International Journal of
Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2017; 2(3): 37-43
© 2017 Stats & Maths
www.mathsjournal.com
Received: 25-03-2017
Accepted: 26-04-2017

Abdellatif Jarjar
Moulay Rachid High School
Taza Morocco

Correspondence
Abdellatif Jarjar
Moulay Rachid High School

Improvement of hill's classical method in image cryptography

Abdellatif Jarjar

Abstract

In this paper, we will introduce a new color image encryption algorithm. These images are of arbitrary sizes (n, m). This technique is based on a coupling of two chaotic maps; Namely, the logistics map and the PWLCM map. These two maps constructed and merged by a secret function *f*; which transforms two real from the interval [0 1] into number a real of the same interval. For confusion, we will use an improvement of the classical method of HILL. This improvement is none other than an affine transformation assured by a square matrix of order three with coefficient in the ring Z / 256Z. To this invertible matrix; we add a chaotic translation vector, this dynamic vector is modified at each iteration by another matrix of any order tree with coefficient in the ring Z / 256Z. A chaotic permutation in the ring Z / 3nmZ will be applied to the entire color image Finally, to avoid any differential attack, a new operating mode will be installed.The simulations carried out on the whole database showed that our new encryption technique is protected against any known attack

Keywords: G=Z/256Z; the Logistic map; H_t=Z/tZ; the Chaotic map PWLCM; Coupled chaotic map.

1. Introduction

The conventional logic card (1D) has been widely used in many color image encryption algorithms or grayscale, due to its simplicity of its good chaotic behavior. It has a strong entropy in its chaotic state. However, it allows only one control parameter and one initial value, which minimizes the key space. Moreover, some weaknesses have recently surfaced, as a non-uniformity of its distribution. Therefore, to divert the problem; A new interlaced map was constructed. This new map has several control parameters and more initial values.

HILL's classical method [1-2] is generally applied to a clear text. This method consists of two major steps. The first is the decomposition of the text to be encrypted into blocks of the same size n, with (n, n) being the size of the square matrix invertible in the ring Z/26Z. This matrix considered as the symmetric encryption key has several disadvantages. The first is that it must remain secret, the second inconveniet lies on its transfer. Finally, the major disadvantage is the linear transformation. The second step consists in making the product of the blocks by the key matrix. This linear transformation is not adapted to the encryption of images because of the strong correlation of the pixels. On the other hand, this technique is not immune to statistical attacks [3]. Nowadays; Several approaches to improving the HILL method have been developed [4-6]. However, while these new approaches sometimes resist brutal and statistical attacks, this is not the case for differential attacks. So the majority of these algorithms are not immune to differential attacks, and this is due to the absence of the application of a well-defined chaining; for the realization of an avalanche effect [7 8]. On the other hand, in our approach, we used an affine transformation, assured by a matrix of order three with a coefficient in the ring Z/256Z. This matrix is chosen from a chaotic vector. To this matrix is added a vector of translation random, but modifiable at each iteration. This ensures good confusion. After this phase, one permutation is applied to the output vector. This chaotic permutation is determined by the transformation of any chaotic vector into permutation. Finally a new operating mode is installed, this mode is other than an improvement of the operatopire mode of encryption CBC [9]. This mode of chaining achieves a better avalanche effect and makes the crypto system safe from differential attacks.

2. The Proposed Encryption Method

This algorithm implements a new color image encryption technique. This model is based essentially on an improvement of the classical HILL method. Moreover, the new crypto system is articulated on three main axes:

- Creating the necessary parameters to encrypt and decrypt the original image.
- Encryption of the clear image
- Decryption of the encrypted image

a. Creating Encryption and Decryption Settings

All parameters necessary for the proper functioning of the new algorithm are chosen from a new chaotic map. These three vectors named are RL, GL, BL. The new chaotic map is given by equation (1)

```
    $x(1), y(1), z(1)$ initialc conditions
    $k_1, k_2, k_3$ are the control parametre
for $i = 1 : N - 1$
    $x(i+1) = mod(u * k1 * y(i) * (1 - x(i)) + z(i),1)$
    $y(i+1) = mod(u * k2 * y(i) + z(i) * x(i)/(1 + x(i)),1)$
    $z(i+1) = mod(u * (x(i) + y(i) + k3) * sin(z(i)), 1)$
Next i
```
(1)

After exiberating all parameters of the vector CL; this last is converted into permutation in the ring Z/3nmZ. This transformation of a chaotic vector in a permutation is ensured by a sorting within the vector in ascending order in the broad sense. This method is described by the algorithm2.

Algorithm2: **Conversion of vector CL in permutation vector CLP in** H_{3nm}

```
For $i = 0$ to $3nm - 1$
    max = CL(i)
        For $j = 0$ to $3nm - 1$
            if CL(j) $\geq$ max Then
            max = CL(j)
            h = j
End if
        Next j
            CLP(h) = i
            CL(h) = -CL(h)
Next i
```

I. *Calculates the multiplicative inverse of in the ring Hn*

An element λ is said to be invertible in a unitary commutative ring if there exists λ^{-1} an element of the same ring such that their product is equal to 1 that is to say $\lambda\lambda^{-1} \equiv 1\,[n]$. The computation of the multiplicative inverse in the ring H_n is described by the algorithm2.

Algorithm2: ***Calculates the multiplicative inverse of*** λ

```
For $i = 1$ to $n$
    $S = (\lambda * i) \bmod n$
        If $s = 1$ then $\lambda^{-1} = i$
Next i
```

b. Encryption Of The Original Image

The encryption phase is based largely on confusion. This part is an improvement of HILL's classical method. It is an affine transformation provided by a matrix of order three invertible in the ring G. the improvement consists in the addition of a chaotic translation vector, this dynamic vector is transformed at each iteration by another affine mapping, This application is assured by any matrix of order three in G and another translation vector chosen from the CLP map. This operation is illustrated by figure1.

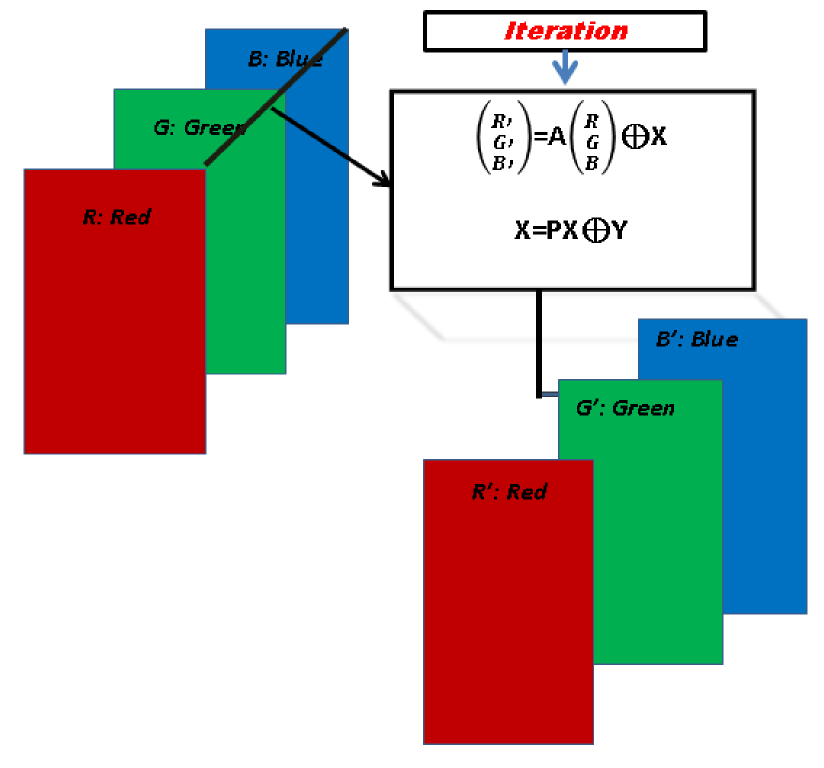
Iteration
B: Blue
G: Green
R: Red
$\begin{pmatrix} R' \\ G' \\ B' \end{pmatrix} = A \begin{pmatrix} R \\ G \\ B \end{pmatrix} \oplus X$
$X = PX \oplus Y$
B′: Blue
G′: Green
R′: Red

Figure1 Encryption by improvement of the HILL method

The diagram of figure1 is translated by the algorithm3

Algorithm3: ***First Improvement of Hill's Method***

```
For $i = 0$ to $n - 1$
    For $j = 0$ to $m - 1$
        $\overbrace{\begin{pmatrix} R'(i,j) \\ G'(i;j) \\ B'(i;j) \end{pmatrix}}^{\text{Pixel of the clear image}} = \overbrace{\begin{pmatrix} 1 & p & 0 \\ q & 1+pq & 0 \\ \alpha & \beta & \lambda \end{pmatrix}}^{A} \overbrace{\begin{pmatrix} R(i,j) \\ G(i;j) \\ B(i;j) \end{pmatrix}}^{\text{Pixel of the noisy image}} \bmod 256 \oplus \overbrace{\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}}^{X}$
// Affine transformation of the vector X
        $\overbrace{\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}}^{X} = \overbrace{\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}}^{P} \overbrace{\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}}^{X} \bmod 256 \oplus \overbrace{\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}}^{Y}$
Next j, i
```

For a sudden recurrence of the parameters of the first phase of confusion, it is necessary at least 2^{120} operations.

All parameters are in the ring G. But only λ is an invertible element in the ring G. While, all the other elements are randomly chosen from the coupled map CLP. At the end of this first step, each color matrix is converted into a vector. These three vectors are concatenated to form a single Noisy vector CV of size (1,3 nm). This constructed vector will be permuted by the chaotic permutation to give the vector CVP. The new vector is determined by the algorithm4.

Algorithm4: ***Calculates the vector CVP***

```
$For \quad i = 0 \quad to \quad 3nm - 1$
    $CVP(i) = CV(CLP(i))$
$Next \quad i$
```

c. The Diffusion

To obtain a better avalanche effect, and thus avoid any differential attack, we will install a new mode of image encryption which is an improvement of the CBC mode. The latter uses an initial value IV determined by the algorithm 6, this value belongs to the ring the ring G will be converted to binary and then permuted by a chaotic permutation *h* in the ring Z / 8Z; This permutation is chosen randomly from the coupled card and then transformed into permutation by the algorithm1.This initialization value is replaced by the value of its position in the chaotic permutation vector PL.

The vector PL is determined by the first 256 value of the chaotic CLP

Algorithm6: ***Calculate the initialization vector IV***

```
    $IV = 0$
$For \quad i = 0 \quad to \quad 3nm - 1$
    $IV = IV \oplus CVP(i)$
    $Next \quad i$
```

The transformation of the initial value calculated by the chaotic permutation ***h*** in the ring **H_8** is done according to the diagram of the figure 2.

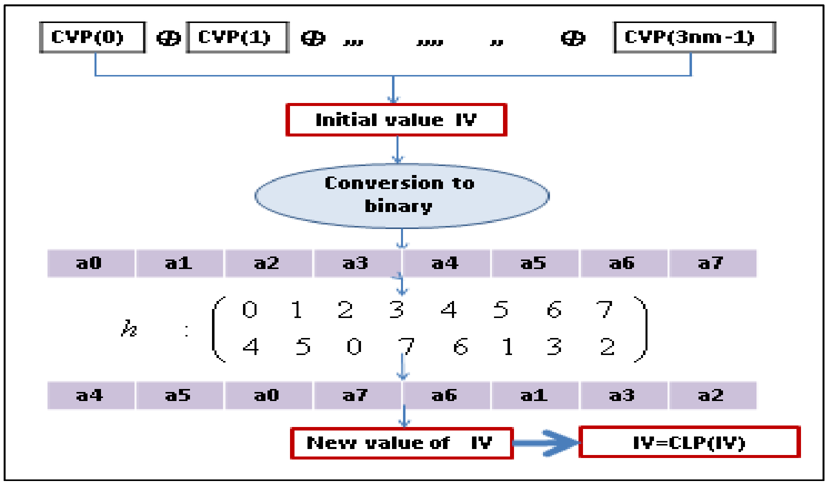

Fig 2: *Transformation of the initial value by the chaotic permutation h*

The new operating mode installed is illustrated in the figure 3. With h is a chaotic permutation in the ring H_8

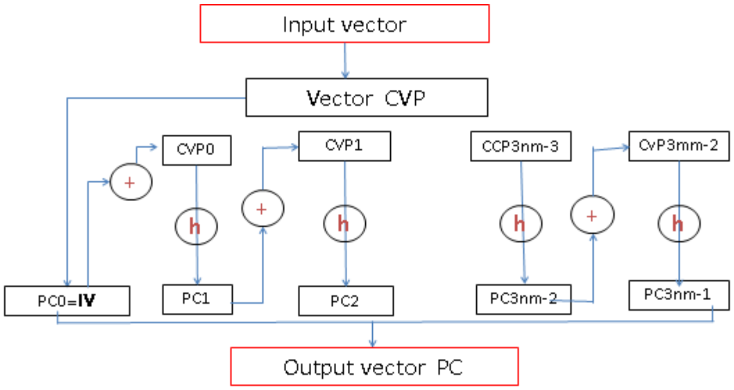

Figure3: ***New operating mode***

3. Comparison With Hill's Classical Method

An effective encryption system must guarantee high security against any type of attack. After simulations made on a database of different sized images, we notice that Hill's classic figure is incapable of correctly encrypting high-resolution images. Figure4 below shows the results of some simulations

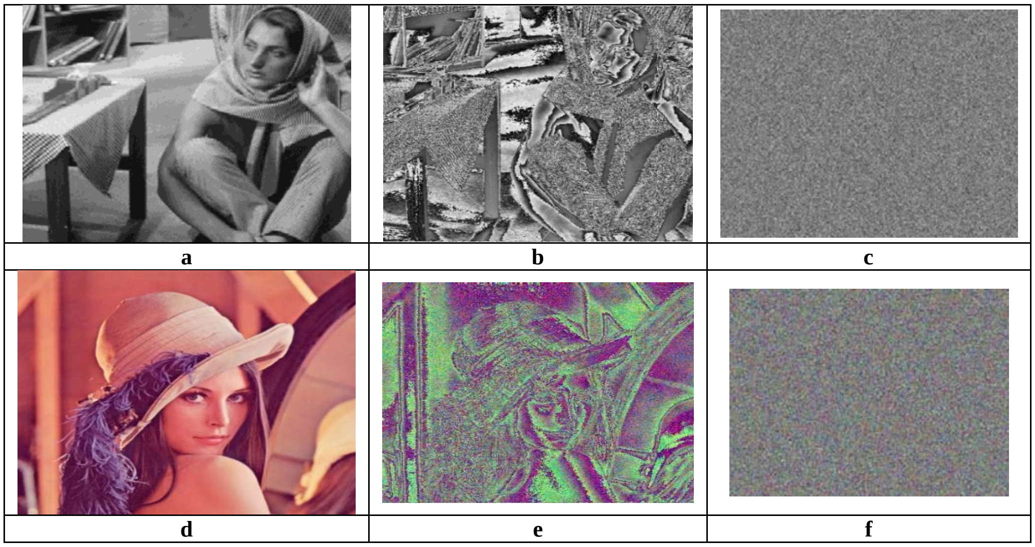

Fig 4: Original images (a,c), corresponding encrypted images by original Hill Cipher Algorithm (b,e), corresponding encrypted images by our proposed Advanced Hill algorithm (c,f)

Therefore the classical method of HILL is not recommended for the encryption of images, and especially those with strong correlation

4. Weakness Of Hill's Classical Method

For color images with strong correlation between adjacent pixels and diagonal pixels, we notice that Hill's classical method is incapable of encrypting this type of image. Figure 5 confirms these statements.

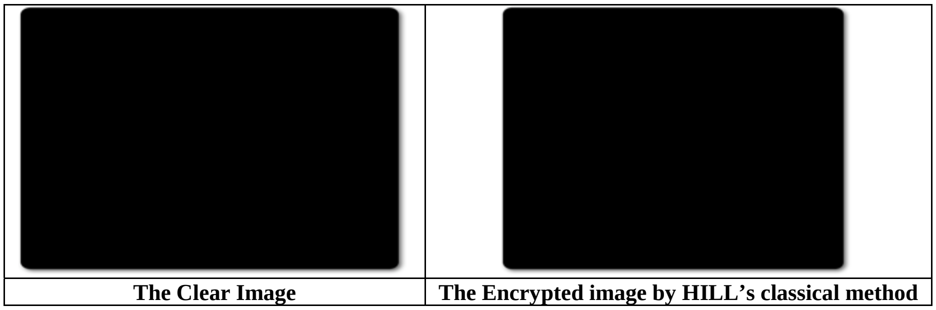

Fig 5: Weakness of the HILL’s classical method for high-resolution image encryption

We clearly see the ineffectiveness of the classical method of HILL for the encryption of images with strong correlation. Figure 6; Shows the efficiency of our method in the encryption of high correlation images

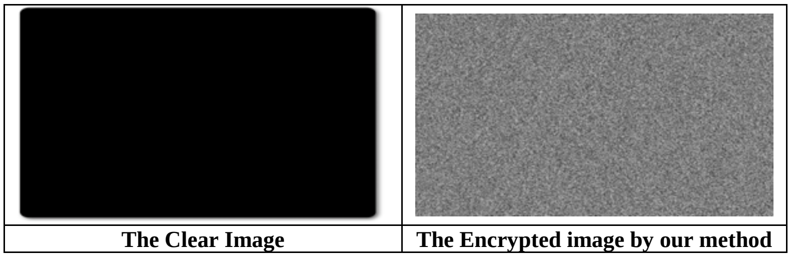

Fig 6: Encryption of high-correlation images by our method

We see clearly that our system is capable of encrypting all kinds of images, even those that have a strong correllation.

5. Security Analysis Of The Crypto System

a. Key space analysis

Our algorithm is based on the construction of the two chaotic maps, starting from four real numbers. This generates key space of the order of 2^{256} bits. So any brutal attack requires at least 2256 operations. This means that our new algorithm is immune to a brutal attack.

Any attack by reconstruction of the parameters necessary for the image encryption used by the system crypto requires at least 2^{192} operations. This size saves the algorithm from any brutal attack

b. Statistical analysis

An image can first be seen as a statistical series with a single input. The statistical constants attached to this series are computed by the equation (7).

Entropy

$$E(M) = -\sum_{i=0}^{i=255} p(i)\log_{2}(p(i)) \qquad \textbf{(7)}$$

c. Information entropy analysis

It is shown that the histogram of an image in each pixel is coded on 8 bits is uniformly distributed and only if its entropy *E (M) = 8*. Practically an encrypted image is protected against any attack by entropy if it is very Close to the maximum value 8.

Table 1 below shows the results of the entropy simulations for the original images "Lena", "Babon", "Peppers" and "Man" extracted from the database and for their corresponding encrypted images

Table 1: The entropy of the sharp image and encrypted image

NET image	Size	Entropy of the net image	Entropy of the image encrypted
Lena	512X512	7.7502	7.9990
Babon	512X512	7.7624	7.9998
Peppers	512X512	7.6698	7.9996
Man	1024X1024	7.5237	7.9994

The results of the simulation of the entropy of the encrypted images obtained in Table 1 whose values are very close to the ideal value 8 confirm the uniformity of the histograms of the encrypted images and prove resistivity to any attack by entropy.

d. Differential analysis

Table 3 below shows the results of the simulations of the differential analysis for original images extracted from the studied database.

Table 2							
Size	1024x1024	512x512	256x256	153x222	640x480	320x240	630x390
NPCR	99,60	99,76	99 ;45	99,63	99,25	99 ;71	99,42
UACI	33,30	33,27	33,40	33,29	33,32	33,32	33,35

The differential constants are in the expected norms (NPCR neighbor of 99.46, UACI neighbor of 33.34) this puts the crypto system in the shelter of any differential attack.

6. Conclusion

In this article, we introduced a new color image encryption system. This new algorithm uses a coupling of two chaotic maps. This coupling is ensured by a secret function f. This map thus created is used to extract all the parameters necessary for the proper functioning of the crypto system. By an improvement of the classical method of HILL, which consists in the addition of a chaotic translation vector, this vector is modifiable at each iteration by an affine transformation. We were able to avoid any statistical and brutal attack. A new encryption mode is installed to give a better avalanche effect and thus a high security against any differential attack. This mode is other than an improvement of the CBC encryption procedure. The application of our approach on a large database of color images of different sizes and very varied showed the robustness of this new algorithm.

7. References

1. Hill L. Cryptography in an Algebraic Alphabet, American Mathematical Monthly, 1929; 36:306-312
2. Hill L. Concerning Certain Linear Transformation Apparatus of Cryptography, American Mathematical Monthly. 1931; 38:135-154
3. Lin CH, Lee CY, Lee CY. Comments on Saeednia's improved scheme for the Hill cipher, Journal of the Chinese institute of engineers, 2004; 27(5):743-746,

4. Bibhudendra Acharya1, Saroj Kumar Panigrahy, Sarat Kumar Patra, Ganapati Panda. Image Encryption Using Advanced Hill Cipher Algorithm Int. J. of Recent Trends in Engineering and Technology, 2009; 1(1).
5. Ahmed Mahmoud, Alexander Chefranov. Hill Cipher Modification based on Pseudo-Random Eigenvalues Applied Mathematics & Information Sciences An International Journal
6. Hill LS. Cryptography in an Algebraic Alphabet American Mathematical Monthly, 1929; 36:306
7. Li C, Zhang D, Chen G. Cryptanalysis of an image encryption scheme based on the Hill cipher. Journal of Zhejiang University - Science A. 2008; 9:1118-1123.
8. Mohsen Toorani, Abolfazl Falahati. A secure variant of the Hill cipher. IEEE 2009, 313-316
9. Generation Methods for Hill Cipher System, IEEE Alvarez G. Some basic cryptographic requirements for, 2006.