldsymbol{k}$, to get $\boldsymbol{k}'$, which is used to encrypt the same image.

(3) Finally, the above two ciphered images, encrypted by the two slightly different keys, are compared.

Table 2 shows the numerical evaluation between the two ciphered images for original Hill cipher and HillMRIV cipher.

Fig.4 and Fig.5 show the original image $\boldsymbol{F}$, the ciphered image by $\boldsymbol{k}$, $c1$, the ciphered image by $\boldsymbol{k}'$, $c2$, and the difference image $\boldsymbol{D}$ for original Hill, and HillMRIV ciphers respectively. For HillMRIV, the image encrypted by the key $\boldsymbol{k}$ has a higher difference from the image encrypted by the key $\boldsymbol{k}'$.

Moreover, when an initial vector $\boldsymbol{IV}$ is used to encrypt an image while another trivially modified vector $\boldsymbol{IV}'$ is used to decrypt the ciphered image, the decryption also completely fails. Fig.6 clearly shows that the image encrypted by the vector $\boldsymbol{IV}$ is not correctly decrypted by using the vector $\boldsymbol{IV}'$ which has only one bit difference from the vector $\boldsymbol{IV}$.

Statistical analysis

Statistical analysis on the proposed image encryption algorithm showed its superior confusion and diffusion properties which strongly resist statistical attacks. This is shown by a test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

1. Histograms of encrypted images

Select several 256 grey-scale images of size $m\times n$ that have different contents, and calculate their histograms. Statistical analysis of Girls image and its encrypted image yielded their grey-scale histograms given in Fig.7. This figure shows that the histogram of the ciphered image is fairly uniform and is signifi-

Table 2 The numerical evaluation between the two ciphered images for original Hill cipher and HillMRIV cipher

Cipher	$M1$		$M2$		$M3$	
	Original Hill	HillMRIV	Original Hill	HillMRIV	Original Hill	HillMRIV
Girls	1025	2095	0.8164	0.0051	24926	19982

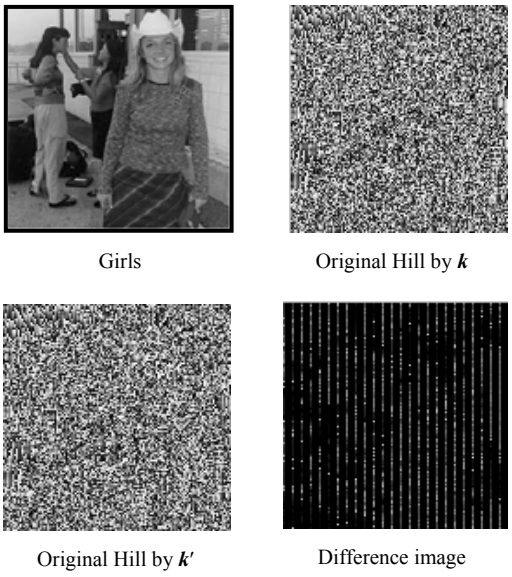


Fig.4 Key sensitive test of original Hill

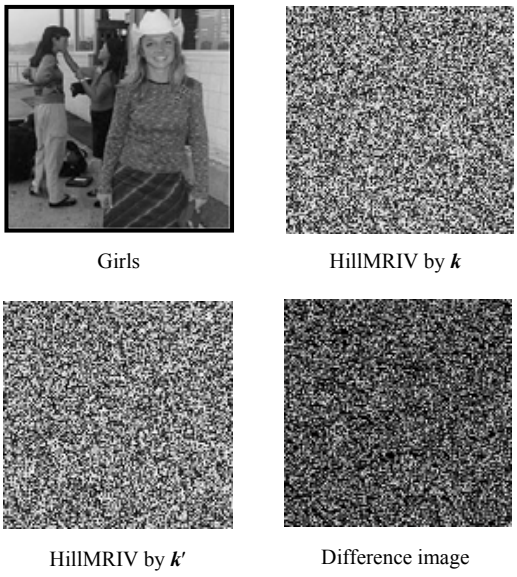


Fig.5 Key sensitive test of HillMRIV

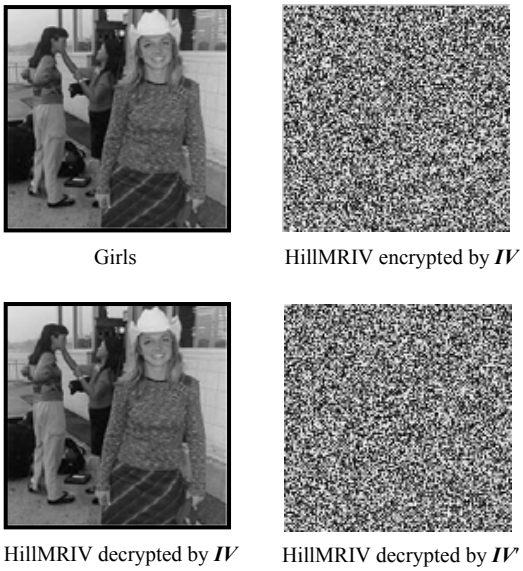


Fig.6 Key sensitive test of HillMRIV with respect to initial vector *IV*

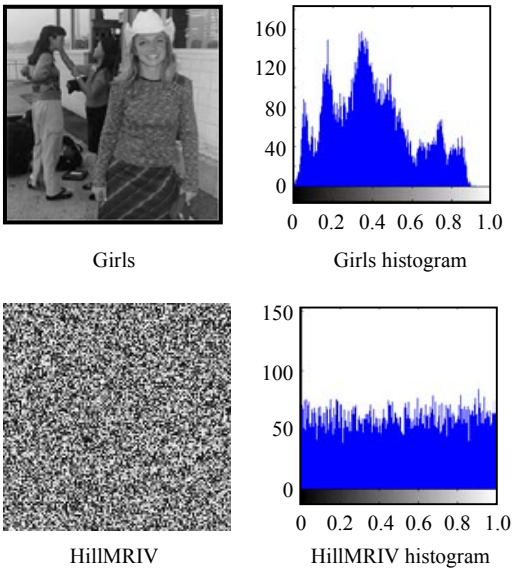


Fig.7 Histogram of the plain image and cipher image

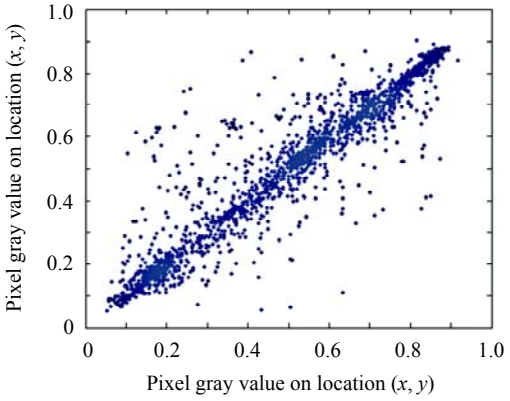
cantly different from that of the original image. Also, it demonstrates that the encryption algorithm has covered up all the characters of the plain image and shows good performance, almost zero correlation and high-level security.

2. Correlation of two adjacent pixels

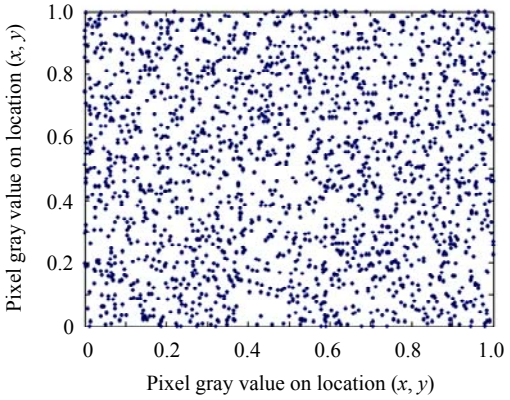
To test the correlation between two adjacent pixels in plain-image and ciphered image, the following procedure was carried out. First, randomly select 1000 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels from an image. Then, referring to (Chen *et al*., 2004), calculate the correlation coefficient of each pair by Eq.(10).

Fig.8 shows the correlation distribution of two horizontally adjacent pixels in the plain image and that in the ciphered image. Similar results for diagonal and vertical directions were obtained, which are shown in Table 3. These correlation analyses prove

that the proposed encryption technique satisfies zero co-correlation.



(a)



(b)

Fig.8 Correlation of two horizontally adjacent pixels in original and encrypted images. (a) Correlation in Girls (Correlation coefficient is 0.9445); (b) Correlation in HillMRIV (Correlation coefficient is 0.000221)

Table 3 Correlation coefficients of two adjacent pixels in original and encrypted images

Direction	Plain image	Cipher image
Horizontal	0.9445	0.000221
Vertical	0.9520	0.009900
Diagonal	0.9028	0.017100

Encryption speed analysis

Apart from security considerations, some other issues for image encryption scheme are also important. This includes the running speed, particularly for real time Internet applications.

Some experimental tests indicated that the running speed of the proposed algorithm is acceptable. The personal computer used in all programs and tests was 1.2 GHz Pentium III with 256 M memory and 40 G hard-disk capacity.

We examined the encryption time for the Girls image (128×128 pixels) as an example, the encryption time of this image when applying the original Hill and the proposed variant HillMRIV, is shown in Table 4 and Fig.9. Although HillMRIV cipher consumes more time (because of its computations for adjusting the key $\boldsymbol{k}$ to produce the modified key $\boldsymbol{k}'$), it achieves better image encryption.

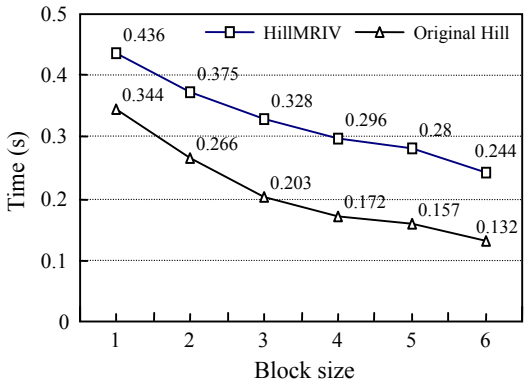


Fig.9 Encryption time test of Girls

Table 4 The time of encryption of Girls (unit: s)

Block size	Original Hill	HillMRIV
2	0.3440	0.4360
3	0.2660	0.3750
4	0.2030	0.3280
5	0.1720	0.2960
6	0.1570	0.2800
7	0.1320	0.2440

From our discussion, the proposed technique aims at showing how to make secure an insecure cipher, that is, how to make a breakable cryptosystem unbreakable. The experimental results demonstrated that the proposed image encryption technique have advantages of large key space and high-level security, while maintaining acceptable efficiency. From the analysis of the results, the proposed algorithm satisfies uniform distribution property. Trials showed that the algorithm has many characteristics of traditional cryptography, such as almost zero correlation. Therefore, it can strongly resist statistical attack. In

addition, the proposed technique complicates the dependence of the statistics of the output on the statistics of the input. The real strength of the modified Hill cipher is that it can be adapted to work on large blocks of data.

CONCLUSION

This paper presents a symmetric cipher that is actually a variation of the Hill cipher. The proposed algorithm is called HillMRIV cipher. This algorithm provides a method for adjusting the encryption key, thereby significantly increasing its resistance to various attacks such as a known plaintext attack and statistical attack. The proposed cipher has matrix multiplication and inversion as the only operations which may be performed efficiently by primitive operators, that is, the proposed cryptosystem does not require any additional operations other than the original Hill cipher.

The results presented showed that the proposed algorithm is more effective in encryption quality than the original Hill cipher. HillMRIV cipher has the property that the statistical information of the plaintext is dissipated in a longer range of statistical structure of the ciphertext by making each ciphertext bit a function of many plaintext bits. Although the algorithm presented in this paper aims at image encryption, it is not just limited to this area and can be widely applied in other information security fields such as video encryption.

References

Barr, T.H., 2002. Invitation to Cryptography. Prentice Hall.

Chen, G., Mao, Y., Chui, C.K., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Soliton & Fractals*, **21**(3):749-761. [doi:10.1016/j.chaos.2003.12.022]

Elkamchouchi, H., Makar, M.A., 2005. Measuring Encryption Quality of Bitmap Images Encrypted with Rijndael and KAMKAR Block Ciphers. Proc. Twenty Second National Radio Science Conference (NRSC 2005), Cairo, Egypt.

Lerma, M.A., 2005. Modular Arithmetic. Http://www.math.northwestern.edu/~mlerma/problem_solving/results/modular_arith.pdf.

Li, S., Zheng, X., 2002. On the Security of an Image Encryption Method. ICIP2002. Http://www.hooklee.com/Papers/ICIP2002.pdf.

Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. *Cryptologia*, **29**(1):59-72.

Petersen, K., 2000. Notes on Number Theory and Cryptography. Http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf.

Saeednia, S., 2000. How to make the Hill cipher secure. *Cryptologia*, **24**(4):353-360.

Stinson, D.R., 2002. Cryptography Theory and Practice (2nd Ed.). CRC Press, Boca Raton, Florida.

Ziedan, I., Fouad, M., Salem, D.H., 2003. Application of Data Encryption Standard to Bitmap and JPEG Images. Proc. Twentieth National Radio Science Conference (NRSC 2003), Egypt. [doi:10.1109/NRSC.2003.1217349]