CONNECTION OF TWO CONVENTIONAL ENHANCED TO ENCRYPT COLOR IMAGES

Said Hraoui  
LIASSE, ENSA, SMBA University  
Fez, Morocco  
said.hraoui@usmba.ac.ma,

Abdellatif JarJar  
Moulay Rachid High School,  
Taza, Morocco  
abdoujjar@gmail.com

Abstract

This document introduces a new cryptosystem mixing two improvement standards generally used for text encryption, in order to give birth a new color image encryption algorithm capable of dealing with known attacks. Firstly, two substitution matrixes attached to a strong replacement function will be generated for advanced Vigenere technique application. At the end of this first round, the output vector is subdivided into size blocks according to the used chaotic map, for acting a single enhanced Hill circuit insured by a large inversible matrix. A detailed description of such a large involutive matrix constructed using Kronecker products will be given, accompanied by a dynamic translation vector to eliminate any linearity. A solid chaining is established between the encrypted block and the next clear block to avoid any differential attack. Simulations carried out on a large volume of images of different sizes and formats ensure that our approach is not exposed to any known attacks.

Article Highlights

This new algorithm is the mixture result of two deeply improved classical systems which we mention the most important changes made.

- New size substitution matrix (256,256) Construction
- Strong replacement functions definition
- Improved Vigenere technology application
- Kronecker products Theoretical reminder
- Kronecker product Application
- Large invertible matrix design
- Single enhanced Hill revolution application

Notation

\[
G_t = \mathbb{Z}/t\mathbb{Z} \quad \text{ring}
\]

\[
A(j): \text{Line number } j \text{ of matrix } A
\]

\[
A(:,j): \text{column number } j \text{ of matrix } A
\]

\[
\oplus: \text{Xor operator} \quad \otimes: \text{Kronecker product}
\]

\[
E(x): \text{The whole part of the real number } x
\]

Key word: Vigenere grid; Involutive matrix; Chaotic map; Broadcast function; genetic operator
I. INTRODUCTION

The rapid development of chaos theory in mathematics provides researchers with opportunities to further improve some classic encryption systems. In front of this great security focus, many techniques for color image encryption have flooded the digital world, mostly exploiting number theory and chaos [1,2]. Others are attempting to update their policies by improving some classical techniques, such as Hill [3 – 4], Cesar, Vignere [5 – 6], Feistel [7 – 8].

1) Vigenere's classical technique

This technology is based on static (V) matrix defined by the following algorithm

\[
\text{Fist Row} \\
\text{For } i = 1 \text{ to } 26 \\
V(1,i) = i \\
\text{Next } i \\
\text{following Rows} \\
\text{For } i = 2 \text{ to } 26 \\
\text{For } j = 1 \text{ to } 26 \\
V(i,j) = V(i-1,(j+1),26) \\
\text{Next } j,i
\]

Let \((P)\): plain text, \((C)\): cypher text; \((K)\): Encryption key, \((V)\) Vigenere matrix and \((l)\): length of clear text. So

\[
\text{equation1} \left\{ \begin{array}{ll}
C_i = V(P_i,K_i) = (P_i + K_i) \mod 26 \\
P_i = V(C_i,K_i) = (P_i - K_i) \mod 26
\end{array} \right.
\]

Even though Vigenere's matrix was known, the encryption was able to withstand several centuries. But, Babagh's cryptanalysis is not efficient in not knowing the size of the encryption key. Several attempts to improve Vigenere's technique have invaded the digital world we quote [9 – 10]. In this work, the new structure of the substitution matrix and its attached replacement function will be described in detail.

2) Hill’s classical technique

Hill's method is a classic symmetric encryption system that uses a linear transformation provided by an invertible matrix in a carefully selected ring [11 – 12].

\((C)\):plain text \((C')\): cypher text; \((K)\): Encryption key, the method is defined by the following linear formula

\[
\text{Equation2} \left\{ \begin{array}{ll}
C' = KC \\
\text{So} \\
C = K^{-1}C'
\end{array} \right.
\]

Unfortunately, this technique is still exposed to known attacks. Since then, over time, several improvements have been made to the system [13 – 14]. The improvement of the classic Hill technique tracked in this document is to prove the construction of a large invertible matrix whose size will be randomly calculated based on the chaotic graph used. Some advanced techniques in the same axis should be taken into consideration [15 – 16].
3) Our contribution
Our contribution in this article is to couple two conventional deeply improved systems to better adapt to color image encryption. These improvements, made on the two classic systems are

\begin{align*}
\text{Vigenere} & \\
\text{New substitution matrices construction} & \\
\text{New attached replacement functions definition} & \\
\text{Application of a diffusion ensured by two size maatrix (256,256)} & \\
\text{Hill} & \\
\text{Large key matrix Construction} & \\
\text{Applying an affine transformation} & \\
\text{Dynamic translation vector} & 
\end{align*}

II. THE PROPOSED METHOD
Based on chaos, our new technology is divided into three main stages

- **first phase:**
  - action on a single pixel with broadcast installation
- **Second phase:**
  - subdivision of the image into blocks of size \((4r)\)
- **Third phase**
  - Construction of an invertible matrix of size \((4r, 4r)\)
  - action on blocks of \((4r)\) pixels by a Hill lap

The image below shows this technology steps
This new cryptosystem is based on the following axes:

**AXE I: CHAOTIC SEQUENCES DEVELOPMENT**

In order to build a new algorithm using a single-encryption key, we will use the 2d logistics map. This choice is due to the simplicity of its development and its high sensitivity to the initial parameters.

1) **2D Logistics Map**

\[
\begin{align*}
    x_0, y_0 & \in [0, 1] \\
    x_{n+1} &= \mu_1 x_n (1 - x_n) + \mu_2 y_n^2 \\
    y_{n+1} &= \mu_3 y_n (1 - y_n) + \mu_4 (x_n^2 + x_n y_n) \\
    \mu_1 &\in [2.75, 3.4] \\
    \mu_2 &\in [0.13, 0.15] \\
    \mu_3 &\in [2.75, 3.45] \\
    \mu_4 &\in [0.13, 0.15]
\end{align*}
\]
2) Chaotic used vector design

Our work requires the construction of three chaotic vectors $(CL), (KR)$ and $(KL)$, with a coefficient in $(G_{256})$, and two $(CR), (CV)$ binary vector will be regarded as the control vector. This construct is seen by the following algorithm

Algorithm 2

\[
\begin{align*}
for \ i = 1 \ to \ 3nm \\
CL(i) &= \text{mod}\left(\frac{x(i) + \sup (x(i), y(i))}{2} \times 10^{11}, 254\right) + 1 \\
KL(i) &= \text{mod}\left(\frac{x(i) \times y(i) + \inf (x(i), y(i))}{2} \times 10^{10}, 253\right) + 2 \\
KR(i) &= E\left(\frac{KL(i) + CL(i)}{2}\right) \\
&\text{if } x(i) \geq y(i) \text{ then} \\
&\text{CR}(i) = 0 \text{ else } CR(i) = 1 \text{ end if} \\
&\text{if } CL(i) < KL(i) \text{then} \\
&CV(i) = 1 \text{ else } CV(i) = 0 \text{ end if} \\
&\text{Next i}
\end{align*}
\]

3) Global permutation Design

Sorting the $(CR)$ vector in a large decreasing order generates the $(PH)$ global permutation. This method is illustrated by the following algorithm

Algorithm 3

\[
\begin{align*}
k &= 1 \\
\text{For } i = 3nm \ to \ 1 \\
&\text{If } CR(i) = 0 \text{ Then } PH(i) = k \\
&k = k + 1 \\
&\text{end if} \\
&\text{Next i}
\end{align*}
\]

Example:

\[
\begin{array}{cccccccccccccccc}
(CR) & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
\hline
\text{Set} & 9 & 8 & 10 & 11 & 12 & 7 & 13 & 6 & 14 & 15 & 5 & 16 & 4 & 17 & 18 & 3 & 2 & 19 & 20 & 1 \\
\end{array}
\]

\[
(PH) = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20)
\]

III. INSTALL THE NEW ENCRYPTION METHOD

Based on chaos, our new technology is based on two encryption processes each using a deep improvement of a classic system.
**AXE 2: VIGENERE UPGRADE**

In the first stage, Vigenere's technology was greatly modified by integrating the new substitution matrix provided by the new powerful replacement function.

1) **Original image Vectorization**

After the three (RGB) color channels extraction and their conversion into size vectors \((Vr), (Vg), (Vb)\) each, a concatenation is established to generate a vector \(X(x_1, x_2, \ldots, x_{3nm})\) of size \((1, 3 nm)\). This operation is described by the following algorithm:

\[
\begin{align*}
\text{Algorithm 5} & \quad \left\{ \\
\text{for } i = 2 \text{ tonm} & \\
X(3i - 2) &= Vr(i) \\
X(3i - 1) &= Vg(i) \\
X(3i) &= Vb(i) \\
\text{Next } i & \\
\end{align*}
\]

2) **Initialization Value Design**

The \((IV1)\) initialization value must be recalculated to change the value of the starting pixel. Ultimately, the \((IV1)\) value is provided by the next algorithm:

\[
\begin{align*}
\text{Algorithm 6} & \quad \left\{ \\
\text{for } i = 2 \text{ to } l & \\
\text{if } CV(i) = 0 \text{ then} & \\
v_1 &= v_1 \oplus X(i) \oplus CL(i) \\
\text{Else} & \\
v_1 &= v_1 \oplus X(i) \oplus KL(i) \\
\text{Next } i & \\
\end{align*}
\]

This initialization value is set only to modify the value of the seed pixel and start the encryption process. By implementing chaotic mapping in the calculation of the initialization value, the problem of uniform image color (black, white, ... ) can be solved.

3) **Vigenere’s advanced methods**

This new technology requires the establishment of two \((VG)\) and \((VD)\) substitution matrices through the process described by the following steps:

- permutation \((RP)\) obtained by descending ordering the first 256 values of the sequence \((U)\),
- permutation \((RR)\) obtained by increasing the ordering the first 256 values of the sequence \((V)\),

with the following restrictions:

\[
\begin{align*}
\text{Equation 7} & \quad \left\{ \\
\text{if } RP(i) = 256 \text{ the } RP(i) = 0 & \\
\text{if } RR(i) = 256 \text{ the } RR(i) = 0 & \\
\end{align*}
\]

This new construction is entirely supervised by the vector \((CR)\) seen as a decision vector. It is given by the following algorithm.
algortithm

\[
\begin{align*}
\text{Fist Row} \\
\text{For } i = 1 \text{ to } 256 \\
V_G(1, i) &= RP(i) \\
V_D(1, i) &= RR(i) \\
\text{Next } i
\end{align*}
\]

\[
\begin{align*}
\text{For } i = 1 \text{ to } 256 \\
\text{For } j = 1 \text{ to } 256 \\
\text{if } CV(i) = 1 \text{ then} \\
V_G(i, j) &= V_G\left(i - 1, RP\left(mod\left(j + CL(i), 256\right)\right)\right) \\
V_D(i, j) &= V_D\left(i - 1, RR\left(mod\left(j + KL(i), 256\right)\right)\right) \\
\text{else} \\
V_G(i, j) &= V_G\left(i - 1, RP\left(mod\left(j + KL(i), 256\right)\right)\right) \\
V_D(i, j) &= V_D\left(i - 1, RR\left(mod\left(j + CL(i), 256\right)\right)\right) \\
\text{end if} \\
\text{next } j, i
\end{align*}
\]

We note that the construction of the two matrices is completely determined by the \((CV)\) decision vector.

**Example: in \((G_8)\)**

\[
\begin{array}{cccccccccccccccc}
\hline
& \text{VG} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \\
\hline
1 & 1 & 3 & 5 & 0 & 6 & 2 & 7 & 1 & 4 \\
2 & 2 & 7 & 1 & 4 & 3 & 5 & 0 & 6 & 1 \\
3 & 4 & 3 & 5 & 0 & 6 & 2 & 7 & 1 & 1 \\
4 & 2 & 7 & 1 & 4 & 3 & 5 & 0 & 6 & 1 \\
5 & 0 & 2 & 7 & 1 & 4 & 3 & 5 & 1 & 1 \\
\hline
\end{array}
\]

**a) New Vigenere’s mathematical expression**

The classical Vigenere transformation expression is given by the following formula

\[Y(i) = V_G(CL(i), X(i))\]

The following equation illustrates the effective expression of the \(Y(i)\) image of the pixel \(X(i)\) through the new Hill technology.

\[
\begin{align*}
\text{if } CR(i) = 0 \text{ then} \\
Y(i) &= V_G(CL(i), V_D(KR(i), (mod(a \times X(i), 256) \oplus KL(i)))) \\
\text{else} \\
Y(i) &= V_D(KL(i), V_G(KR(i), (mod(c \times X(i), 256) \oplus CL(i)))) \\
\end{align*}
\]

With; \(a, c \in G_{256}^*\)

\[
\begin{align*}
\text{Let} \\
a &= \text{mod}\left(2 \times \text{mod}\left(\sum_{i=1}^{n} CL(i)\right) + 1, \ 256\right) \\
c &= \text{mod}\left(2 \times \text{mod}\left(\sum_{i=1}^{nm} KL(i)\right) + 1, \ 256\right)
\end{align*}
\]
We noticed that this new expression is firmly attached to the (CR) decision vector, and uses two general substitution matrices to contain powerful substitution functions.

2) First Encryption Process

With a powerful broadcast function, this first encryption process will protect the system from differential attacks and increase the time complexity of the attack. The figure below illustrates the first encryption process improved using only Vigenere

![Vigenere Encryption Diagram]

\(\text{(VG)}:\) advanced substitution matrix

\(\text{(Π)}:\) New diffusion function

The new diffusion function using matrix \((VD)\) is described by the following formula

\[
\text{Equation10} \quad \Pi(X(i+1)) = VD(KR(i), X'(i) \oplus X(i+1))
\]

This schema is translated by the algorithm below

\[
\text{Algorithm8} \quad \begin{cases} 
X'(1) = VG(KR(1), VD(CL(1), v_1) \oplus X(1) \\
\text{For } i = 2 \text{ to } 3n_m \\
\Pi(X(i)) = VD(KR(i), X'(i-1) \oplus X(i)) \\
\text{if } CR(i) = 0 \text{ then} \\
X'(i) = VG(CL(i), \left(mod(a \ast \Pi(X(i)), 256) \oplus KL(i) \right) \\
\text{else} \\
X'(i) = VG(KL(i), \left(mod(c \ast \Pi(X(i)), 256) \oplus CL(i) \right) \\
\text{Next } i
\end{cases}
\]

We note that this first step uses only substitutions, which ensures an extreme speed in the execution. The output vector \(X'(x'_1, x'_2, \ldots \ldots, x'_{3nm})\), will undergo a second encryption attempt.
AXE 3: APPLYING HILL UPGRADE

Before starting the second encryption stage, we will introduce in detail some mathematical knowledge useful for constructing invertible matrix and, install a hill lap.

1) Math reminder
Several new knowledges with mathematical bases must be clarified

a. related information
In this section, we will introduce the concept of diastereomeric matrices and Kronecker products used to construct large invertible matrices.

i. Involutive matrix

a) Definition
A is an involutive matrix if and only if we have

\[ A^{-1} = A \]

In other words

\[ A^2 = I \]  \text{I identity matrix}

b. Building the \((A)\) matrix
Assume that the size of \((A)\) matrix is \((2r_h, 2r_h)\), and is defined by block as follows

\[ A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \text{ of size } (r_h, r_h) \]

We got

\[ A^2 = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} A_1^2 + A_3A_2 & A_2A_1 + A_4A_2 \\ A_1A_3 + A_3A_4 & A_2^2 + A_2A_3 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} \]  \text{Identity Matrix}

Since matrix \((A)\) is involutive, we get

\[
\begin{align*}
A_1^2 + A_2A_3 &= I \\
A_2A_1 + A_4A_2 &= 0 \text{ with } 0: \text{Null matrix} \\
A_1A_3 + A_3A_4 &= 0 \\
A_2^2 + A_3A_2 &= I
\end{align*}
\]

So

\[
\begin{align*}
A_2A_3 &= I - A_1^2 = (I - A_1)(I + A_1) \\
A_3A_2 &= I - A_4^2 = (I - A_4)(I + A_4)
\end{align*}
\]

Since \((A_1)\) matrix is given randomly, other matrices can be selected by the following formula

\[
\begin{align*}
A_2 &= k(I - A_1) \\
A_3 &= k^{-1}(I + A_1) \quad (k \in G_{256}^*) \\
A_4 &= 256 - A_1
\end{align*}
\]
Or We can take

\[
\begin{align*}
A_2 &= k(I + A_1) \\
A_3 &= k^{-1}(I - A_1) \\
A_4 &= 256 - A_1
\end{align*}
\]

This gives

\[
A = \begin{pmatrix}
A_1 & k(I - A_1) \\
k^{-1}(I + A_1) & 256 - A_1
\end{pmatrix}
\]

Example

\[
\begin{pmatrix}
1 & 3 \\
2 & 5
\end{pmatrix} \quad k = 3 \quad \text{and} \quad k^{-1} = 3
\]

So

\[
A = \begin{pmatrix}
1 & 3 & 0 & 7 \\
2 & 5 & 2 & 4 \\
6 & 1 & 7 & 5 \\
6 & 2 & 6 & 3
\end{pmatrix}
\]

Under these conditions, the obtained matrix (A) is involute. This choice is not unique, and it increases the complexity of matrix (A) reconstruction.

2) **Kronecker matrix product**

Matrix theory is widely used in cryptography. Due to its difficulties, classical computing techniques are rarely used. For example, it is difficult to reverse the large matrix using conventional methods. At present, the Kronecker product and the tensor product are not only connected with physics or biology, but also take a safe path in cryptography. We are going to take advantage of the Kronecker product to increase the size of the involutive matrix.

a. **Definition**

Let \(A = (a_{i,j})\) of size \((n,m)\) and Let \(B = (b_{i,j})\) of size \((p,q)\). We call the Kronecker product of \(A\) and \(B\), denoted by

\[
C = A \otimes B = \begin{pmatrix}
a_{1,1}B & \cdots & a_{1,m}B \\
\vdots & \ddots & \vdots \\
a_{n,1}B & \cdots & a_{n,m}B
\end{pmatrix}
\]

of size \((np;mq)\)

Example

\[
A = \begin{pmatrix}
1 & 3 \\
2 & 5
\end{pmatrix} \quad B = \begin{pmatrix}
1 & 2 & 0 \\
3 & 1 & 2 \\
0 & 5 & 4
\end{pmatrix}
\]

so

\[
C = A \otimes B = \begin{pmatrix}
1 & 2 & 0 & 3 & 6 & 0 \\
3 & 1 & 2 & 9 & 3 & 6 \\
0 & 5 & 4 & 0 & 15 & 12 \\
2 & 4 & 0 & 5 & 10 & 0 \\
6 & 2 & 4 & 15 & 5 & 10 \\
0 & 10 & 8 & 0 & 25 & 20
\end{pmatrix}
\]

b. **Kronecker Product Properties**

The product is not commutative

\[A \otimes B \neq B \otimes A\]

c. **Reversibility**
If $A$ and $B$ are involutive matrices, then their Kronecker product is involutive and we have

\[
(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}
\]

**Equation 22**

**3) ($X'$) Vector Adaptation**

In order to facilitate the implementation of the second encryption stage, the vector ($X'$) must be cut into blocks uniform, we are going to calculate two constants $r_1$ and $r_2$

\[
\begin{cases}
    r_1 = \left( \text{mod} \left( \frac{1}{n} \sum_{i=1}^{n} |CL(i) - KL(i)|, 4 \right) + 2 \right) \text{ so } 2 \leq r_1 \leq 5 \\
    r_2 = \left( \text{mod} \left( \frac{1}{m} \sum_{i=1}^{m} |CL(i) - KR(i)|, 3 \right) + 2 \right) \text{ so } 2 \leq r_2 \leq 4
\end{cases}
\]

**Equation 23**

We put

\[16 \leq r = 4r_1r_2 \leq 80\]

Therefore, the new vector size ($X'$) can be obtained by the following formula

\[
\begin{cases}
    \text{let } 3nm \equiv s \ [r] \\
    l = 3nm - s \\
    t = \frac{l}{r}
\end{cases}
\]

**Equation 24**

By truncating the last ($s$) ($X'$) pixel, and placing it in the ($XD$) vector after modification, the ($XT$) adaptive vector can be obtained by the following algorithm

\[
\text{Algorithm 9}
\]

\[
\begin{cases}
    \text{for } i = 1 \text{ to } l \\
    XT(i) = X'(i) \\
    \text{Next } i
\end{cases}
\]

\[
\begin{cases}
    \text{Amputated pixel storage} \\
    \text{for } i = 1 \text{ to } s \\
    \text{if } CR(i + l) = 0 \text{ then} \\
    XD(i) = X'(i + l) \oplus CL(i + l) \\
    \text{else} \\
    XD(i) = X'(i + l) \oplus KL(i + l) \\
    \text{end if} \\
    \text{Next } i \\
    \text{end if}
\end{cases}
\]

**4) Switching to a size matrix**

The following figure illustrates the transaction from vector to size matrix ($t,r$) used in the Hill circuit
Hill’s classical method is predominantly oriented on invertible matrices in accurately indexed rings. Inverting a large matrix remains the main challenge of this technique, which prompts scholars to use only small matrices typically of size $\leq 4$.

2) New Hill matrix Development

In our algorithm, in order to overcome this problem, we will introduce in detail a new simple method of constructing large invertible matrix based on involute matrix.

Let $(A_1)$ be an arbitrary matrix of size $(r_1, r_1)$ and let the matrix $(A)$ defined by

$$Equation \ 25 \quad A = \begin{pmatrix} A_1 & k(l - A_1) \\ k^{-1}(I + A_1) & 256 - A_1 \end{pmatrix} \quad (k \in G_{256}^*) \ \text{of size} \ (2r_1, 2r_1)$$

Let $(B_1)$ be an arbitrary matrix of size $(r_2, r_2)$ and let the matrix $(B)$ defined by

$$Equation \ 26 \quad B = \begin{pmatrix} B_1 & h(l - B_1) \\ h^{-1}(I + B_1) & 256 - B_1 \end{pmatrix} \quad (h \in G_{256}^*) \ \text{of size} \ (2r_2, 2r_2)$$

The two matrices $(A)$ and $(B)$ are involutive.

We put

$$Equation \ 27 \quad H = A \otimes B$$

The matrix $(C)$ is invertible and involutive of size $(4r, 4r)$. The matrix $(C)$ is condadate for a key Hill matrix.

3) New encryption matrix construction

This second encryption process is illustrated by the following figure
4) Enhanced HILL function expression

\[
\text{Algorithm 11} \quad \text{Hill} \quad \begin{cases} 
\text{if } CV(k) = 0 \text{ then} \\
GM(k:) = H \ast MT(k:) \oplus KT(k:)
\end{cases} \\
\text{else} \\
GM(k:) = H \ast MT(k:) \oplus CT(k:)
\]

Build diffusion to increase the impact of the avalanche effect

\[
\text{Equation 28} \quad \{F(MT(k + 1:) = GM(k:) \oplus MT(k + 1:) \oplus CT(k:))
\]

An insertion of the pixels of the vector \((XD)\) at the end of the obtained vector \((CX)\) on which the permutation \((PH)\) is established by the following algorithm

\[
\text{Algorithm 16} \quad \begin{cases} 
\text{for } i1 = 1 \text{ to } 3nm \\
X(C) = CX(PH(i)) 
\end{cases} \\
\text{Next } i
\]

The vector \((XC)\) represents the encrypted image.
**STEP 5: DECRYPTION ENCRYPTED IMAGES**

The solid chaining establishes between the encrypted block and the next clear block in the broadcast process, forcing us to start decryption from the last block using the opposite functions. So, the decryption process should follow these steps:

- **Read the encrypted image and switch to vector** \((XC)\)
- **Application of the permutation** \((HP)\) **inverse of the permutation** \((PH)\)

\[
\text{Algorithm 17}
\begin{align*}
\text{For } i = 1 \text{ to } 3nm \\
HP(\text{PH}(i)) &= i \\
\text{Next } i
\end{align*}
\]

\[
\text{Algorithm 18}
\begin{align*}
\text{For } i = 1 \text{ to } 3nm \\
CX(i) &= XC(HP(i)) \\
\text{Next } i
\end{align*}
\]

- **Recalculates the value** \((r)\) **size of the subdivision blocks**
- **Recalculates** \((A)\) **and** \((B)\)
- **Reverse Hill application** \((A^{-1} = A, B^{-1} = B \quad H = A \otimes B = H^{-1})\)

1) **Mathematical HILL inverse expression**

\[
\text{Algorithm 11} \quad HILL^{-1}
\begin{cases}
\text{if } CV(k) = 0 \text{ then} \\
MT(k:) = H^{-1}(MT(k:) \oplus KT(k:)) \\
\text{else} \\
MT(k:) = H^{-1}(MT(k:) \oplus CT(k:))
\end{cases}
\]

- **Reconstruct the image vector and add vector pixels** \((XD)\) **to the queue**
- **Reverse Vigenere application**

\[
\text{Algorithm 20}
\begin{cases}
\text{for } i = 1 \text{ to } 256 \\
\text{for } j = 1 \text{ to } 256 \\
GV(i, VG(i, j)) &= j \\
DV(i, VD(i, j)) &= j \\
\text{Next } j, i
\end{cases}
\]

**Example**

![Image of Vigenere's Table](image)

By following the same logic of Vigenere’s traditional technique, we obtain

\[
\text{Equation 21}
\begin{cases}
\text{if } z = VG(y, x) \\
\text{Then} \\
x &= GV(y, z)
\end{cases}
\]
2) Mathematical Vigenere inverse expression

We have

\[
\begin{align*}
\text{Algorithm 8} & \quad \text{For } i = 2 \text{ to } 3n \\
\Pi(X(i)) &= VD(KR(i), X'(i - 1) \oplus X(i)) \\
\text{if } CR(i) &= 0 \text{ then} \\
X'(i) &= VG(CL(i), (mod(a \ast \Pi(X(i)), 256) \oplus KL(i)) \\
\text{else} & \\
X'(i) &= VG(KL(i), (mod(c \ast \Pi(X(i)), 256) \oplus CL(i)) \\
\text{Next } i
\end{align*}
\]

So

\[
\begin{align*}
X'(i) &= VG(CL(i), (mod(a \ast \Pi(X(i)), 256) \oplus KL(i)) \\
(mod(a \ast \Pi(X(i)), 256) \oplus KL(i)) &= GV(CL(i), X'(i)). \\
(mod(a \ast \Pi(X(i)), 256) &= GV(CL(i), X'(i)) \oplus KL(i) \\
\Pi(X(i)) &= a^{-1}(GV(CL(i), X'(i)) \oplus KL(i)) \\
VD(KR(i), X'(i - 1) \oplus X(i)) &= a^{-1}(GV(CL(i), X'(i)) \oplus KL(i)) \\
X'(i - 1) \oplus X(i) &= DV(KR(i), a^{-1}(GV(CL(i), X'(i)) \oplus KL(i)) \\
X(i) &= DV(KR(i), a^{-1}(GV(CL(i), X'(i)) \oplus KL(i))) \oplus X'(i - 1)
\end{align*}
\]

**AXIS6: EXAMPLES AND SIMULATIONS**

In order to measure the performance of our encryption system, we randomly select a large number of reference images, and then use our method to test them

1) Brutal assaults

They consist in reconstructing the encryption keys in a random manner.

a) Key-space analysis

The chaotic sequence used in our method ensures strong sensitivity to initial conditions and can protect it from any brutal attacks. The secret key to our system consists of

- \( x_0 = 0.7655412001, \) \( \mu_1 = 3.89231541 \)
- \( y_0 = 0.865421331, \) \( \mu_2 = 0.563215 \)
- \( \mu_3 = 1.3561, \) \( \mu_4 = 0.563215 \)

If we use single-precision real numbers \( 10^{-10} \) to operate, the total size of the key will greatly exceed \( 2^{180} \gg 2^{110} \), which is enough to avoid any brutal attacks.

b) Secret key’s sensitivity Analysis

Our encryption key has a high sensitivity, which means that a small degradation of a single parameter used will automatically cause a large difference from the original image. The image below illustrates this confirmation
This ensures that in the absence of the real encryption key, the original image cannot be restored.

a) **Hystogram analysis**

all images tested by our algorithm have a uniformly distributed histogram. This reflects that the entropy of the encrypted images is around 8, which makes the system immune to histogram attacks. The table 1 shows that the horizontal correlation values of the encrypted images are close to zero. This ensures high security against correlation attacks.

Table 1: Encrypted image histogram

2) **Statistics Attack Security**

a) **Entropy Analysis**

Entropy is the measure of the disorder diffused by a source without memory. The entropy expression is determined by the equation below
\begin{equation}
H(MC) = \frac{1}{t} \sum_{i=1}^{t} -p(i) \log_2(p(i))
\end{equation}

The entropy values on the 150 images arbitrarily chosen from a large database of images of different sizes and formats, tested by our method are represented graphically by the following figure.

\textbf{Figure 12: Entropy of 150 images}

All the entropy values of the images tested by our algorithm are close to 8, which confirms the uniformity of the histogram. This proves that the method is far from a statistical attack.

\textbf{a) Entropy statistical analysis}

We will study the uniformity of the distribution of entropy released by the test.

\textbf{(a) Position parameter analysis}

The values derived from the entropy by applying our approach to over 150 images in our image database, constitute a statistical series with position, dispersion and concentration parameters have been recalculated to verify the safety of our approach.

The purpose of this analysis is to show that the distribution follows a reduced central normal distribution. So

\begin{equation}
\begin{cases}
Q_1 & = \text{First quartile} \\
Q_2 & = \text{Second quartile} \\
Q_3 & = \text{Third quartile}
\end{cases}
\end{equation}
Position Parameters

<table>
<thead>
<tr>
<th>Average</th>
<th>Max</th>
<th>Min</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
</tr>
</thead>
<tbody>
<tr>
<td>7,999480662</td>
<td>7,999993872</td>
<td>7,999004283</td>
<td>7,99921863</td>
<td>7,99946043</td>
<td>7,999737</td>
</tr>
</tbody>
</table>

The moustache box of the entropy is illustrated in the diagram in Figure below

![Entropy Moustache Box Diagram](image)

**Figure13: Entropy moustache box**

**a) Correlation analysis**

Correlation is a technique that compares two images to estimate the displacement of pixels in one image relative to another reference image. The relevant expression is defined by the following equation

\[
  r = \frac{\text{cov}(x, y)}{\sqrt{V(x)} \sqrt{V(y)}}
\]

**Equation 29**

(a) **Horizontal Correlation**

The following figure graphically represents the simulation of 150 color images of the same size, which are selected from an image database of various sizes, formats and related values.
Figure 15: Entropy of 150 images

(b) Vertical Correlation
Simulations made on 150 images of the database gave the vertical correlation scores are displayed in Figure below

Figure 16: Vertical correlation of 150 images

Figure 17 shows that the vertical correlation values of the encrypted images are close to zero. This ensures high security against correlation attacks.

(c) Diagonal Correlation
Simulations made on 150 images of the database gave the diagonal correlation scores are displayed in Figure below
Figure above shows that the diagonal correlation values of the encrypted images are close to zero. This ensures high security against correlation attacks.

**b) Differential analysis**

Let be two encrypted images, whose corresponding free-to-air images differ by only one pixel, from \( C_1 \) and \( C_2 \), respectively. The **NPCR** mathematical analysis of an image is given by the equation below

\[
NPCR = \left( \frac{1}{nm} \sum_{i,j=1}^{nm} D(i,j) \right) \times 100
\]

**With**

\[
D(i,j) = \begin{cases} 
1 & \text{if } C_1(i,j) \neq C_2(i,j) \\
0 & \text{if } C_1(i,j) = C_2(i,j)
\end{cases}
\]

The **UACI** mathematical analysis of an image is given by the below

\[
UACI = \left( \frac{1}{nm} \sum_{i,j=1}^{nm} \text{Abs}(C_1(i,j) - C_2(i,j)) \right) \times 100
\]

The study of the 150 selected images revealed the following diagram.
Figure 18: NPCR of 150 images

All detected values are inside the confidence interval [99.63, 99.95]. These values are largely sufficient to affirm that our crypto system is protected from known differential attacks.

The study of the 150 selected images revealed the following diagram.

Figure 19: UACI of 150 images

All detected values are inside the confidence interval [33; 34, 33,35]. These values are largely sufficient to affirm that our crypto system is protected from known differential attacks.

a) Avalanche effect

The avalanche effect is a required property in virtually all cryptographic hash functions and block coding algorithms. It causes progressively more important changes as the data is propagating in the structure of the algorithm. This constant determines the avalanche impact of the cryptographic structure in place. It is approximated by the equation below.
\[ AE = \left( \frac{\sum_{i \text{ bit change}}}{\sum_{i \text{ bit total}}} \right) \times 100 \]

Figure below depicts the evaluation of the AE score for 150 images examined by our approach.

All values returned from the (AE) by our method are all in the range of residual values [73,96 74;02]. This guarantees that a one-bit change in the clear image will be reflected by a change of at least 78% of the encrypted image’s bits.

\textit{b) Signal-To-Peak Noise Ratio (PSNR)}

\textit{(a) MSE}

The image quality estimation to be based on the pixel change was obtained by processing the (PSNR) values and the (MSE). It is calculated by the following equation

\[ MSE = \sum_{i,j} (P(i,j) - C(i,j))^2 \]

\((P(i,j))\): pixel of the clear image
\((C(i,j))\): pixel of the cypher image

\textit{(b) PSNR}

The signal-to-peak noise ratio, often abbreviated PSNR, is an engineering term for the ratio between a signal’s maximum possible power and the power of distorted noise that affects the precision of its display. The PSNR mathematical analysis of an image is given by the next equation

\[ PSNR = 20 \log_{10} \left( \frac{I_{\text{max}}}{\sqrt{MSE}} \right) \]

For RGB color images, the definition of PSNR is the same except that the MSE is the sum of all square value changes. In the alternative, for color images, the image is transcoded
into a separate color space and the PSNR is displayed for each channel in that color space.

![PSNR graph](image)

**figure21: PSNR of 150 images**

All values returned from the PSNR by our method are all in the range of residual values [8.99, 8.993].

**a) Speed analysis**

For an evaluation of the execution time, our algorithm is tested on a personal computer "Intel core i5 3337 U 1.86 Gz CPU 8 GB ram. We use Matlab as programming software. We measure the encryption and decryption time of the tested images.

![Time graph](image)

**figure22: time of 300 images**

4) Math Security

The first round eliminates any correlations and protects the system from differential attacks. Not knowing the size of the encryption matrix will increase the complexity of the attack. Without knowing the encryption key, it is difficult to replicate the structure of this matrix.
IV. CONCLUSION

The first encryption stage is provided by the deep enhancement of Vigenere’s classic system, which can protect our new algorithm from any differential attack, while the second stage uses dynamic affine transformation, which consists of a large invertible matrix of uncertain size. Provide without knowing the secret encryption keys, are difficult to construct from Kronecker’s products, making the system resistant to any known attacks. The system only uses the replacement, which greatly reduces the execution time.

Conflict of Interest

I am the sole author of this article, and there are no private or public organizations or laboratories to fund my research, thus avoiding any expected conflicts.

This document does not contain any research or experiments conducted on animals.

References

[16] Mohamed JarJar “Further improvement of the HILL method applied in image encryption” Procedia computer sciences 00(2019)000-000
[20] Liu H « Color image encryption based on one time keys and robust chaotics maps” Computer and mathematic application 59(2010),3320-3327