Journal of Multimedia Information System VOL. 8, NO. 1, March 2021 (pp. 45-56): ISSN 2383-7632 (Online)
http://doi.org/10.33851/JMIS.2021.8.1.45

Development of Standard Hill Technology for Image Encryption over a 256-element Body

Abdellatif JarJar[1*]

Abstract

This document traces the new technologies development based on a deep classical Hill method improvement. Based on the chaos, this improvement begins with the 256 element body construction, which is to replace the classic ring used by all encryption systems. In order to facilitate the application of algebraic operators on the pixels, two substitution tables will be created, the first represents the discrete logarithm, while the second represents the discrete exponential. At the same time, a large invertible matrix whose structure will be explained in detail will be the subject of the advanced classical Hill technique improvement. To eliminate any linearity, this matrix will be accompanied by dynamic vectors to install an affine transformation. The simulation of a large number of images of different sizes and formats checked by our algorithm ensures the robustness of our method.

Key Words: Chaotic map, 256-Bady, Discrete exponential, Discrete logarithm

I. INTRODUCTION

The operation of digital data and its transmission through the network are uncertain operations and are vulnerable to various attacks, cryptography is becoming the most effective means for data security. In the literature, almost all classical methods are still vulnerable to statistical and differential attacks.

2.1. Conventional Hill technique

This technique, discovered by HILL [1], [2] in 1929, was only applicable to the text. It is based on two main steps. The first step is to divide the message to be encrypted into n character (natural number) blocks, and the second step is in a carefully selected ring as $usually\ Z/26Z\ or\ Z/256Z$) The difficulty of constructing a large invertible matrix prompts researcher to only Use a matrix with $n \geq 4$. Equation 1 fully describes this standard technique

$$\{C_i' = KC_i\}\ \forall\, i \geq 1. \qquad (1)$$

With$(C_i)$is the clear block, $(\boldsymbol{C_i'})$is the encrypted block, and (K) is the encryption key. Each $(\boldsymbol{C_i})$ block is translated to an element of a well selected (G_t) ring. In such a case, the encryption matrix (K) is assigned coefficients in the same ring $(\boldsymbol{G_t})$. Due to the high degree of linearity, this technique is always exposed to selected plain text and known statistical attacks. On the other hand, the high correlation between adjacent pixels and diagonal pixels of the image makes this technique unsuitable for image encryption. Finally, there is no chain in the encryption system, so this method is vulnerable to differential attacks. The decryption operation is described by next equation.

$$\{C_i = K^{-1}C_i'\}\ \ \forall\, i \geq 1. \qquad (2)$$

2.2. Hill's classic method survey

Several successive developments in the methodology have taken place over time, but all using a reference ring such as $(\boldsymbol{G_{256}})$ or$(\boldsymbol{G_{26}})$ which significantly reduces the number of invertible matrixes and increases the risk of brutal attacks.

A first improvement [3-4-5] consists in modifying at each iteration; the encryption matrix by a secret permutation

Manuscript received January 02, 2021; Revised March 04, 2021; Accepted March 22, 2021. (ID No. JMIS-21M-01-001)

Corresponding Author (*): Abdellatif JarJar, Moulay Rachid High School, Taza Morocco, abdoujjar@gmail.com
[1]Moulay Rachid High School, Taza Morocco, abdoujjar@gmail.com

$(\boldsymbol{h})$ and fixed in the ring $(\boldsymbol{G_{256}})$, on the rows or on the columns. This improvement is given by the equation 3

$$\begin{cases} C_1' = K_1 C_1 \\ C_i' = h(K_{i-1})C_i \quad \forall\, i \geq 2, \end{cases} \tag{3}$$

where $\boldsymbol{h}\,(\boldsymbol{K_{i-1}})$ is the transform of the matrix $(\boldsymbol{K_{i-1}})$by fixed permutation $(\boldsymbol{h})$. Other improvements accompany the static encryption matrix of a translation vector$(\boldsymbol{T})$, and this to overcome the problem of uniform blocks $[6-7]$ and null blocks, still others modify the translation vector at each iteration by a linear transformation provided by a fixed matrix $(\boldsymbol{Q})$ of size $(\boldsymbol{n},\boldsymbol{n}\ )$, not necessarily inversible. This method is described by equation4.

$$\begin{cases} C_1' = KC_1 \oplus T_1, \\ T_i = QT_{i-1} With \quad i \geq 2\,, \\ C_{i+1}' = KC_i \oplus T_i \quad \forall\, i \geq 1. \end{cases} \tag{4}$$

These improvements overcome statistical attacks and selected text attacks, but due to the lack of clear links between the original pixels, encrypted pixels, and encryption keys, they are still vulnerable to differential attacks. However, unless there is a strong correlation between the adjacent pixels of the image and the diagonal, all these methods are still powerless. Recently, the algorithm based on the classic chaotic method has exploded, and the chaotic suite $[8-9]$ has been created to increase the key space, thereby protecting the method from brutal attacks. Unfortunately, due to the difficulty of calculating the inverse of higher-order matrices, these methods still use general non-invertible matrices with $n > 4$ [10], [11], which poses complexity problems. So far, all encryption algorithms have considered the pixel values of the image in ring $\boldsymbol{G_{256}}$, and the number of invertible matrices of size (n, n) with coefficient $\boldsymbol{G_{256}}$ is given by the following formula [12], [13].

2.3. Our contribution

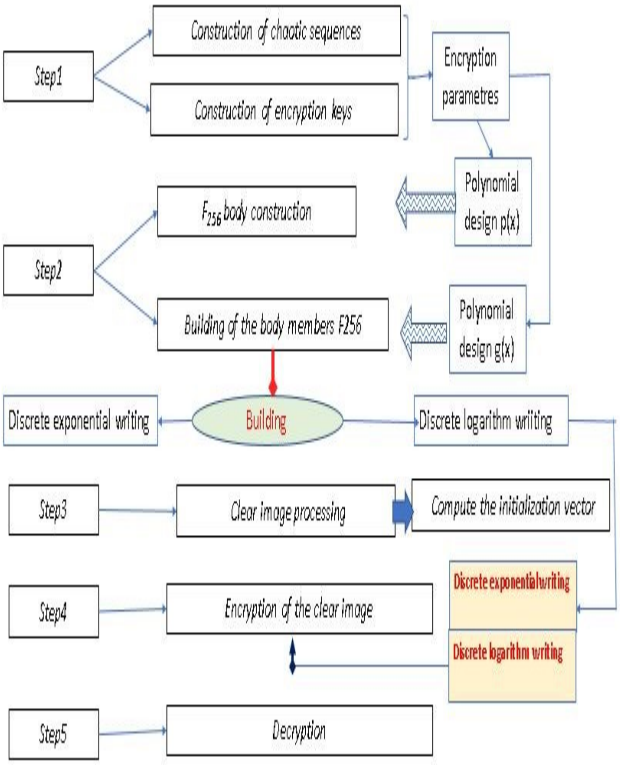
Faced with the great difficulty of inverting in large-size matrices, the researchers were content to handle matrices of sizes generally less than five, in the classic ring $(\boldsymbol{G_{256}})$ To correct this anomaly, our contribution provides a convincing solution by treating all pixel values as elements of one of the constructed subjects. Working in the body greatly increases the number of invertible matrices and provides protection. To facilitate algebraic calculations, two chaos tables will be generated.

- Discrete logarithmic table
- Discrete exponential table

Moreover, taking advantage of the properties of the involuntary matrices, a new technique for constructing invertible matrices of random size will be determined.

II. THE PROPOSED METHOD

This new technology that works at the pixel level is explained in the following aspects, and its value is regarded as an element of the built company.



Step1
Construction of chaotic sequences
Construction of encryption keys
Encryption parametres
Polynomial design p(x)
Step2
F256 body construction
Building of the body members F256
Polynomial design g(x)
Discrete exponential writing
Building
Discrete logarithm writing
Step3
Clear image processing
Compute the initialization vector
Discrete exponentialwriting
Step4
Encryption of the clear image
Discrete logarithm writing
Step5
Decryption

Fig. 1. Steps of realization of the algorithm.

Finally, a detailed analysis of our methodology performance will be discussed and compared with other reference systems.

Step 1: Chaotic sequences Development

Our algorithm uses two of the most famous and widely used chaotic maps in cryptography.

(1) The Logistics' Map

Due to its high sensitivity to initial conditions, chaos is largely utilized symmetric cryptography for the construction of cipher keys [14], [15], [16].

$$\begin{cases} u_0 \in \,]0{,}5 \quad 1[\quad , \quad \mu \in [3{,}75 \quad 4], \\ u_{n+1} = \mu u_n(1-u_n). \end{cases} \tag{5}$$

(2) HENON'S Map

Henon's chaotic two-dimensional map was first discovered in 1978. It is described by equation below.

$$\begin{cases} v_0 \ , w_0 \ a = 0.3 \ , b \in [1.07 \quad 1.4] \\ \quad v_{n+1} = 1 + w_n - a v_n^2 \\ \quad w_{n+1} = b v_n \end{cases} \qquad (6)$$

We can convert the two-dimensional map expression to a one-dimensional map that is easy to implement in the encryption system. This formula is described by next equation.

$$\begin{cases} v_0 \ , v_1 \ in\ [0 \ \ 1]\ a \ = 0.3, b \in [1.07 - 1.4] \\ \qquad v_{n+2} = 1 - a v_{n+1}^2 + b v_n \end{cases} \qquad (7)$$

(3) Chaotic used vector design

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

$$Alg2 \begin{cases} for \ \ i = 1 \ to \ 3nm \\ CL(i) = \ mod\left(E\left(\frac{u(i) + 2v(i)}{3} * 10^{11}, 254\right) + 1\right) \\ KL(i) = \ mod\left(E\left(\frac{w(i) + u(i) + v(i)}{3} * 10^{11}, 253\right) + 2\right) \\ KR(i) = E\left(\frac{KL(i) + CL(i)}{2}\right) \\ if \ u(i) \geq \frac{v(i) + w(i)}{2} \ then \\ CR(i) = 0 \ else \ CR(i) = 1 \\ end \ if \\ Next \ i \end{cases}$$

We note that

$$\forall \ i \in [\![1 \ \ 3nm]\!] \begin{cases} CL(i) \not\approx 0 \\ KL(i) \not\approx 0 \\ KR(i) \not\approx 0 \end{cases}$$

These elements are all non-zero; as a result, they are invertible within the built body.

Step 2: $\mathrm{F_{256}}$ Body Construction

The most important step is to create an entity with 256 $elements$, which will replace the classical (G_{256}) in the calculation.

(1) Mathematical overview

For it

$$\text{Let} \qquad F_{256} = \left\{h(x) \in \tfrac{F[x]}{d} \circ h \leq 7\right\}$$

Let $\boldsymbol{p(x)}$ eighth-order polynomial and irreducible in $\boldsymbol{F[x]}$. We define two internal composition laws described by the following formula on such a set.

$$\begin{cases} \quad First \ Internal \ Composition \ Law \\ h(x) \oplus k(x) = \big(h(x) + k(x)\big) \ modulo \ 2, \\ \quad Second \ Internal \ Composition \ Law \\ h(x) \otimes k(x) = \big(h(x)k(x)\big) \ modulo \ \boldsymbol{p(x)}. \end{cases} \qquad (8)$$

It is easy to prove that these two internal composition laws provide the $(\boldsymbol{F_{256}},\oplus; \otimes)$with a commutative finite body structure with 256 elements.

(2) $\boldsymbol{F_{256}}$ Elements Representation

Any element of the $\boldsymbol{F_{256}}$ body can be represented in five different forms:

a) Polynomial Writing

We know that

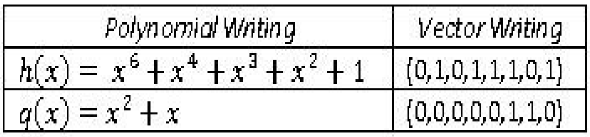
$$F_{256} = \left\{h(x) \in \tfrac{F[x]}{d} \circ h \leq 7\right\}. \qquad (9)$$

Consequently, any element can be written in the form of a polynomial of degree at most equal to 7 with (G_2) components. For example:

$$\boldsymbol{h(x) = \ x^6 + x^4 + x^3 + x^2 + 1\ , \ \ q(x) = x^2 + x}$$

b) Vector Writing

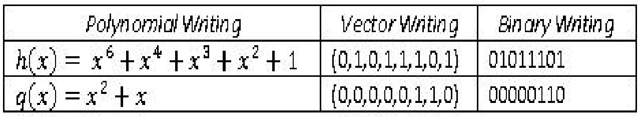
Any element of the body F_{256} can be represented as a size vector $(\boldsymbol{1, 8})$ with a coefficient in $(\boldsymbol{G_2})$



Polynomial Writing	Vector Writing
$h(x) = x^6 + x^4 + x^3 + x^2 + 1$	(0,1,0,1,1,1,0,1)
$q(x) = x^2 + x$	(0,0,0,0,0,1,1,0)

c) Binary Writing

By simple conversion from vector writing to binary writing, any element of such a subject can be written in binary form

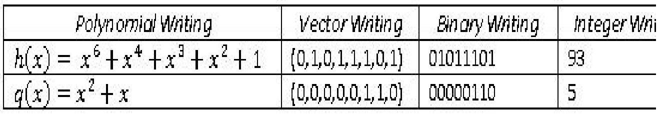


Polynomial Writing	Vector Writing	Binary Writing
$h(x) = x^6 + x^4 + x^3 + x^2 + 1$	{0,1,0,1,1,1,0,1}	01011101
$q(x) = x^2 + x$	{0,0,0,0,0,1,1,0}	00000110

d) Integers Writing

All body elements are displayed in 8 bits, consequently their value is located between 0 and 255. So, we have

$$\boldsymbol{F_{256}} = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \dots, \mathbf{255}\}$$



Polynomial Writing	Vector Writing	Binary Writing	Integer Wri
$h(x) = x^6 + x^4 + x^3 + x^2 + 1$	{0,1,0,1,1,1,0,1}	01011101	93
$q(x) = x^2 + x$	{0,0,0,0,0,1,1,0}	00000110	5

This notation can be extended to the coefficient matrix in $\boldsymbol{F_{256}}$. For example:

$$M = \begin{pmatrix} x^2 + x + 1 & x \\ x^3 + x^2 & x^6 + x^4 + 1 \end{pmatrix} \Rightarrow M = \begin{pmatrix} 7 & 2 \\ 12 & 81 \end{pmatrix}$$

e) Discrete Exponential Writing

Note that, $(\boldsymbol{F_{256}}, \oplus; \otimes)$ is a finite body, consequently, the set $(F_{256}^*, \otimes)$ is a cyclic group. As a result, it is generated by a single element $g(x)$ closely related to the constructor polynomial $p(x)$. This can be illustrated by the following formula:

$$F_{256}^* = \{h(x) \in F[x] \ \ that\ d\,°h \leq 7\,, and\ \ h(x) \neq 0\}$$
$$= F_{256} - \{0\}$$
$$\begin{cases} \forall h \in F_{256}^* \exists!\, i \in [0 \quad 254] : \ h(x) = g(x)^i \ mod\ (p(x)), \\ \qquad by\ convention \qquad g(x)^{255} = 0, \end{cases} \tag{9}$$

where i is called the exponential notation of the polynomial $h\ (x)$.

$$We\ note\ that \qquad ;\ Exp(i) = h(x)$$

We confirm that the change of the generator $g(x)$ will lead to a fundamental change in the sign of the exponent, which will result in serious distortion of the entire encryption system.

f) Discrete logarithm Writing

Function (Exp) is bijective, and its inverse function is the function defined by the following formula (Log):

$$Al3 \begin{cases} \quad for\ \ i = 0 \quad to \quad 254 \\ \quad Log\big(Exp(i)\big) = i \\ \qquad Next \quad i \\ by\ convention \ \ Log(0) = 255 \end{cases}$$

This rating will greatly facilitate algebraic calculations

(3) Algebraic operations over $\boldsymbol{F_{256}}$

The two algebraic operations will be defined from the two tables constructed to facilitate the calculations.

a) The multiplication

To facilitate the multiplication of $\boldsymbol{F_{256}}$ elements, it is recommended to use the two notations $(Exp)\ and\ (Log)$. This technique is clarified by the equation below:

$$g(x)^i \otimes g(x)^j = \begin{cases} 0 \quad if \quad i = 255 \ \ or \ \ j = 255, \\ \qquad else \\ \ g(x)^{[mod(i+j, \quad 255)]}. \end{cases} \tag{10}$$

So, we can deduce the equation below

$$\Big\{ x_i \otimes x_j = \begin{cases} 0 \ \ if \quad x_i = 0 \ \ or \ \ x_j = 0 \\ Exp(mod(Log(x_i) + Log(xj), 256)) \end{cases} \tag{11}$$

Please note that multiplication is closely related to the choice of generator $g(x)$

b) $\mathrm{F_{256}}$ Inverse of elements

The calculation of the inverse of the elements of the basic set is very important and very useful in the decryption process.

i. Inverse for addition

We know that

$$\forall x \in F_{256} \quad x \oplus x = 0. \tag{12}$$

ii. Inverse for multiplication

$$\forall\, x \in \ F_{256}^* \quad x^{-1} = Exp\big(255 - Log(x)\big). \tag{13}$$

Note that any non-zero element is invertible in $\boldsymbol{F_{256}}$.

(4) Matrix analysis in body $\boldsymbol{F_{256}}$

Every matrix used in this system are all in coefficients in $\boldsymbol{F_{256}}$

a) Image of a vector by a matrix (3,3)

The multiplication of a size matrix $(3, 3)$ and a size vector $(1,3)$ is determined by the following formula below

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \\ \delta \end{pmatrix} = \begin{pmatrix} a \otimes \alpha \oplus b \otimes \beta \oplus c \otimes \delta \\ d \otimes \alpha \oplus e \otimes \beta \oplus f \otimes \delta \\ g \otimes \alpha \oplus h \otimes \beta \oplus i \otimes \delta \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \\ \delta \end{pmatrix} = \begin{pmatrix} a \otimes \alpha \oplus b \otimes \beta \oplus c \otimes \delta \\ d \otimes \alpha \oplus e \otimes \beta \oplus f \otimes \delta \\ g \otimes \alpha \oplus h \otimes \beta \oplus i \otimes \delta \end{pmatrix}. \qquad (14)$$

b) Second order determinant

The determinant of a second order matrix is defined by the equation below.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = a \otimes d \oplus c \otimes b, \qquad (15)$$

$$So\ \ The\ matix\ A\ of\ size\ (l, l)\ is\ inversible\ \Leftrightarrow\ det(A) \not\approx 0.$$

This greatly increases the number of invertible matrices. We know that the number of invertible size matrix (p, p) in $\boldsymbol{F_{256}}$ is:

$$\delta = \prod_{i=1}^{p-1} (2^p - 2^i) \gg 2^{100}. \qquad (16)$$

This proves that the brutal attacks on the matrices in $\boldsymbol{F_{256}}$ of higher order are remote.

III. INSTALL THE NEW CRYPTOSYSTEM

Throughout the document, the pixel intensity values of the color image pixels will be considered as elements of $\boldsymbol{F_{256}}$. Our method is articulated on the following points.

(1) Original image Vectorization

After extraction of the three color channels (RGB) and their conversion into vectors $(Vr), (Vg), (Vb)$, a cohabitation is carried to form the vector $\boldsymbol{X(x_1, x_2, \dots\dots, x_{3nm})}$. To apply Hill's new method, the vector (X) must be cut into blocks of the size of $(\boldsymbol{r_h})$ calculated from the chaotic map and the original image size.

(2) $(\mathrm{r_h})$ value Determination

$$\boldsymbol{r_h} = \left(mod \left(E \left(10^{10} \left(\frac{1}{nm} \sum_{i=2}^{nm} \frac{u(i) + \sup(w(i), v(i))}{2} \right) \right), 6 \right) + 15 \right). \qquad (17)$$

So, we can conduct as:

$$15 \le \boldsymbol{r_h} \le 20. \qquad (18)$$

(3) Size vector image Adaptation

In order to implement the new technology, we need to cut the image vector (X) into large and small blocks $(2\boldsymbol{r_h})$. This operation follows the following formula:

$$\begin{cases} \text{let} \quad 3nm \equiv s\ [2\boldsymbol{r_h}] \\ l = 3nm - s \\ t = \frac{l}{2r_h} \end{cases}, \qquad (19)$$

The vector (X) must be imputed by (s) pixels by the following method:

$$AlG8 \begin{cases} for \quad i = 1\ \ to\ \ l \\ XT(i) = X(i) \\ Next\ i \end{cases}$$

$$If\ s \neq 0, then \begin{cases} Amputated\ pixel\ storage \\ for\ i = 1\ \ to\ \ s \\ if\ CR(i + l) = 0\ then \\ XD(i) = X(i + l) \oplus CL(i + l) \\ else \\ XD(i) = X(i + l) \oplus KL(i + l) \\ end\ if \\ Next\ \ i \\ end\ if \end{cases}. \qquad (20)$$

We noticed that this decomposition is completely controlled by the decision vector (CR)

(4) $(\mathbf{2r_h})$-Bit Blocks Decomposition

In parallel, convert two chaotic vectors (KR) and (KL) into matrices (MR) and (ML) of size $(t, \boldsymbol{2r_h})$ following Fig. 2. After adjusting the size of the image vector, convert the latter to a matrix (MC) of size $(t, \boldsymbol{2r_h})$ as shown in Fig. 3.

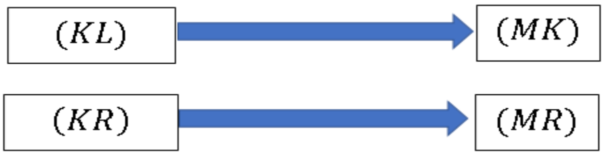


Fig. 2. Converting two chaotic vectors.

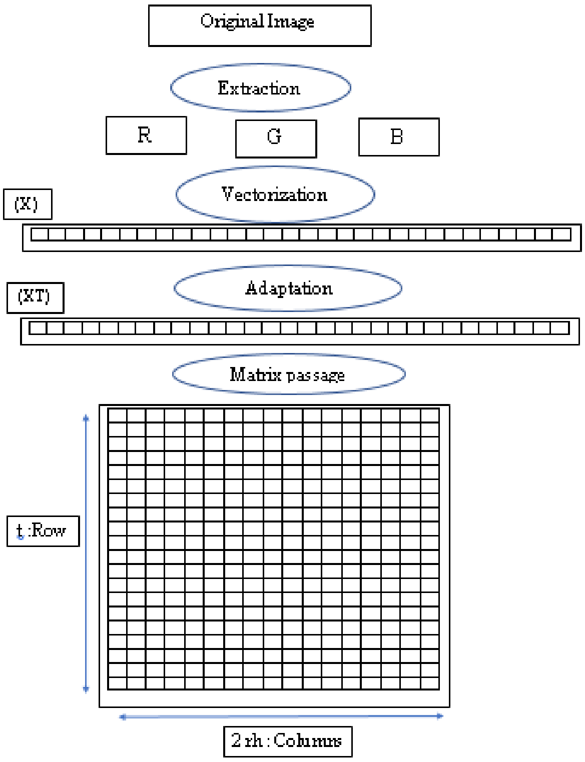


Fig. 3. Image vector decomposition.

(5) Initialization Vector Design

First, the(VI) initialization vector of size $(1, \boldsymbol{2r_h})$ must be recalculated to change the value of the starting block. Ultimately, the $(\boldsymbol{VI})$ value is provided by the next algorithm

$$Alg9\left\{\begin{array}{c} for\ \ i=2\ to\ t \\ VI(i)=0 \\ for\ j=2\ to\ \boldsymbol{2r_h} \\ VI(i)=VI(i)\oplus\ MC(i,j) \\ Next\ j,i \end{array}\right.$$

To surpass the uniform image problem $(Black, White\ \ldots)$ the setup value (VI) will be combined with the chaotic vector (TT) specified by the following algorithm.

$$Alg10\left\{\begin{array}{c} for\ \ i=1\ to\ \boldsymbol{2r_h} \\ VI(i)=VI(i)\oplus\ CL(i) \\ Next\ i \end{array}\right.$$

The value calculated from the clear image and the chaotic map, will only be used to change the value of the start pixel and restart the encryption process.

$$Alg11\left\{\begin{array}{c} for\ \ i=1\ to\ \boldsymbol{2r_h} \\ CM(1,i)=CM(1,i)\oplus VI(i) \\ Next\ i \end{array}\right.$$

IV. NEW IMPROVEMENT CLASSICAL HILL TECHNIQUE

The difficulty of reversing large matrices forces researchers to use matrices with sizes generally less than 5. However, due to linearity, classical HILL methods are still subject to statistical attacks. Our algorithm overcomes this anomaly by constructing an arbitrarily large invertible matrix, accompanied by chaotic vectors generated from the chaotic map used under binary chaotic vector control.

4.1. Encryption matrix construction

According to our technical steps, it will be easier to construct a large invertible matrix based on involute blocks and non-empty eigenvalue matrices

4.4.1 Involutive matrix

A is an involutive matrix if and only if we have

$$A=\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}\ A_i\ of\ size\ (\boldsymbol{r_h},\boldsymbol{r_h})\ \ with\ (r)\ \in G_{256}^*$$

We got

$$A^2=\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}\begin{pmatrix}A_1 & A_2\\ A_3 & A_4\end{pmatrix}$$

$$=\begin{pmatrix}A_1^2\oplus A_3A_2 & A_2A_1\oplus A_4A_2\\ A_1A_3\oplus A_3A_4 & A_4^2\oplus A_2A_3\end{pmatrix}=\begin{pmatrix}I & 0\\ 0 & I\end{pmatrix}. \quad (21)$$

$$I\text{: }Identity\ Matrix$$

Since matrix A is involutive, we get

$$\left\{\begin{array}{c} A_1^2\oplus A_2A_3=I, \\ A_2A_1\oplus A_4A_2=0, \\ A_1A_3\oplus A_3A_4=0, \\ A_4^2\oplus A_2A_3=I. \end{array}\right. \quad (22)$$

So,

$$\left\{\begin{array}{l} A_2A_3=I-A_1^2=(I\oplus A_1)(I\oplus A_1), \\ A_2A_3=I-A_4^2=(I\oplus A_4)(I\oplus A_4). \end{array}\right. \quad (23)$$

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

$$\left\{\begin{array}{c} A_2=k(I\oplus A_1), \\ A_3=k^{-1}(I\oplus A_1), \\ (k\in F_{256}^*) \\ k^{-1}=Exp\big(255-\ Log(k)\big), \\ A_4=-A_{1=}A_1, \\ A_1\neq 0\ and\ A_1\neq I. \end{array}\right. \quad (24)$$

Or we can take as:

$$\begin{cases} A_2 = k(I\oplus A_1), \\ A_3 = k^{-1}(I\oplus A_1), \\ A_4 = -A_1 = A_1, \\ So\ \ A = \begin{pmatrix} A_1 & k\otimes(I\oplus A_1) \\ k^{-1}\otimes(I\oplus A_1) & A_1 \end{pmatrix}. \end{cases} \qquad (25)$$

4.1.2. D matrix building

The eigenvalue(D) matrix has the form as:

$$D = \begin{pmatrix} e_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e_{2r_h} \end{pmatrix} \forall\, i \in [\![1\ \ r]\!]\ \ e_i \in F^*_{256}. \quad (26)$$

The number of matrices (D) is much higher than 2^{16r_h}.

Finally, the new Hill matrix will have the following form

$$\mathrm{H} = \mathrm{A}\otimes\mathrm{D}\otimes\mathrm{A}. \qquad (27)$$

$$X' = \Big(\big(H\otimes(X)\big)\oplus MK\Big)\otimes MR. \qquad (28)$$

V. ORIGINAL IMAGE ENCRYPTION

After preparing the original image and constructing all the parameters, the following figure will explain the encryption process in detail.

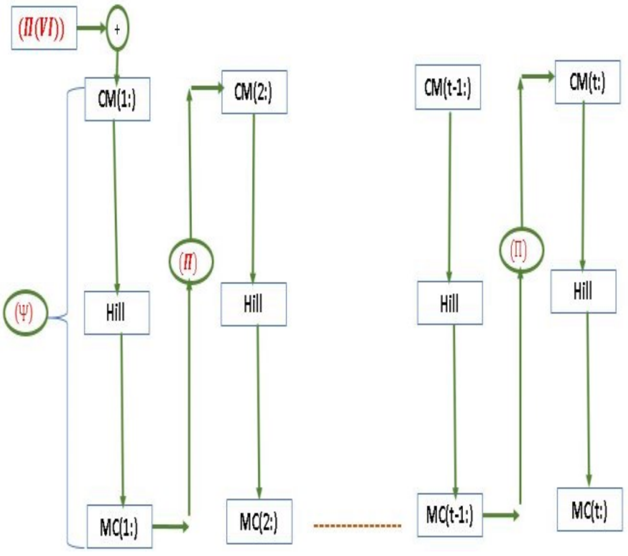


Fig. 4. Clear image encryption.

(Π) Spread function, used to increase the impact of avalanche effects and protect the system from any difference. It is defined by the following formula:

$$\Pi(CM(i+1:)) = MC(i:)\oplus CM(i+1:). \qquad (29)$$

VI. DECRYPTING THE ENCRYPTED IMAGE

Our technique is a symmetric encryption system using a spread function, which forces us to start the decryption process from the last block to the first block, and then recalculate the initialization vector to extract the exact value of the first block. The figure below illustrates the decryption process

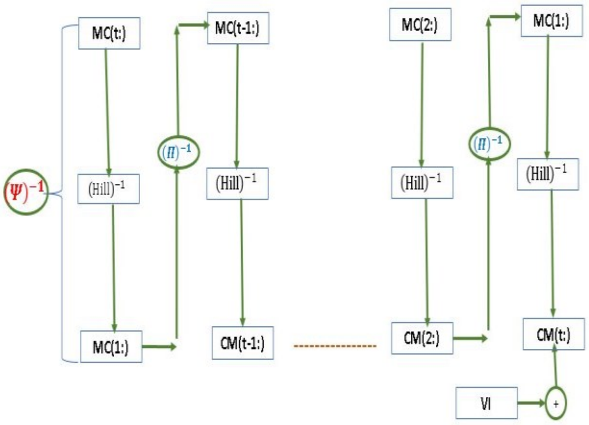


Fig. 5. Decryption process.

A decryption function can be described as:

$$\begin{cases} \boldsymbol{Improved\ Hill\ inverse\ function} \\ X' = \Big(\big(H\otimes(X)\big)\oplus MK\Big)\otimes MR \\ \boldsymbol{X}'\otimes Exp(255 - Log(MR) = \Big(\big(H\otimes(X)\big)\oplus MK\Big) \\ (\boldsymbol{X}'\otimes Exp(255 - Log(MR)\oplus MK) = H\otimes(X) \\ (X) = H^{-1}\Big((\boldsymbol{X}'\otimes Exp(255 - Log(MR)\oplus MK)\Big) \end{cases}$$

$$\begin{cases} \boldsymbol{Reverse\ diffusion} \\ \boldsymbol{We\ have}\ \boldsymbol{CM}(i+1:) = \Pi\big(MC(i:)\big)\oplus CM(i+1:) \\ \boldsymbol{MC(i:)} = \ \Pi^{-\mathbf{1}}\big(CM(i+1:)\oplus CM(i+1:)\big) \end{cases}$$

VII. Simulation Result

The polynomial $\mathrm{p(x) = x^8 + x^7 + x^2 + x + 1}$ is irreducible and eighth order on $F\,[x]$, so it is a candidate for this study in the construction of the simulation body $\boldsymbol{F_{256}}$. In addition, the polynomial $g(x) = x$ is a generator of such agents. Under these conditions, the $(\boldsymbol{TS})$ dispersion index table is shown below.

Table 1. Discrete exponential table.

(TS)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	4	8	16	32	64	128	135	137	149	173	221	61	122	244
1	111	222	59	118	236	95	190	251	113	226	67	134	139	145	165	205
2	29	58	116	232	87	174	219	49	98	196	15	30	60	120	240	103
3	206	27	54	108	216	55	110	220	63	126	252	127	254	123	246	107
4	214	43	86	172	223	57	114	228	79	158	187	241	101	202	19	38
5	152	183	233	85	170	211	33	66	132	143	153	181	237	93	186	243
6	76	97	194	3	6	12	24	48	96	192	7	14	28	56	112	224
7	142	155	177	229	77	154	179	225	69	138	147	161	197	13	26	52
8	71	104	208	39	78	156	191	249	117	234	83	166	203	17	34	68
9	151	169	213	45	90	180	239	89	178	227	65	130	131	129	133	141
10	136	157	189	253	125	250	115	230	75	150	171	209	37	74	148	175
11	53	106	212	47	94	188	255	121	242	99	198	11	22	44	88	176
12	217	231	73	146	163	193	5	10	20	40	80	160	199	9	18	36
13	144	167	201	21	42	84	168	215	41	82	164	207	25	50	100	200
14	72	23	46	92	184	247	105	210	35	70	140	159	185	245	109	218
15	51	102	204	31	62	124	248	119	238	91	182	235	81	162	195	255

Example:

$$TS(10{,}3) = Exp(163) = 253.$$

So

$$Log(253) = 163$$

By applying inverse permutation, a table of discrete logarithms can be derived from a table of discrete exponents. The two tables are used mutually in the field (F_{256}).

$$152^{-1} = \; Exp\left(255 - Log\;(152)\right) = \\ Exp\;(255 - 80)\;\; = Exp(174) = 179.$$

So

$$\left\{ \begin{array}{c} 183 \otimes 250 = \\ Exp(mod(L\,og(152) + L\,og(250)\,, 255)) \\ = Exp(80 + 163) = Exp(243) = 31 \end{array} \right.$$

In matrix notation,

$$M = \begin{pmatrix} x^2 + x + 1 & x \\ x^3 + x^2 & x^6 + x^4 + 1 \end{pmatrix} \Rightarrow M \\ = \begin{pmatrix} 7 & 2 \\ 12 & 81 \end{pmatrix}.$$

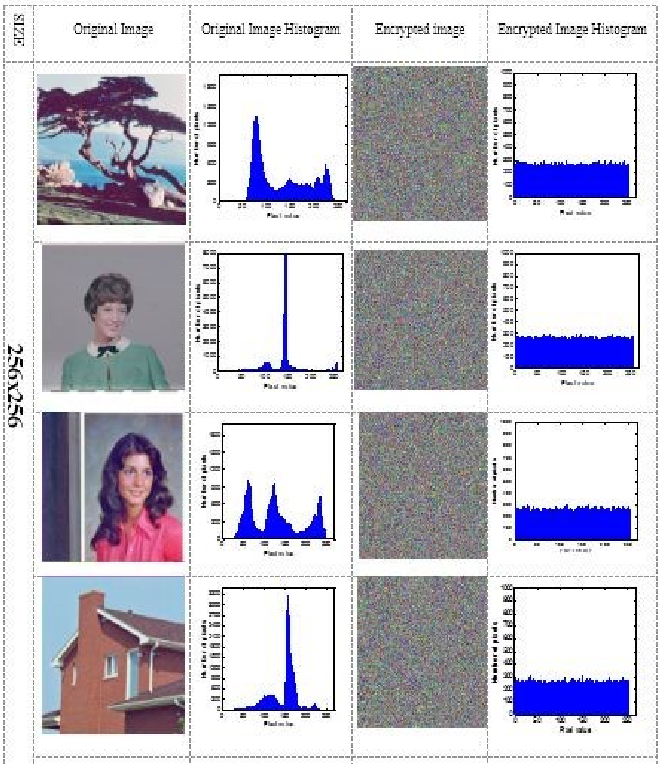
So

$$Exp(M) = \begin{pmatrix} 123 & 4 \\ 211 & 183 \end{pmatrix}, \\ and \\ Log(M) = \begin{pmatrix} 106 & 1 \\ 101 & 251 \end{pmatrix}.$$

VIII. INVESTIGATION OF CRYPTO SYSTEM PERFORMANCE

In this section, all the experiments were performed on a large color image database and using a *core i*7 personal computer, 16*Gb* memory, 500 *Gb* hard disk under the *matlab* software running under *windows* 7. Some of the most used reference images in cryptography and tested by our approach.

Table 2. Images encrypted by our approach.


SIZE
Original Image
Original Image Histogram
Encrypted image
Encrypted Image Histogram
256x256

1) Key-space analysis

In our example simulation we took as encryption key

$$u_0 = 0{,}7655412001\;\;, \mu = 3.89231541, \\ \textit{for logistic map,} \\ v_0 = 0.865421331, v_1 = 0{,}563215, b = 1{,}3561 \\ \textit{for Henon map}$$

$$\boldsymbol{The\ global\ Key\ space} \;\approx \mathbf{2^{180}} \gg \mathbf{2^{100}}.$$

2) Secret key's sensitivity Analysis

The high sensitivity of the encryption keys used in our system indicates that a very slight degradation of the encryption key automatically leads to an image that is so different from the original image. This confirmation can be viewed below the scheme in the next figure:

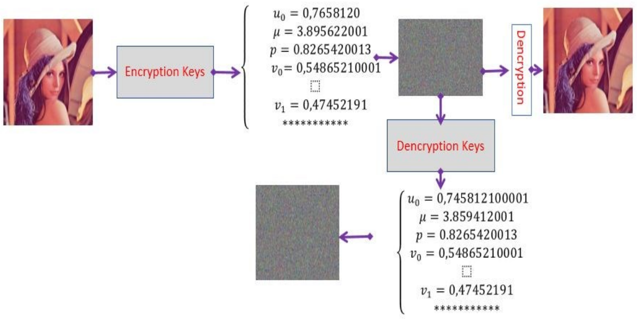


Fig. 6. Secret key's sensitivity.

We note that a 10^{-15} change in a single encryption parameter of this technology is incapable of restoring the clear image by the same decryption process.

2) Strength analysis of the new generation

Our design has given a new opportunity to survive and to partner with the strongest members in the hope of rebuilding a new population more adapted to intruder aggression. To do that, we randomly selected an image and studied the strength of the original populations and the new generation, with the following results:

3) Statistics attack security

a) Histogram analysis

The histogram gives the distribution of the pixel intensity level of any original image passed under our algorithm, showing the concentration near certain intensity values and sometimes the maximum value, while the histograms of all encrypted images are uniformly distributed Yes, this eliminates any statistical histogram attacks.

b) Entropy Analysis

Entropy information is very important in measuring the randomness of the encrypted image. It is defined by the following equation: (MC) image of size (n, m), we pose$(t = nm)$, so

$$H(MC) = \frac{1}{t}\sum_{i=1}^{t} -p(i)\, log_2(p(i)), \qquad (29)$$

where $p(i)$ is the probability of occurrence of level (i) in the image of the selected database. If $H(MC)$ is close to the value 8 ($8 - bit\ coded\ image$), the completely random aspect of the encrypted image is ensured. The following table illustrates the entropy of some reference images tested by our method:

Table 3. Encrypted image histogram.

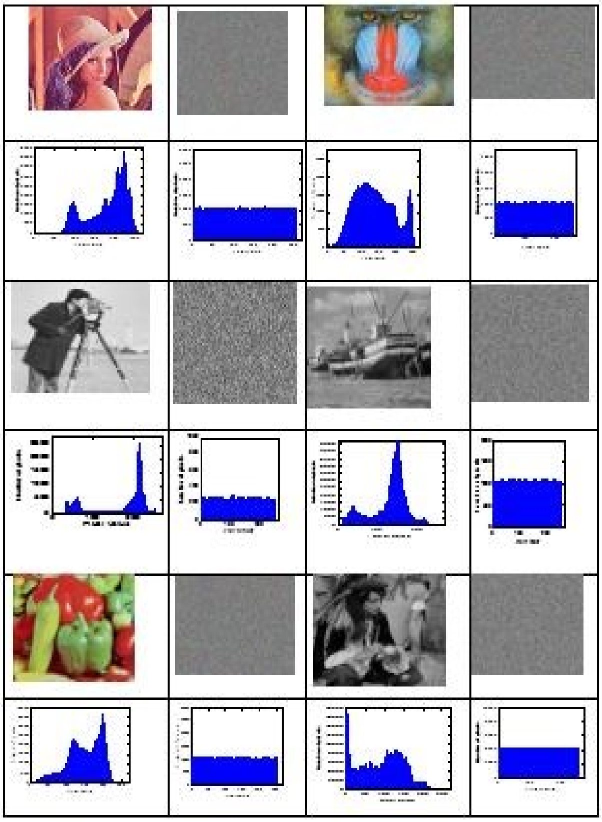


Table 4. Entropy of some tested images.

Image	*Size*	*Cypher*	*Entropy*
	256x256		7,9993
	512x512		7,9998
	512x512		7,9997
	1024x1024		7,9999
	256x256		7,9991

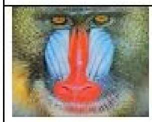
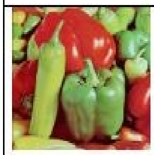
c) Correlation analysis

The correlation is given by:

$$r = \frac{cov(x,y)}{\sqrt{V(x)}\sqrt{V(y)}}. \qquad (30)$$

The following table illustrates the entropy of some reference images tested by our method:

Table 5. Correlation of some tested images.

		Original Image			Encrypted Image		
Image	Size	H-C	V-C	D-C	H-C	V-C	D-C
	512x512	0.9047	0.8520	0.8238	-0.0007	-0.0004	0.0001
	1024x1024	0.9774	0.9813	0.9668	-0.0001	-0.0002	-0.0010
	512x512	0.9786	0.9820	0.9694	-0.0002	0.0006	0.0002
	512x512	0.9774	0.9881	0.9696	0.0023	-0.0001	-0.0003

5) Differential analysis

Let be two encrypted images, whose corresponding free-to-air images differ by only one bit, from $(\boldsymbol{C_1})$and$(\boldsymbol{C_2})$, respectively. The expressions of these two statistical constants $(NPCR) and\ (UACI)$ are given by equations below

$$NPCR = \left(\frac{1}{nm}\sum_{i,j=1}^{nm} D(i,j)\right) * 100, \qquad (31)$$

$$\text{with} \quad D(i,j) = \begin{cases} 1 & if \quad C_1(i,j) \neq C_2(i,j), \\ 0 & if \quad C_1(i,j) = C_2(i,j) \end{cases}.$$

The $UACI$ mathematical analysis

$$UACI = \left(\frac{1}{nm}\sum_{i,j=1}^{nm} Abs\big(C_1(i,j) - C_2(i,j)\big)\right) * 100. \qquad (32)$$

a) Signal-To-Peak Noise Ratio (PSNR)

i. MSE

Mean Square Error (MSE): This is the cumulative square deviation between the original image and other noisy images. When the MSE level decreases, the error also decreases. This constant measure the distance between the pixels of the clear image and the encrypted image. Calculated by the next equation.

$$MSE = \sum_{i,j}(P(i,j) - C(i,j)^2, \qquad (33)$$

where $(P(i,j))$: pixel of the clear image and
$(C(i,j))$: pixel of the cypher image.

ii. PSNR

Since many signals have a large dynamic range, PSNR is usually expressed on a logarithmic decibel scale. The next equation gives the PSNR mathematical analysis of the image:

$$PSNR = 20Log_{10}\left(\frac{I_{max}}{\sqrt{MSE}}\right). \qquad (34)$$

Table 6. Differential parameters.

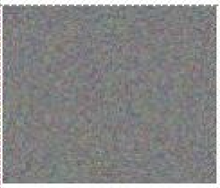
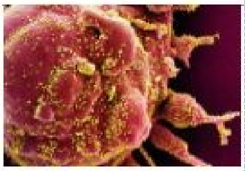
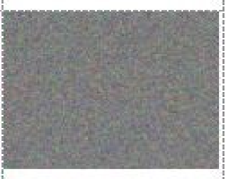
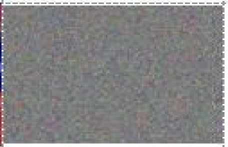
Image	Size	NPCR	UACI	PSNR
	256x256	**99,92**	**33,35**	**8,36**
	512x512	**99,67**	**34,23**	**8,65**
	1024x1024	**99,96**	**33,37**	**8,10**

b) Avalanche effect

Our algorithm uses a strong link between encrypted pixels and pixels with clear policies. As a result, as data propagates through the structure of the algorithm, gradual changes become increasingly important. The avalanche effect is the number of bits that have been changed if a single bit in the original image is changed. The mathematical expression of this avalanche effect is given by

$$AE = \left(\frac{\sum_i bit\ change}{\sum_i bit\ total}\right) * 100. \qquad (35)$$

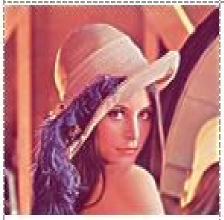
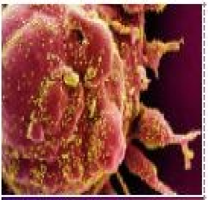
Table 7. Avalanche effect.

Original Image	Cypher Image	AE
		78,25
		77,04
		76,26

c) Performance time

In our technique, the encryption and decryption times are very similar and vary in the interval [0.05, 0.1].

Table 8. Performance time.

		Time	
Original Image	Size	Enc	Decr
	512x512	0,04	0,032
	256x256	0,011	0,008
	512x512	0,01	0,009

d) Speed analysis

To approve and document the quality of our methodology in a timely fashion. And finally, thanks to these properties, we have selected the "Lena" grayscale image with three different sizes (256×256) (512×512) and (1024×1024). The results are presented in Table 9.

Table 9. Execution time (in second).

Image	Our method	DES	AES
Lena (256×256)	0,09647	0.639772	5.687244e-002
Lena (512×512)	0,27448	7.449005	0.347506
Lena (1024×1024)	0,20154	29.11398	1.152980

We compared the results with two classic algorithms, AES and DES, and can determine that the execution time is reasonable. The test was conducted on other images of different sizes, and we obtained an acceptable score. This is due to the low algorithm complexity of the algorithm implemented in our strategy.

IX. MATH SECURITY

Our algorithm uses a large symmetric key that is extremely sensitive to initial conditions and control parameters. This ensures that small interference in the key will regenerate a new subject and a new calculation table. In addition, the complexity of using discrete logarithms in calculations increases the difficulty of attacking our systems. The construction of the key matrix is closely linked to the chaotic maps used, which eliminates any brutal attacks.

X. CONCLUSION

Hill's conventional system is very easy to install in the color image encryption system, as long as the inversion matrix is determined in the carefully selected ring. But due to linearity, this technique is still vulnerable to statistics and brute force attacks. Carried on instead of the classic $Z/256Z$ ring. Similarly, the construction of a large-sized invertible matrix has been introduced based on the involution block, and the non-zero eigenvalue matrix has been described in detail. The large number of matrices built in this way ensures better protection against any brutal attack. Using logarithms and discrete exponents and translation vectors to overcome linear problems will increase the complexity of our method.

Acknowledgement

This article is not subsidized by any public or private

organization. It is a personal work.

References

[1] Y. P. K. Nkandeu, A. Tiedeu, and Hill L., "Cryptography in an algebraic alphabet," *American Mathematical Monthly*, vol. 1929, no. 36, pp. 306-312, 2019.

[2] Y.P.K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 10013-10034, 2019.

[3] A. Jarjar, "Improvement of hill's classical method in image cryptography," *International Journal of statistics and Applied Mathematics*, vol. 2, no. 3, Part A, 2017.

[4] Lin CH, Lee CY, Lee C. Y., "Comments on Saeednia's improved scheme for the Hill cipher," *Journal of the Chinese Institute of Engineers*, vol. 27, no. 5, pp. 743-746, 2004.

[5] Bibhudendra Acharya1, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image encryption using advanced Hill cipher algorithm," *International Journal of Recent Trends in Engineering and Technology*, vol. 1, no. 1, 2009.

[6] C. Fu, G. Y. Zhang, M. Zhu, Z. Chen, and W. M. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," *Security and Communication Networks*, vol. 2018, pp. 1-13, 2018.

[7] Chang'e Dong, "Color image encryption using one-time keys and couple chaotic systems," *Signal Processing: image Communication*, vol. 29, no. 5, pp. 628-640, 2014.

[8] Xing-Yuan Wang, Sheng-Xian Gu, and Ying-Qian Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering,* vol. 68, pp. 126-134, 2015.

[9] Abdellatif JarJar, "Improvement of Feistel method and the new encryption scheme," *Optik*, vol. 157, pp. 1319-1324, 2018.

[10] S. Hraoui, F. Gmira, A. O. Jarar, K. Satori, A. Saaidi, "Benchmarking AES and chaos based logistic map for image encryption," in *Proceeding of ACS International Conference Computer Systems and Applications (AICCSA)*, 2013.

[11] M. Essaid, I. Akharraz, and A. Saaidi, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *Journal of Information Security and Applications*, vol. 47, pp. 173-187, 2019.

[12] Pand uranga and S. Naveen Kumar, "Advanced partial image encryption using two-stage Hill cipher technique," *International Journal of Computer Applications,* vol. 60, no.16, pp. 14-19, 2012.

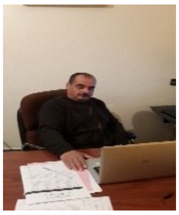
[13] Rifaat Zaidan Khalaf and Alharith Abdulkareem Abdullah, "Novel quantum encryption algorithm based on multiqubit quantum shift register and Hill cipher," *Advances in High Energy Physics*, vol. 2014, Article ID 104325, pp. 1-5, 2014.

[14] Rajwant Kaur, S. A. Khan, and Simranjit Kaur, "An efficient image encryption using DNA cryptography and reversible cellular automata," *International Journal of Computer Applications*, vol. 182, no. 24, pp. 32-38, 2018.

[15] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Tao Xiang, and Guanrong Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773-1783, 2009.

[16] Jan Sher Khan and J. Ahmad, "Chaos based efficient selective image encryption" *Multidimensional Systems and Signal Processing*, vol. 30, pp. 943–961, 2019.

Authors



Mr. Abdellatif JarJar is the alone author of this article, and therefore no conflict. To finalize this document, I did not receive any assistance funds from any organization. This document does not contain any studies or experiments on animals. This article does not contain any studies with animals performed by any of the authors. This article does not contain any studies with human participants or animals performed by any of the author.