Medicon Engineering Themes
Volume 1 Issue 2 November 2021
Research Article

New Image Encryption Scheme Based on Dynamic Substitution and Hill Cipher.

Younes Qobbi[1]*, Abdeltif Jarjar[2], Mohammed Essaid[3] and Abdelhamid Benazzi[1]

[1]First Mohamed University, HSTO, AMSPCS Laboratory, Oujda, Morocco

[2]High school Moulay Rachid, Taza Morocco

[3]Sidi Mohamed Ben Abdellah University, LSI, Taza, Morocco

***Corresponding Author:** Younes Qobbi, First Mohamed University, HSTO, AMSPCS Laboratory, Oujda, Morocco.

Received: November 01, 2021; **Published:** November 08, 2021

Abstract

In this work, we propose a new color image encryption technique. After transiting of the original image into a vector and decomposing it into blocks of three pixels, along with modifying of a seed block by an initialization vector computed from the plain image, a preliminary confusion will be handled by a substitution matrix developed under the control of the two chaotic maps used in the system. The achieved block will be injected in affine transformation provided by an invertible matrix accompanied by a dynamic translation vector to surmount the problem of null or uniform blocks. The encrypted block will be linked to the original block to setup diffusion and avalanche effect to protect the system from differential attacks. Simulations ap-plied to on a large number of color images prove the robustness of the pro-posed approach against known attacks.

Keywords: Chaotic maps; Affine transformation; Substitution

Introduction

In the last few years, and thanks to the immense development of communication and information technologies, the security of information exchanges through insecure networks has become a tangible problem. This is the rationale for developing effective systems to protect the transfer of confidential information. In particular the transmission of images raises a significant number of problems, such as confidentiality, and integrity [1]. Chao-based cryptography has asserted potential reliability and appropriateness for image encryption, where as traditional encryption systems (DES, IDEA, etc.) have become useless [2-4]. Currently, several crypto systems are proposed, taking advantage of the interesting properties of chaotic systems, namely pseudo-random behavior, ergodicity, and sensitivity to initial conditions [2, 5]. Fridrich is considered as the first author who introduced, in 1998, a chao-based image encryption scheme in 1998 [6, 4]. Permutation and substitution are the main pillars of any encryption system. The permutation is a bijective transformation that allows to change the position of the pixels, substitution is a new technique which makes it possible to grasp confusion, one of the Shannon's main recommendations. A. Belazi and M. Khan [7] proposed an encryption algorithm based on permutation and substitution by S-boxes. In this work, the encryption is done over two phases: a) The permutation phase of three image matrices using a chaotic cat map. b) Then a substitution is applied to the three matrices permuted by three 16×16 S-boxes created using a logistic chaotic map. In this vein, Authors Yannick P and A Tiedeu [2] suggested a fast image encryption algorithm based on new chaotic map and technique dependent on the plain image. Such as a new chaotic map is used to generate two S-Boxes. The substitution is applied to the plain image by displacement and Boolean operator XOR. In another proposal [8], Sajjad T Ali and Rashid Ali offer a three-step image encryption algorithm: In the first phase, the image pixels are swapped using a chaotic map. In the second phase a chaotic S-Box is used to replace the pixels, finally a Boolean operator XOR is used to mix a sequence of pseudo-random numbers with the pixels of the substituted image. Other algorithms [9] have adopted to improve the Hill cipher method (HC). This classic method is generally used

Citation: Younes Qobbi., et al. "New Image Encryption Scheme Based on Dynamic Substitution and Hill Cipher". Medicon Engineering Themes 1.2 (2021): 22-30.

for text encryption. It consists of choosing an encryption key in the form of an invertible 2×2 matrix. In the article [10], the authors HRAOUI and al proposed an improvement of the classical Hill algorithm, this improvement is due to the use of an invertible matrix of order three and of a vector of dynamic translation chaotic. The authors M ESSAID et al [11] presented a new image encryption algorithm based on the improvement of several chaotic maps (logistics map, sine map and Chebyshev map) and also on the use of a new version of Hill cipher, which is deemed more secure. The authors of [12] proposed an improvement of HC called HC-PRE (Hill Cipher Modification based on Pseudo-Random Eigenvalues), this technique uses pseudo-random eigenvalues to generate dynamic key matrices. The authors of the article [13] recommended a modified HC algorithm that used a single-use key matrix to encrypt each block of plain text. In this algorithm, each block is encrypted using its own key. This unique key is calculated by multiplying the current key by a secret initial vector (IV). The multiplication operation is performed row by row. The authors of [14] arrived at a new technique for generating an auto-reversible matrix used in HC. Their main objective is to overcome the problem of using any key matrix, since the encrypted message cannot be decrypted if the matrix is not invertible. The authors claimed that the computational complexity can be reduced by avoiding the process of finding the inverse of the matrix at the time of decryption, as they use a self-reversible key matrix for encryption. The authors of [15] proposed an image scrambling algorithm derived from chaos theory and Vigenère cipher in which every pixel's grey level is encrypted with the Vigenère encryption mode.

Eliminating the diffusion, the classical encryption systems of Vigenère and Hill Cipher, which apply only the confusion, are always vulnerable to differential attacks.

Respecting the Shannon's recommendations. Our method based on a combination of three basic encryption techniques namely, substitution, confusion, and diffusion, in order to increase the complexity of our encryption system. The developed scheme is founded on two chaotic maps with excellent pseudo-random properties. The effectiveness of the proposed crypto system has been validated by several experiments.

This paper is organized as follows: In the next section, the mechanism of encryption and decryption of image is described in details. In the 3rd section, the performance analyses and simulation are illustrated at length. Finally, conclusion of the present contribution is drawn in the 4th section.

Proposed Method

Based on chaos, our method is an enhanced of the HILL method and that the Vigenère. This method is articulated along five main axes:

Generating of Chaotic Sequences

Our technique is a symmetric encryption system of secret keys. Chaotic sequences are generated by two chaotic maps which are the most widely used in cryptography.

Logistics Map. It's a float sequence generated and controlled by a second-degree polynomial. Defined by the following equation:

$$\{ x_{n+1} = \mu_1 x_n (1-x_n) : \mu1 \in [3.57, 4] \text{ and } x_0 \in [0.5, 1] \qquad (1)$$

Tent Map. It is a very simple map to use in color image encryption. Defined by the following equation:

$$y_{n+1} = \begin{cases} \mu_2 y_n & \text{if } y_n < 0.5 \\ \mu_2 (1-y_n) & \text{Otherwise} \end{cases} : \mu2 \in [0, 2] \text{ } and \text{ } y_0 \in]0, 1]. \qquad (2)$$

These conditions ensure the chaotic behavior of two chaotic maps.

Preparation of Plain Image

Split the plain image of size (h, w) into the three vectors VR, VG and VB of size (1, t) such as t=h×w, which are concatenated to generate a vector Vc1 of size (1, 3×t), then a pixel's permutation is performed to decrease the correlation between adjacent pixels. this vector is divided into the blocks of three pixels.

Permutation vector Vp. The permutation vector Vp of proposed method is obtained by an ascending sort of the elements of the chaotic vector T of size (1, 3×t) created by using the chaotic sequence of PRN (Pseudo-Random Numbers) which is generated by the tent map.

Encryption Settings

Generated of Substitution Table ST. In this part, we will present the technique for generating the substitution table ST of size (256, 256). The first row of our substitution table is a permutation achieved through ascending a sort performed on the binary vector Vb, which is generated by the following algorithm.

```
For i=0 to 255
Vb(i)=(int)(x(i)*$10^{10}$)mod 2
Next i
```

The ascending sort performed on the elements of the Vb generate the initialization vector Vi.

The row of index k is obtained by a displacement of the previous row of step con-trolled by the rotation vector Vr. It is defined by the following algorithm:

```
For i=0 to 255
Vr(i)=(int)((y(i)*$10^{6}$)mod 200)+10
Next i
```

Therefore, this substitution matrix represents an enhanced Vigenèr's table. resulted by the following algorithm.

```
For j=0 to 255
  ST(1,j)=Vi(j)
Next j
For i=1 to 255
For j=0 to 255
  ST(i,j)=ST((i-1),(j+Vr(i))mod 256)
Next j
Next i
```

Enhanced Hill Cipher (EHC). In this article we use the enhanced classic cipher Hill (ECH). This improvement use a full matrix of size (3, 3) of the following form:

$$\mathrm{CH} = \begin{pmatrix} a1 & a2 & a3 \\ b1 & b2 & b3 \\ c1 & c2 & c3 \end{pmatrix} \qquad (3)$$

This matrix, used for image encryption, must be invertible in the ring *Z/256Z*. The invertible matrix used for image decryption.

Translation Vector Tv. After implementing the EHC (Enhanced Hill Cipher), a translation phase will be initiated by using the boolean operator XOR between the Vc2 vector and Tv vector. The translation vector is generated from two chaotic sequences of PRN (Pseudo-Random Numbers) created by iterating the logistics map and tent map for (3×t) times by the following algorithm.

```
For i=0 to 3*t-1
  Tv(i)=(int)(max(x(i),y(i))*$10^6$)mod 256
Next i
```

Encryption Process

Once the plain image and the encryption settings are prepared, the image encryp-tion process proposed by our method goes through the following steps.

Step (1): applying the permutation Vp on the plain image vector Vc1. This permuta-tion is attained through the following algorithm.

```
For i=0 to 3*t-1
  Vc2(Vp(i))=Vc1(i)
Next i
```

Step (2): Improving the security of our encryption algorithm against differential attacks, the diffusion action starts from the beginning of the encryption system by using the setup vector Vs of size (1, t), computed from the plain image, which allows to changing only the value of the first block of the vector Vc2. This action performed by adopting the following algorithm:

```
For i=0 to 2
  Vc2(i)=Vc2(i) ⊕ Vs(i)
Next i
```

Step (3): After the setup action, this block goes through a substitution phase by using the Substitution Table ST of size (256, 256). The block substitution is carried out by using two vectors. The first is the translation vector Tv, which used to choose the substitution row from ST. The second is the plain image vector Vc2, which used to choose the substitution column from ST. The substitution is provided by the following algorithm:

```
For i=0 to t-1
  Vc1(3*i)=ST(Tv(3*i),Vc2(3*i))
  Vc1(3*i+1)=ST(Tv(3*i+1),Vc2(3*i+1))
  Vc1(3*i+2)=ST(Tv(3*i+2),Vc2(3*i+2))
Next i
```

Step (4): After the substitution phase, the result block will be encrypted by implementing the Enhanced Cipher Hill, using the complete invertible matrix CH. The equation below stimulates the abovementioned process:

$$\begin{pmatrix} Vc2(3*i) \\ Vc2(3*i+1) \\ Vc2(3*i+2) \end{pmatrix} = \begin{pmatrix} a1 & a2 & a3 \\ b1 & b2 & b3 \\ c1 & c2 & c3 \end{pmatrix} \times \begin{pmatrix} Vc1(3*i) \\ Vc1(3*i+1) \\ Vc1(3*i+2) \end{pmatrix} \quad (4)$$

Step (5): Increasing the complexity of our encryption system, a translation phase is performed by using the following algorithm:

```
For i=0 to t-1
  Vc2(3*i)=Vc2(3*i⊕ Tv(3*i)
  Vc2(3*i+1)=Vc2(3*i+1) ⊕ Tv(3*i+1)
  Vc2(3*i+2)=Vc2(3*i+2) ⊕ Tv(3*i+2)
Next i
```

The result of this phase gives an encrypted block of three pixels, which is attached to the next plain block. The diagram below (Figure 1) represents the encryption process of the proposed method.

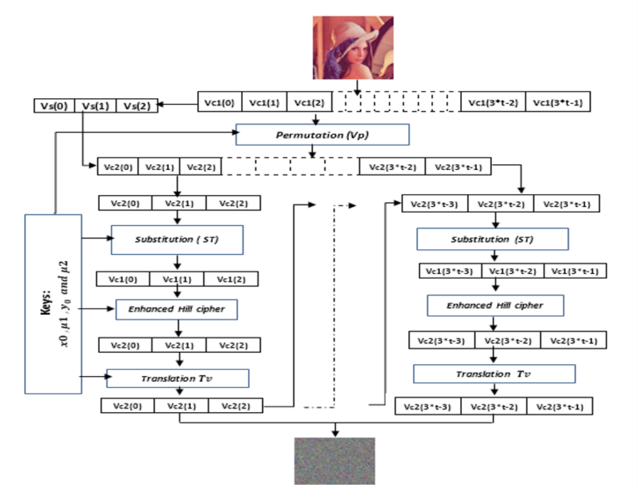


Figure 1: Diagram of encryption process.

Decryption Process

The proposed method is based on symmetric encryption of keys (x_0, μ_1) and (y_0, μ_2), afterwards, the decryption process uses the same encryption keys on condition to start with the last encryption phase.

Step (1): Split the cipher image into the blocks of three pixels.

Step (2): Using the vector (Tv) and the equation below for translation:

$$Vc1(i)=Vc1(i)\oplus Tv(i) \tag{5}$$

Step (3): Use the inverse matrix of CH.

Step (4): In this step we execute the reverse substitution by the following algorithm:

The inverse substitution of Vc2(i) giving by the algorithm as bellow.

```
For j=0 to 255
  If(ST(Tv(i),j)=Vc2(i)
  Vc1(i)=j
  Break
  End
Next j
```

Step (5): Inverse diffusing by using the following algorithm:

```
If (i>0)
   Vc1(3*i)=Vc1(3*i⊕ Vc1(3*(i-1))
   Vc1(3*i+1)=Vc1(3*i+1) ⊕ Vc1(3*(i-1)+1)
   Vc1(3*i+2)=Vc1(3*i+2) ⊕ Vc1(3*(i-1)+2)
Else
   Vc1(0)=Vc1(0) ⊕ Vs(0)
   Vc1(1)=Vc1(1) ⊕ Vs(1)
   Vc1(2)=Vc1(2) ⊕ Vs(2)
End
```

Experimental Results and Analysis

In order to prove the robustness of our proposed encryption algorithm. We present in this section several simulations: histogram analysis, Key sensitivity, correlation coefficients, entropy, NPCR and UACI. We choose several color plain images, Lena (256×256) Baboon (512×512) and ucid00622 (348×512) The plain images and its encrypted images are displayed in the following figure.

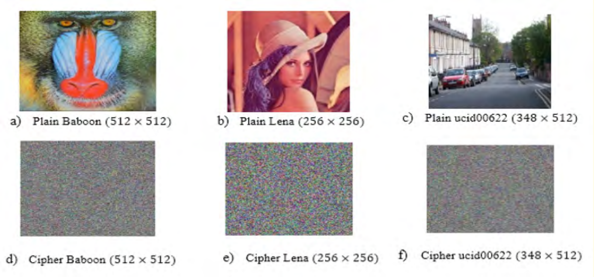

a) Plain Baboon (512 × 512)
b) Plain Lena (256 × 256)
c) Plain ucid00622 (348 × 512)
d) Cipher Baboon (512 × 512)
e) Cipher Lena (256 × 256)
f) Cipher ucid00622 (348 × 512)

Figure 2: Plain and ciphered images.

Correlation Analysis

$$Corr_{x\,y} = \frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)\times D(y)}} \qquad (6)$$

$$E(x) = \frac{1}{N}\sum_1^N x_i \text{ and } E(y) = \frac{1}{N}\sum_1^N y_i \qquad (7)$$

$$D(x) = \frac{1}{N}\sum_1^N (x_i - E(x))^2 \text{ and } D(y) = \frac{1}{N}\sum_1^N (y_i - E(y))^2 \qquad (8)$$

Where E(x), D(x) are the expectation and variance of variable x and E(y), D(y) are the expectation and variance of variable y.

The correlation of adjacent pixels from the plain images and the ciphered images of Lena (256×256) and Peppers (512×512) are shown in the table below.

	Horizontal	*Vertical*	*Diagonal*
Plain Lena (256×256)	0.9354	0.9576	0.8964
Cipher Lena (256×256)	-0.0072	0.0078	0.0039
Plain Peppers (512x512)	0.8397	0.7195	0.6985
Cipher Peppers (512x512)	-0.0064	-0.0062	-0.0049

Table 1: Correlation of adjacent pixels.

Entropy Analysis

The entropy of information is used to assess the uncertainty of a encrypted image's information. It is defined by the following equation:

$$e(m) = -\sum_{i=1}^{255} \mathrm{Pr}\,(m_i) \times \log\ \mathrm{Pr}\,(m_i) \qquad (9)$$

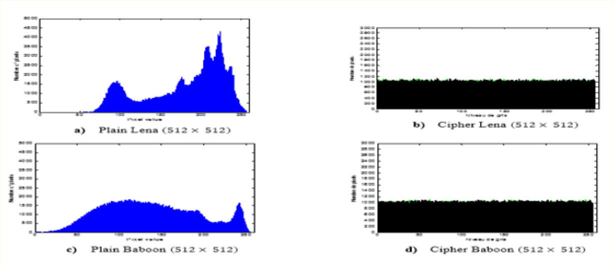
The maximum information entropy is about 8. The information entropy of our algorithm and some references are listed in the table below.

Image	*Proposed algorithm*	*Ref [6]*	*Ref [11]*	*Ref [10]*
Lena (512 x 512)	7.9998	7.9997	7.9998	7.9997
Baboon (512 x 512)	7.9998	7.9997	7.9997	--------
Peppers (512 x 512)	7.9998	7.9997	7.9998	7.9995

Table 2: Entropy of the encrypted image.

Histogram Analysis

An image histogram is a graphical representation showing the number of pixels with the same intensity value. Intensity distribution of an encrypted image has the potential to be exploited in a statistical attack. The histograms of plain images and cipher-images are shown in the following figure.



a) Plain Lena (512 × 512)

b) Cipher Lena (512 × 512)

c) Plain Baboon (512 × 512)

d) Cipher Baboon (512 × 512)

Figure 3: Histogram analysis.

Keys Analysis

In the proposed system, the key composed of two initial values x_0 and y_0, and two control parameters μ_1 and μ_2. Which are the floats represented in 32 bits. The key space size is much greater to 2^{104}. Then the key space is large to stay secure against the brute force attack [16].

Differential Analysis

Sometimes, attackers make a small modification in the plain image, and then ap-ply the encryption algorithm to encrypt the original image and the changed image in order to observe how a tiny change in the plain image influence the encrypted image by comparing the two encrypted images. The sensitivity of a cryptosystem is evaluated through a Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Their definitions are presented as follows.

$$NPCR = \frac{\sum_1^w \sum_1^h D_{i\,j}}{w * h} \times 100\% \tag{10}$$

$$UACI = \frac{1}{w \times h} \frac{\sum_{i\,j} \left| IC1_{i\,j} - IC2_{i\,j} \right|}{255} \times 100\,\% \tag{11}$$

$$D_{i\,j} = \begin{cases} 1 & if \quad IC1_{i\,j} \neq IC2_{i\,j} \\ 0 & \qquad else \end{cases} \tag{12}$$

The following table below shows the measurement of NPCR and UACI between two cipher images of the Babon (512×512) Lena (512×512) and Peppers (512×512). When making a slight change in the plain image.

Plain image	***Proposed scheme***		***Ref [6]***	
	NPCR	***UACI***	***NPCR***	***UACI***
Baboon	99.6189	33.4695	99.6090	33.457
Lena	99.6150	33.4277	99.6190	33.447
Peppers	99.6120	33.4650	99.6080	33.466

Table 3: NPCR and UACI value.

Conclusion

This work outlines a new color image encryption technique involving a substitution matrix that represents a deep refinement of Vigenère's method combined to a Hill's technique application on three pixels blocks, provided by an invertible matrix of arbitrary form. The new S-Box design technique can be easily modified and improved. The encryption method applied in the present paper brings strength to our algorithm. The simulation results and security analysis presented by a correlation coefficient close to zero and a flat histogram of the encrypted image ensure an entropy value close to 8, which have proved that the proposed image encryption scheme meets all the performance requirements of image encryption design criteria.

References

1. Machkour M., et al. "A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher". 3D Research 6.4 (2015): 36.
2. Nkandeu YPK and Tiedeu A. "An image encryption algorithm based on substitution technique and chaos mixing". Multimedia Tools and Applications 78.8 (2019): 10013-10034.
3. Chen G., et al. "A symmetric image encryption scheme based on 3D chaotic cat maps". Chaos, Solitons & Fractals 21.3 (2004): 749-761.
4. Fridrich J. "Symmetric ciphers based on two-dimensional chaotic maps". International Journal of Bifurcation and chaos 8.6 (1998): 1259-1284.
5. Jakimoski G and Kocarev L. "Chaos and cryptography: block encryption ciphers based on chaotic maps". Ieee transactions on circuits and systems i: fundamental theory and applications 48.2 (2001): 163-169.
6. Fu C., et al. "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy". Security and Communication Networks (2018).

7. Belazi A., et al. “Efficient cryptosystem ap-proaches: S-boxes and permutation–substitution-based encryption”. Nonlinear Dynamics 87.1 (2017): 337-361.
8. Ali TS and Ali R. “A new chaos-based color image encryption algorithm using permutation substitution and Boolean operation”. Multimedia Tools and Applications 79.8 (2020): 1-21.
9. Hill LS. “Cryptography in an algebraic alphabet”. The American Mathematical Monthly 36.6 (1929): 306-312.
10. Hraoui S., et al. “A New Cryptosystem of Color Image Using a Dynamic-Chaos Hill Cipher Algorithm”. Procedia computer science 148 (2019): 399-408.
11. Essaid M., et al. “Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps”. Journal of Information Security and Applications 47 (2019): 173-187.
12. Mahmoud A and Chefranov A. “Hill cipher modification based on pseudo-random eigenvalues”. Applied Mathematics & Information Sciences 8.2 (2014): 505.
13. Ismail IA., et al. “How to repair the Hill cipher”. Journal of Zhejiang University-Science A 7.12 (2006): 2022-2030.
14. Overbey J., et al. “On the key space of the Hill cipher”. Crypto-logia 29.1 (2005): 59-72.
15. Li S and Zhao Y. “Image scrambling based on chaos theory and Vigenère cipher”. In 2011 Seventh International Conference on Computational Intelligence and Security, IEEE (2011): 555-558.
16. François M., et al. “A new image encryption scheme based on a chaotic function”. Signal Processing: Image Communication 27.3 (2012): 249-259.

Volume 1 Issue 2 November 2021