New Cryptosystem Using Two Improved Vigenere Laps Separated by a Genetic Operator

Mohamed JARJAR (jarjar.mohamed@gmail.com)
USMBA FSTF: Universite Sidi Mohamed Ben Abdellah Faculte des Sciences et Techniques de Fes
https://orcid.org/0000-0003-2785-6258
Said HRAOUI
ENSAF: Universite Sidi Mohamed Ben Abdellah Ecole Nationale des Sciences Appliquees de Fes
Said NAJAH
USMBA FSTF: Universite Sidi Mohamed Ben Abdellah Faculte des Sciences et Techniques de Fes
Khalid ZENKOUAR
USMBA FSTF: Universite Sidi Mohamed Ben Abdellah Faculte des Sciences et Techniques de Fes

Research Article

Keywords: Vigenere grid, Chaotic map, Encryption function, S-Box, Genetic mutation

Posted Date: February 3rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1035932/v1

NEW CRYPTOSYSTEM USING TWO IMPROVED VIGENERE LAPS SEPARATED BY A GENETIC OPERATOR

1st.Mohamed JARJAR
Lab-SIA, Faculty of Sciences and Technologies
Sidi Mohamed Ben Abdellah University
Fez, Morocco
jarjar.mohamed@gmail.com

2nd.Said HRAOUI
LIASSE, National School of Applied Sciences
Sidi Mohamed Ben Abdellah University
Fez, Morocco
said.hraoui@usmba.ac.ma

3rd.Said NAJAH
Lab-SIA, Faculty of Sciences and Technologies
Sidi Mohamed Ben Abdellah University
Fez, Morocco
said.najah@usmba.ac.ma

3rd.Khalid ZENKOUAR
Lab-SIA, Faculty of Sciences and Technologies
Sidi Mohamed Ben Abdellah University
Fez, Morocco
khalid zenkouar@yahoo.fr

Abstract

This document traces the development of a new cryptosystem using two circuits ensured by a deep Vigenere classical technique improvement, separated by a genetic operator. This new technique employs several dynamic substitutions matrices attached to chaotic replacement functions; whose construction will be detailed. Firstly, we will be start by modifying the seed pixels by an initial value calculated from the original image, and will be infected through the chaotic map used to overcome the uniform image problem, followed by the improvements Vigenere injection technology. The output vector will be subdivided into sub blocks for future application of deeply improved genetic mutations to better adapt to color and medicals image encryption. The second round will increase the compdlexity of the attack and improve the installed systems. Simulations performed on a large number of images of different sizes and formats ensure that our approach is not exposed to known attacks.

Article Highlights

This new algorithm offers two tricks ensured by a deep improvement of Vigenere. We mention the most important changes made.

- First Vigenere's rotation
- Genetic mutation applied
- Second Vigenere's lap

$$Notation \begin{cases} G_t = {}^{Z}/_{tZ}\ ring \\ G_t^* = Set\ of\ G_t\ reversers \\ A(j:): Line\ number\ j\ of\ matrix\ A \\ A(:j): column\ number\ j\ of\ matrix\ A \end{cases}$$

Key word: ***Vigenere grid; Chaotic map; Encryption function; S-Box; Genetic mutation***

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. Despite the knowledge of the substitution matrix, this method has been able to withstand more than three centuries.

$$algorithm1 \begin{cases} Fist\ Row \\ For\ i = 1\ to\ 26 \\ V(1,i) = i \\ Next\ i \\ folloying\ Rows \\ For\ i = 2\ to\ 26 \\ For\ j = 1\ to\ 26 \\ V(i,j) = V(i-1,(j+1),26) \\ Next\ j,i \end{cases}$$

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

$$equation1 \begin{cases} C_i = V(P_i,K_i) = (P_i + K_i) \quad mod\ 26 \\ P_i = V(C_i,K_i) = (P_i - K_i) \quad mod\ 26 \end{cases}$$

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) Our contribution

This work puts into practice the implementation of a deeply modified genetic operator in a color image encryption system. This operator will be surrounded by two improved Vigenere circuits [11 – 12]

II. THE PROPOSED METHOD

Based on chaos [13 – 14], this new technology which acts at the pixel level by two Vigenere turns provided by a dynamic substitution's matrices and replacement functions [15 – 16 – 17]. These two rounds will be separated by a deeply improved genetic operator for future use in color image encryption. The following steps describe this algorithm

- Construction of chaotic sequences
  - New substitution matrices Construction
  - New attached replacement functions Definition
- Vectorization the original image
- Calculation of the first initialization value
- First Vigenere round Application
- Chaotic mutation application
- Calculation of the second initialization value
- second Vigenere round application
- Chaotic permutation application

At the end of this work, the follow-up operations of each encryption round will be described in detail to show the development of the system. and detailed analysis of the performance of our methodology will be discussed and compared with other referencing systems.

STEP 1: CHAOTIC SEQUENCES DEVELOPMENT

All the encryption parameters required to successfully run our system come from the two most commonly used chaotic maps in the field of cryptography. This choice is due to the simplicity of its development and its high sensitivity to the initial parameters.

1) The Logistics Map

The logistic map is a recurrent sequence described by a simple polynomial of second degree defined by the following equation[17 – 18],

$$Equation\ 2 \begin{cases} u_0 \in]0{,}5\ \ 1[\quad , \quad \mu \in [3{,}75 \quad 4] \\ u_{n+1} = \mu u_n (1 - u_n) \end{cases}$$

2) HENON'S Map

Henon's chaotic two-dimensional map was first discovered in 1978. It is described by equation below $[15-16]$

$$Equation3 \begin{cases} v_0 \ et \ \ w_0 \ \ a = 0.3 \ \ et \ \ b \in [1.07 \quad 1.4] \\ v_{n+1} = 1 + w_n - a v_n^2 \\ w_{n+1} = b v_n \end{cases}$$

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

$$Equation4 \begin{cases} v_0 \ and \ \ v_1 \ \ in \ [0 \quad 1] \ and \ a \ = 0.3 \ \ et \quad b \in [1.07 \quad 1.4] \\ v_{n+2} = 1 - a v_{n+1}^2 + b v_n \end{cases}$$

3) Chaotic used Vector design

Our work requires the construction of three chaotic vectors(GL), , $(GR)$and (LR), with a coefficient of(G_{256}), and the binary (VC) vector will be regarded as the control vector. This construct is seen by the following algorithm

$$Algorithm2 \begin{cases} for \ i = 1 \ to \ 3nm \\ GL(i) = mod\left(E\left(\dfrac{Sup\big(u(i), v(i)\big) + u(i) * v(i)}{2} * 10^{11}, 254\right) + 1\right) \\ GR(i) = mod\left(E\left(\dfrac{u(i) + 2 * v(i)}{2} * 10^{11}, 253\right) + 2\right) \\ LR(i) = E\left(\dfrac{|GL(i) - MR(i)|}{2}\right) \\ Next \ i \end{cases}$$

The binary vector (VC) is considered as a control vector

$$Algorithm3 \begin{cases} for \ i = 1 \ to \ 3nm \\ if \ u(i) \geq v(i) \ then \\ VC(i) = 0 \ else \ VC(i) = 1 \\ end \ if \\ Next \ i \end{cases}$$

the complexity of our algorithm.

AXE 2: PLAIN IMAGE PREPARATION

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

$$Algorithm5 \begin{cases} for\ i = 2\ to\ nm \\ X(3i-2) = Vr(i) \\ X(3i-1) = Vg(i) \\ X(3i) = Vb(i) \\ Next\ i \end{cases}$$

This step slightly reduces the high correlation between the pixels.

1) First Initialization Value Design

First, the$(IV1)$ initialization value must be recalculated to change the value of the starting pixel. Ultimately, the $(\boldsymbol{IV1})$ value is provided by the next algorithm

$$Algorithm4 \begin{cases} for\ \ i = 2\ to\ 3nm \\ IV1 = IV1 \oplus\ X(i) IV1 \oplus\ GL(i) \\ Next\ i \end{cases}$$

The presence of the vector (GL) is to overcome the problem of the uniform image.

STEP3: 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) Vigenere's Advanced Methods

This classical technique requires the generation of a substitution matrix and a replacement function

a) Substitution matrices generation

This technique requires the establishment of two substitutions matrices $(VG1)$ and $(VD1)$ of size $(256,256)$, 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

$$Equation\ 5 \quad \begin{cases} if RP(i) = 256\ the\ RP(i) = 0 \\ if RR(i) = 256\ the\ RR(i) = 0 \end{cases}$$

This new construction is entirely supervised by the vector (CR). It is given by the following algorithm

$$algorithm6 \begin{cases} Fist\ Row \\ For\ \ i = 1\ \ to\ 256 \\ VG1(1,i) = RP(i) \\ VD1(1,i) = RR(i) \\ Next\ i \end{cases} \begin{cases} Next\ lines \\ For\ \ i = 2\ \ to\ 256 \\ For\ \ j = 1\ \ to\ 256 \\ if\ VC(i) = 1\ then \\ VG1(i,j) = VG1\left(i-1, RP\left(mod\left(j + GL(i)\right), 256\right)\right) \\ VD1(i,j) = VD1\left(i-1, RR\left(mod\left(j + GR(i)\right), 256\right)\right) \\ else \\ VG1(i,j) = VG1\left(i-1, RP\left(mod\left(j + GR(i)\right), 256\right)\right) \\ VD1(i,j) = VD1\left(i-1, RR\left(mod\left(j + GL(i)\right), 256\right)\right) \\ end\ if \\ next\ j,i \end{cases}$$

Example: in (G_8)

(VG)	1	2	3	4	5	6	7	0		CR	KL	CL
1	3	5	0	6	2	7	1	4				
2	2	7	1	4	3	5	0	6		1	5	4
3	4	3	5	0	6	2	7	1		1	3	5
4	2	7	1	4	3	5	0	6		0	3	4
5	0		2	7	1	4	3	5		1	4	2

(VD)	1	2	3	4	5	6	7	0
1	0	4	5	7	1	2	6	3
2	7	1	2	3	3	0	4	5
3	0	4	5	7	1	2	6	3
4	1	2	6	3	0	4	5	7
5	0	4	5	7	1	2	6	3

1) New Vigenere's Mathematica expression

Based on the classic Vigenere technique, we have developed this new encryption method.

a) Classic Vigenere function expression

These two matrices will be used together in the encryption process and will be completely under vector control (VC). We remember to pass Vigenere's classic replacement function through the following formula

$$Equation6 \quad \{ \quad Y(i) = VG1(K, X(i))$$

(K) key duplicated to the size of the text to be encrypted.

b) New Vigenere function expression

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

$$Equation7 \quad V_1(X(i)) = \begin{cases} if\ CR(i) = 0\ then \\ Y(i) = VG1\big(GL(i), VD1\big(GR(i), \mathrm{X}(i)\big) \oplus \mathrm{LR}(i)\big) \\ else \\ Y(i) = VD1\big(LR(i), VG1\big(GL(i), \mathrm{X}(i)\big) \oplus \mathrm{GR}(i)\big) \end{cases}$$

c) First-round spread function Expression

The first round will be equipped with a powerful diffusion function to connect encrypted pixels with subsequent transparent pixels to increase the impact of the avalanche effect and protect the system from any differential attacks. The expression of this new diffusion function is given by the formula below

$$\text{Equation 8} \quad \forall\, i > 1 \quad \Phi\big(X(i)\big) = VD1(GL(i), X'(i-1) \oplus X(i))$$

2) The first-round analysis

This first round is defined by the following algorithm,

$We\ note: V_1(X'(1)) = Y(i)$

$$Algorithm\,7 \begin{cases} X'(1) = IV1 \oplus X(1) \\ Y(1) = V_1(X'(1)) \\ For\ i = 2\ to\ 3nm \\ X'(i) == \Phi\big(X(i)\big) \\ Y(i) = V_1(X'(1)) \\ Next\ i \end{cases}$$

The figure below shows the first round

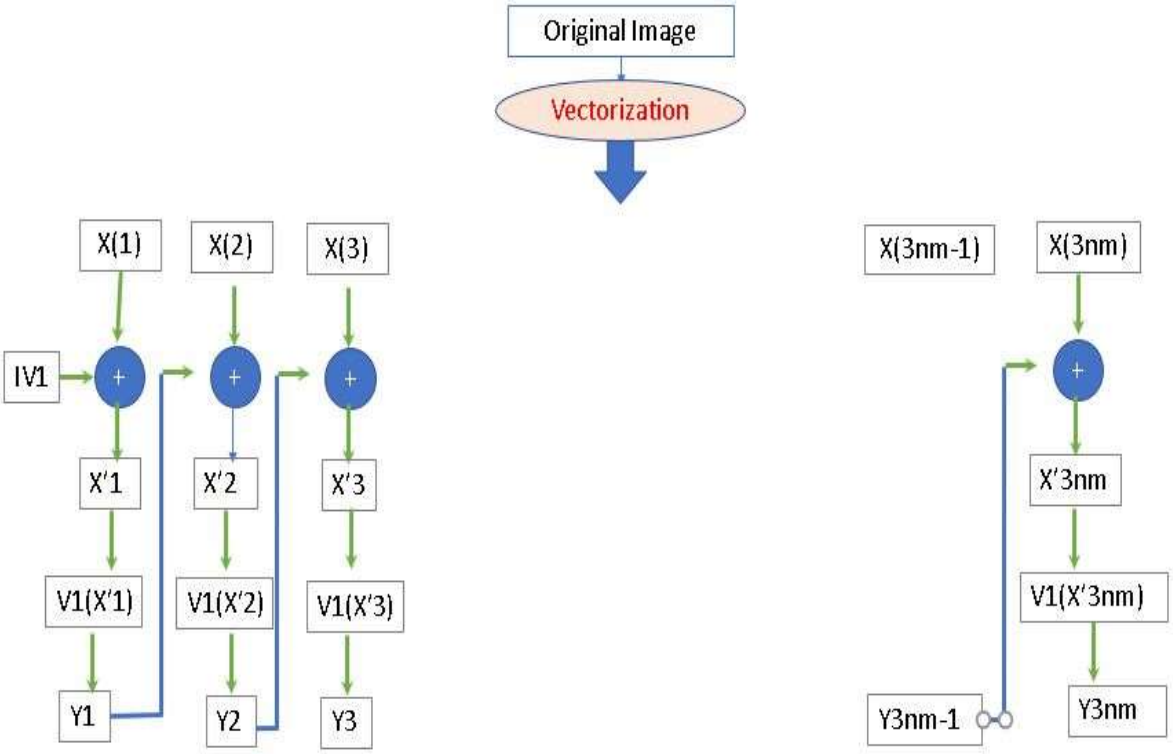
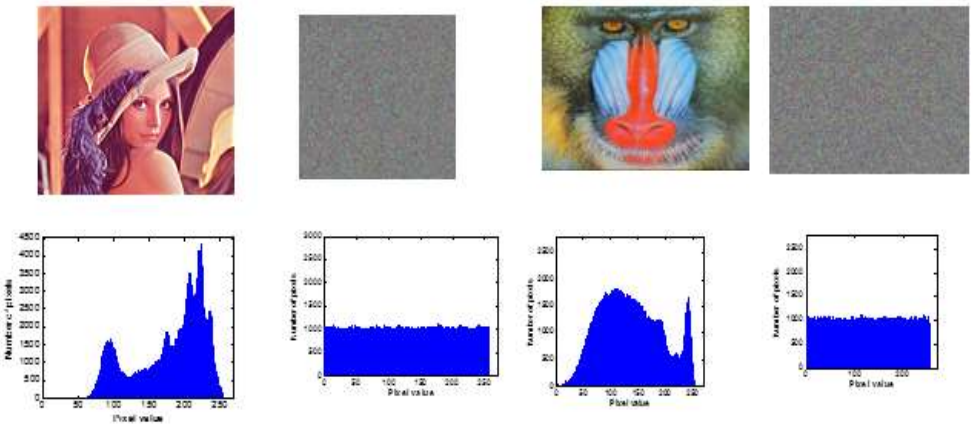


Figure1: First round

a) First round analysis

For a better follow-up of our algorithm, several reference images were tested by this first round, we quote



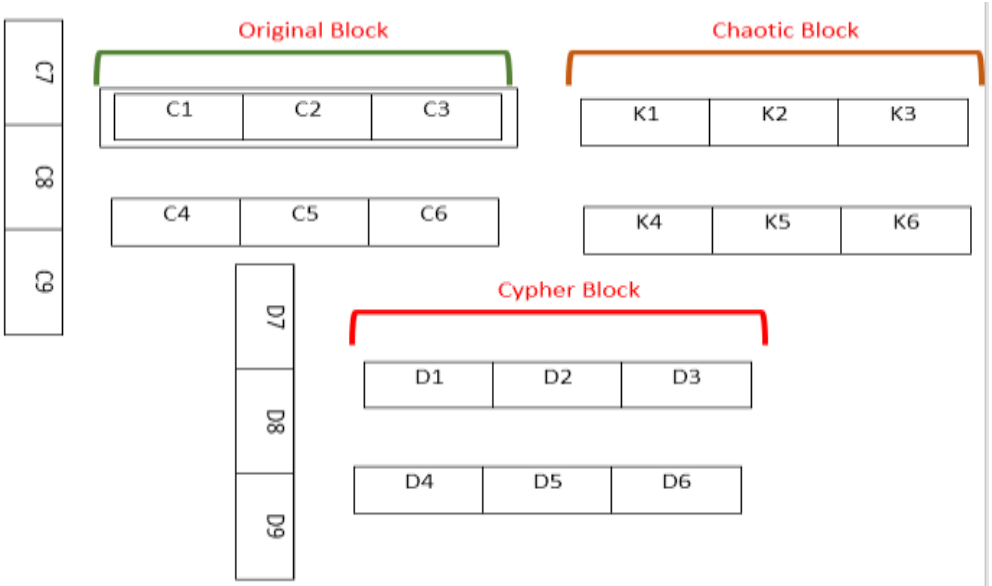
At the end of the first round, the output vector (Y) will be treated as a clear image and subdivided into three sub-blocks of equal size for future submission to genetic mutation.

3) Genetic mutation

Gene mutation is the exchange of sub-blocks between three blocks of the same size. This exchange is provided by two chaos constants (CP) and (CE). The first indicates the starting position of the sub-block to be swapped, and the second indicates the size of the sub-block. In our method, these two constants are defined as

$$EQuation\ 9 \begin{cases} CP = mod\left(\sum_{i=1}^{Sup(n,m)} |GL(i) - RL(i)|, E(\frac{n}{2})\right) + E(\frac{n}{2}) \\ CE = mod\left(\sum_{i=1}^{Inf(n,m)} |GL(i) + RL(i)|, E(\frac{m}{2})\right) + E(\frac{m}{2}) \end{cases}$$

The mutation process between three blocks of size $(1,nm)$ each is illustrated by the following figure

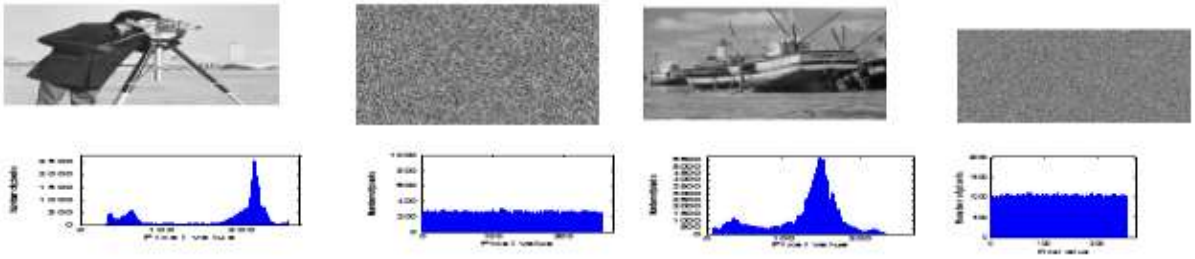


This mutation process follows the following formula

$$Equation\ 10 \begin{cases} D1 = C7 \oplus K1 \\ D2 = C5 \\ D3 = C6 \oplus K6 \\ D4 = C1 \\ D5 = C8 \oplus K5 \\ D6 = C3 \\ D7 = C4 \oplus K4 \\ D8 = C2 \\ D9 = C9 \oplus K3 \end{cases}$$

1) Second round analysis

For a better follow-up of our algorithm, several reference images were tested by this first round, we quote



The generated vector will be submitted to a second round of Vigenere provided by two other substitution matrices.

1) *Second Vigenere round*

At the end of the first round, the new (IV2) initialization value will be calculated according to the following algorithm

$$Algorithm8 \begin{cases} for\ \ i = 2\ to\ 3nm \\ IV2 = IV2 \oplus\ Y(i) \\ Next\ i \end{cases}$$

In the second round, by simply replacing the position of the replacement matrix, the output vector will be treated as a new image to be encrypted by the same method as the first round.

a) *Second round analysis*

The second round can also be ensured by using a different same matrix in the first round.

$$Equation11 \quad V_2(X(i)) \begin{cases} if\ VC(i) = 0\ then \\ Y(i) = VD1(GL(i), VG1(MR(i); X(i))) \oplus ML(i) \\ else \\ Y(i) = VG1(ML(i), VD1(GL(i), X(i))) \oplus MR(i) \end{cases}$$

The same mold will be used in the second round, but in a different way

a) *Second-round spread function Expression*

The second round will be equipped with the diffusion (Ω) ensured by the replacement matrix generated. The expression of this function is defined by the following notation

$$\text{Equation12} \quad \forall\, i > 1 \quad \Omega(X(i)) = VD1(ML(i), X'(i-1) \oplus X(i))$$

a) *The Second-round analysis*

This second round is defined by the following algorithm

$$Algorithm\,9 \begin{cases} Y'(1) = IV2 \oplus Y(1) \\ Z(1) = V_2(Y'(1)) \\ For\ i = 2\ to\ 3nm \\ \quad \alpha = \Omega(Y(i)) \\ \quad Z(i) = V_2(\alpha) \\ \quad Next\ i \end{cases}$$

The figure below shows the first round

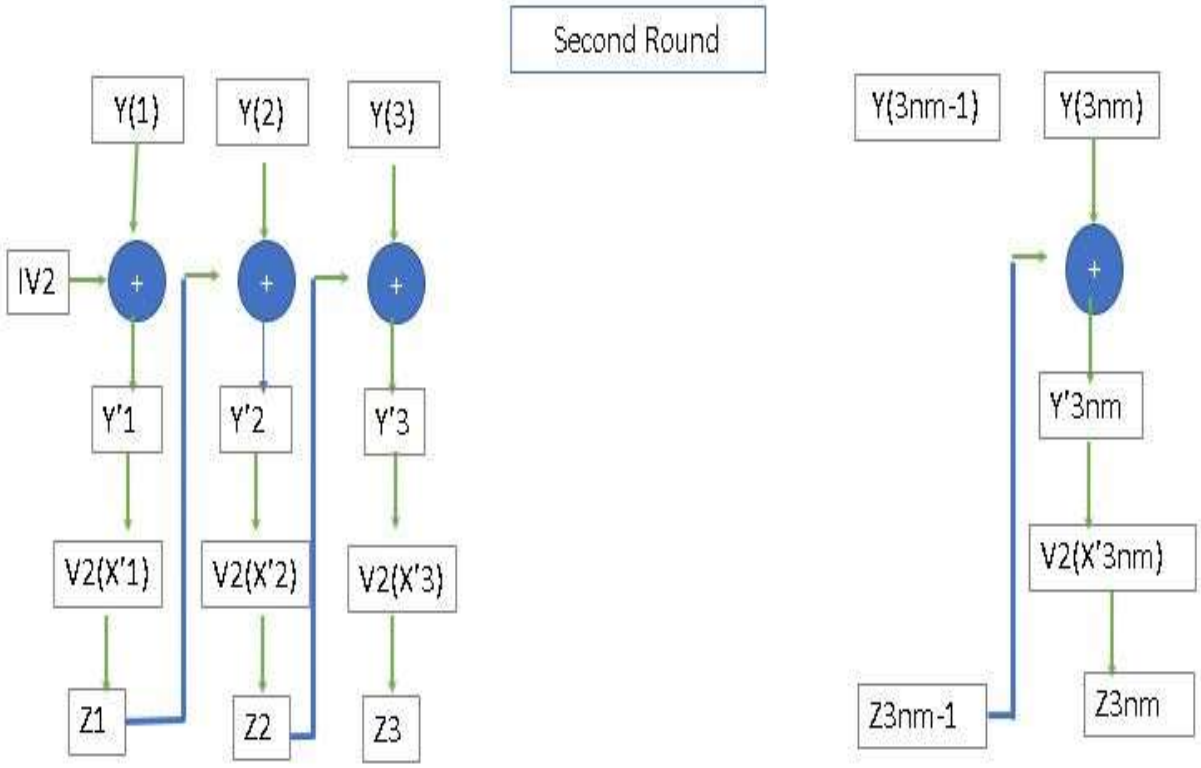


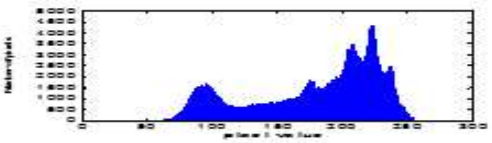
Figure7: The Second round of our approach

2) Third round analysis

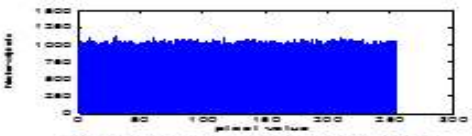
For a better follow-up of our algorithm, several reference images were tested by this first round, we quote

a) Plain image

b) Cipher image



c) Histogram of plain image



d) Histogram of cipher image

The output vector (Z) will be subjected to permutation (PH) to possibly suppress any correlation.

STEP 5: DECRYPTION OF ENCRYPTED IMAGES

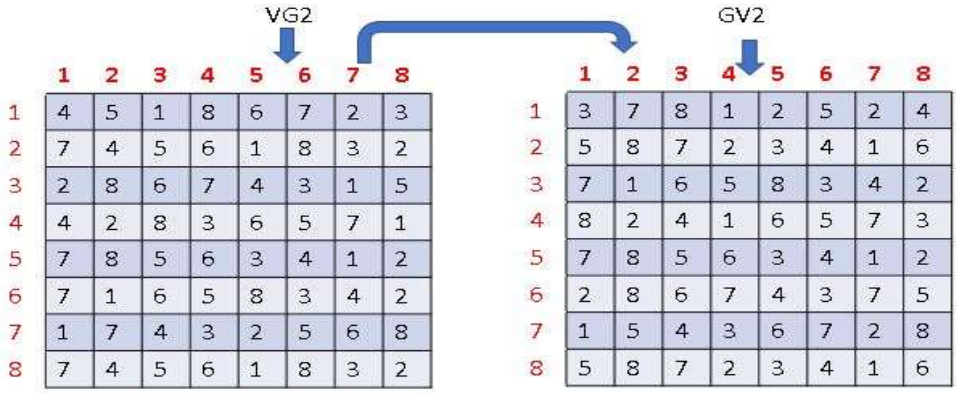
In the literature, the classic Vigenere method uses the same matrix in both processes. Our contribution in this work is that the matrix used in encryption is different from the matrix used in decryption. Therefore, the calculation of the decryption matrix is necessary.

2) *Decryption matrix structure*

Each row of the encrypted S-box is a permutation in (G_{256}), so the decryption matrix will consist of reverse permutations. For this reason, two decrypted $S-Box$ generations are given by the following algorithm

$$Algorithm11 \begin{cases} for\ i=1\ to\ 256 \\ for\ j=1\ to\ 256 \\ VG2\big(i,VG1(i,j)\big)=j \\ VD2\big(i,VG2(i,j)\big)=j \\ Next\ j,i \end{cases}$$

Example



	1	2	3	4	5	6	7	8
1	4	5	1	8	6	7	2	3
2	7	4	5	6	1	8	3	2
3	2	8	6	7	4	3	1	5
4	4	2	8	3	6	5	7	1
5	7	8	5	6	3	4	1	2
6	7	1	6	5	8	3	4	2
7	1	7	4	3	2	5	6	8
8	7	4	5	6	1	8	3	2

	1	2	3	4	5	6	7	8
1	3	7	8	1	2	5	2	4
2	5	8	7	2	3	4	1	6
3	7	1	6	5	8	3	4	2
4	8	2	4	1	6	5	7	3
5	7	8	5	6	3	4	1	2
6	2	8	6	7	4	3	7	5
7	1	5	4	3	6	7	2	8
8	5	8	7	2	3	4	1	6

1)*Decryption function*

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

In the first round

$$Equation15 \begin{cases} if\ \ z=VD_1(y,x)\oplus b \\ Then \\ x=(VD_2(y,z\oplus b)) \end{cases}$$

In the second round

$$Equation16 \begin{cases} if\ \ z=VG_1(y,x) \\ Then \\ x=VG_2(y,z) \end{cases}$$

2)*Decrypt the encrypted image*

Our algorithm is a symmetric encryption system, so the same key will be used in the decryption process. In addition, installing the broadcast function requires us to start the decryption process from the last pixel to the first pixel, and recalculate the initialization value to get the exact value of

the first pixel. In addition, decryption uses the countdown function of encryption.

a) Reverse permutation

The inverse permutation (HP) of (PH) is given by the following algorithm

$$Algorithm12\begin{cases}For\ i=1\ to\ 3nm\\ HP\big(PH(i)\big)=i\\ Next\ i\end{cases}$$

After vectorization of the image encrypted in vector (ZC), an intervention of the permutation (HP) to recover the vector (Z). This operation is determined by the following algorithm

$$Algorithm\ 13\begin{cases}For\ i=1\ to\ 3nm\\ Z(i)=HP\big(ZC(i)\big)\\ Next\ i\end{cases}$$

b) The reciprocal of the Second lap function

$$Algorithm14\begin{cases}For\ i=3nm\ to\ 1\\ if\ VC(i)=0\ Then\\ Y(i)=VD_2\Big(ML(i),VG_2\Big(MR(i),VD_2\big(GL(i),Z(i)\big)\Big)\oplus MLi(i)\Big)\oplus Z(i-1)\\ Else\\ Y(i)=VD_2\Big(VD_2\Big(ML(i),VG_2\big(GL(i),X(i)\big)\oplus MR(i)\Big)\Big)\oplus Z(i-1)\\ NExt\ i\end{cases}$$

A recalculation of the initialization value will make it possible to retrieve the exact value of pixel $Y\ (1)$

c) The reciprocal of the First lap function

$$Algorithm\ 15\begin{cases}FOr\ i=3nm\ to\ 1\\ if\ VC(i)=0\ Then\\ X(i)=VD_2(ML(i),a^{-1}\big(VD_2\big(MR(i),VG_2(GL(i),X(i))\big)\oplus ML(i)\big))\oplus Y(i-1)\\ Else\\ X(i)=VD_2(ML(i),c^{-1}\big(VG_2\big(ML(i),VD_2(GL(i),X(i))\big)\oplus MR(i)\big)\oplus Y(i-1)\end{cases}$$

A recalculation of the initialization value will make it possible to retrieve the exact value of pixel $X\ (1)$

d) The reverse mutation

In general, mutation is an involutive operation, therefore we have

$$equation17\ (Mt)^{-1} = Mt$$

III. DEEP SIMULATIONS

We randomly selected 150 images from a chaotic vector that contained a database of thousands of color images in different sizes and formats. All these images were tested by our system. all experiments are performed under the Matlab software running under Windows 7, on a basic i7 personal computer, $16\ GB\ RAM, and\ 500\ GB\ hard\ disk$, and we found the following results.

1)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 is

$$\begin{cases} u_0 = 0{,}7655412001 \\ \mu = 3.89231541 \\ v_0 = 1{,}3561 \\ v_1 = 0.865421331 \\ b = 1{,}071 \end{cases}$$

If we use single-precision real numbers $\mathbf{10^{-10}}$ to operate, the total size of the key will greatly exceed $\approx \mathbf{2^{150}} \gg \mathbf{2^{110}}$, which is enough to avoid any brutal attacks.

2)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

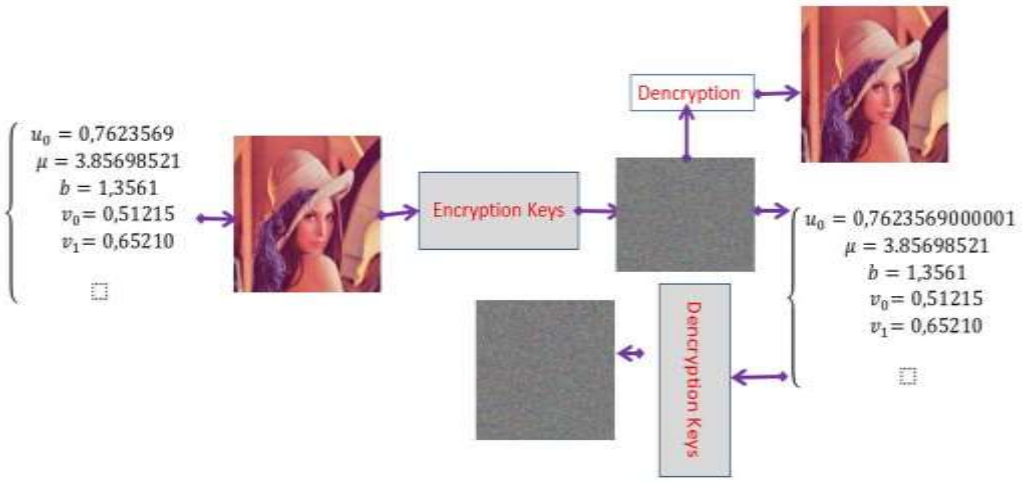


Figure6: Encryption key sensitivity

This ensures that in the absence of the real encryption key, the original image cannot be restored.

1) *Statistics Attack Security*

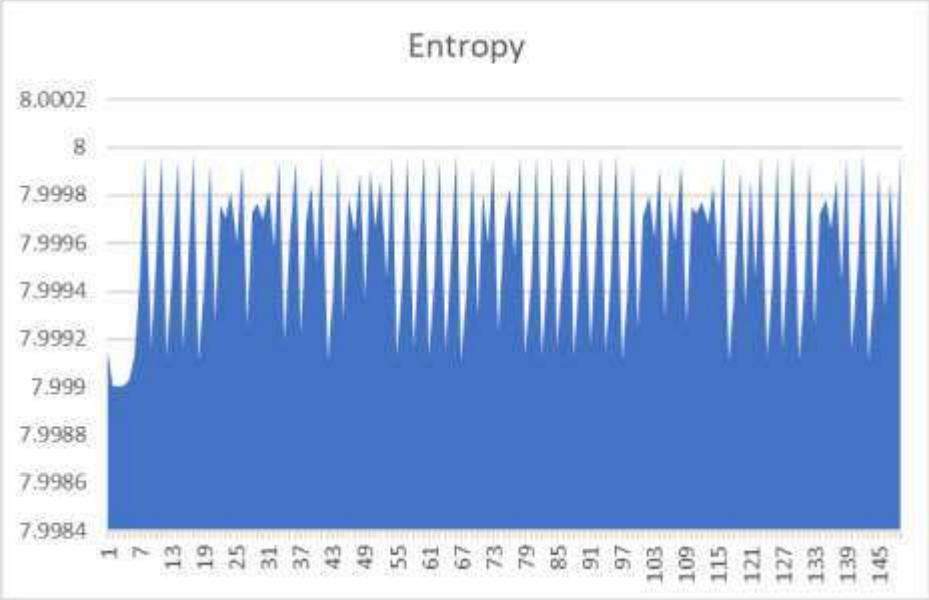
a) Entropy Analysis

The entropy of an image of size $(n, m)$is given by the equation below

$$Equation15 \quad H(MC) = \frac{1}{t}\sum_{i=1}^{t} -p(i)\, log_2(p(i))$$

$p(i)$ is the probability of occurrence of level (i) in the original image.

The entropy values on the $150\, images$ tested by our method are represented graphically by the following figure



Fugure8: Entropy of 150 images of the same size

The entropy values calculated for the $150\, images$ tested by our system are all stored in$[7{,}997 \quad 7{,}9998]$. These values are close to the maximum value 8, therefore our system is safe from entropy attack.

b) Correlation analysis

The correlation of an image of size $(n, m)$is given by the equation below

$$Equation18 \quad r = \frac{cov(x, y)}{\sqrt{V(x)}\sqrt{V(y)}}$$

Simulations made on 150 images of the database gave the vertical correlation scores are displayed in Figure below

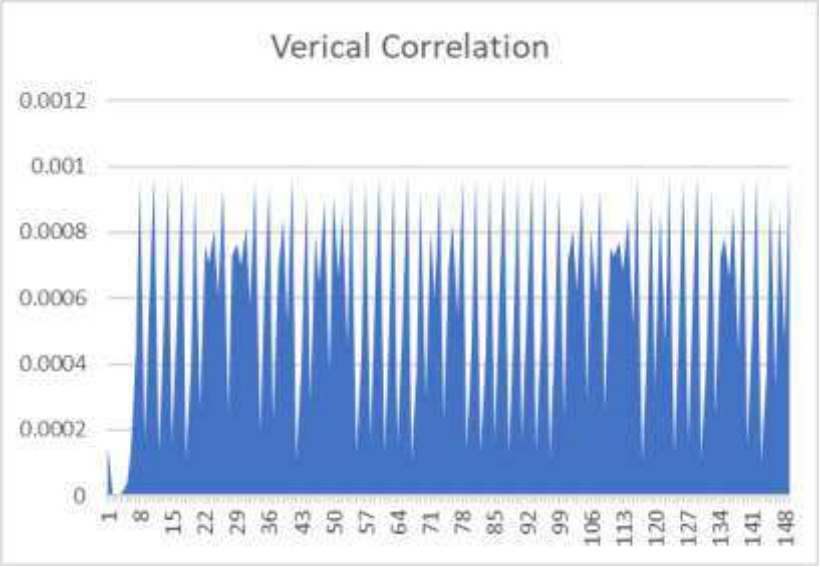


fIgure10: Vertical correlation of 70 images of the varying sizes

Figure 10 shows that the vertical correlation values of the encrypted images are close to zero. This ensures high security against correlation attacks.

c) Differential analysis

In cryptography, differential attacks are managed by the following constants

(a)The NPCR constant

It is determined by the equation below

$$Equation19 \qquad NPCR = \left(\frac{1}{nm}\sum_{i,j=1}^{nm} D(i,j)\right) * 100$$

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

(b)The UACI constant

The $UACI$ mathematical analysis of an image is given by the next equation

$$Equation\ 20 \qquad UACI = \left(\frac{1}{nm}\sum_{i,j=1}^{nm} Abs\big(C_1(i,j) - C_2(i,j)\big)\right) * 100$$

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

(i) MSE

The MSE mathematical analysis of an image is given by the next equation

$$Equation21 \quad MSE = \sum_{i,j} (P(i,j) - C(i,j)^2$$

$(P(i,j))$; pixel of the clear image

$(C(i,j))$: pixel of the cypher image

(a)PSNR

The $PSNR$ mathematical analysis of an image is given by the next equation

$$Equation22 \quad PSNR = 20Log_{10}\left(\frac{I_{max}}{\sqrt{MSE}}\right)$$

The study of the 150 $selected\ images$ revealed the following diagram

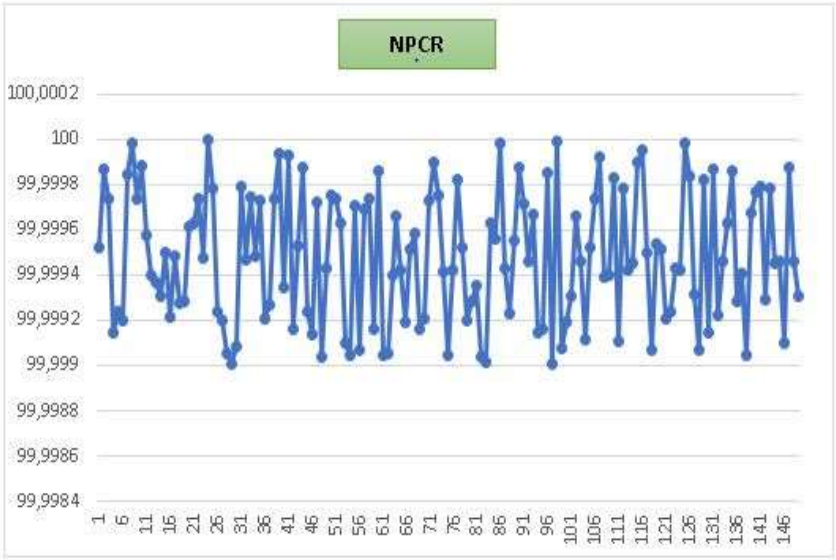


figure12: NPCR of 150 images of the varying sizes

All detected values are inside the confidence interval $[99{,}63 \quad 99{,}95]$. 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

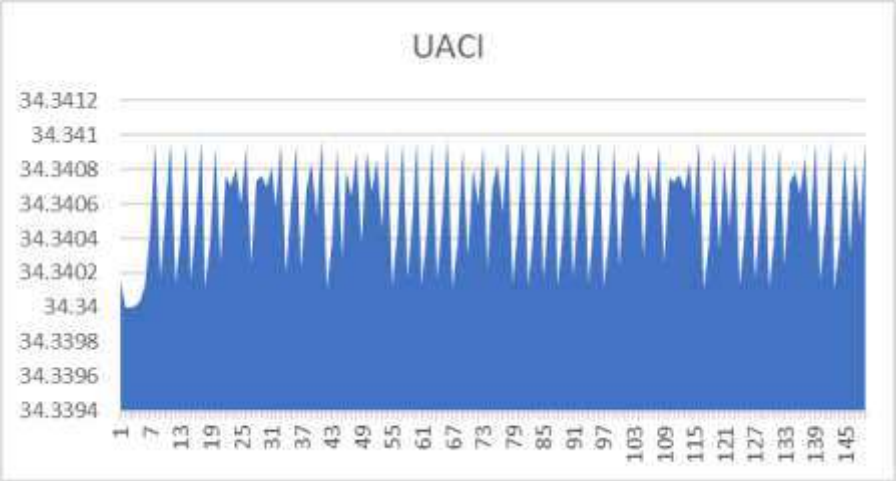


fIgure13: UACI of 150 images of the varying sizes

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.

d) Avalanche effect

Our algorithm uses a strong link between encrypted pixels and subsequent clear pixels in the strategy. This leads to a gradual change in the value, which becomes more and more important as the data spreads through the structure of the algorithm. The avalanche effect is the number of bits that have been changed if a single bit of the original image is changed. The mathematical expression of this avalanche effect is given by

$$Equation23 \quad AE = \left(\frac{\sum_i bit\ change}{\sum_i bit\ total}\right) * 100$$

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

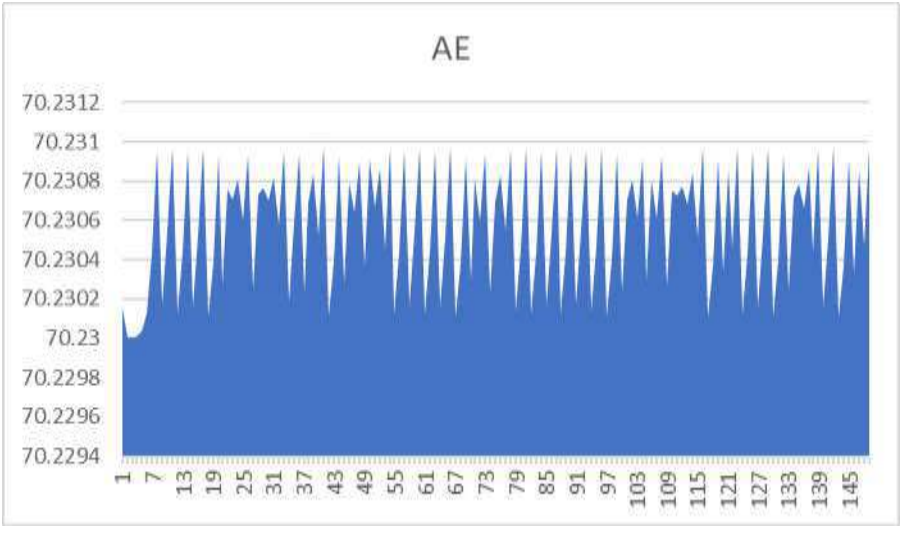
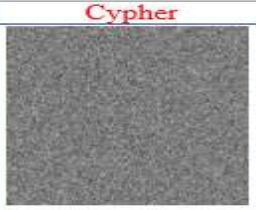
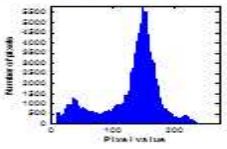
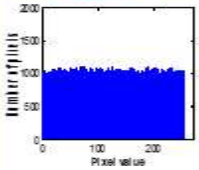


Figure14: Avalanche effect

All values returned from the AE by our method are all in the range of residual values $[73{,}96 \quad 74;02]$. This ensures that a single bit change

a) Performance time

In our technique, the encryption and decryption times are very similar and vary in the $interval$ $[0{,}05 \quad 0{,}1]$.

image		Histogram		Round *Time*		
Original	Cypher	Original	Chypher	1	2	3
				0,03	0,05	0,08

IV. MATH SECURITY

Our encryption keys are large, which can ensure that the new system is protected from brute force attacks. At the same time, the randomness of the operators described in the system makes it difficult to unlock any encrypted images, which increases the difficulty of statistical attacks. In addition, due to the high sensitivity to the initial parameters of our three chaotic cards, and the broadcast installed in each tower confirmed the robustness of our encryption system.

V. CONCLUSION

Due to their high sensitivity to initial conditions, our algorithm can prevent sudden attacks. This new technology is based on two deeply improved Vigenere rounds, using dynamic substitution matrices to attach to highly developed substitution functions. These two techniques are separated by genetic mutations suitable for color image encryption. The two calculated initialization values increase the complexity of the system. The monitoring of encryption in three rounds showed robustness and improved results from round to round. The global analysis of the system, ensures that our algrithm can cope with any known attack.

Conflict of Interest

All the authors of this article, there is no conflict of interest and add that no organization or private or public laboratory finances its research, moreover the research carried out no experiment on animals or human beings.

Informed consent

We all have the approval to write and write this article giving a new method of encryption of color images.

Ethical approval

We have respected the ethics of the journal

References

[1] F Sum.S.Lin.Z.Li.ZChaos solution & Fractal 3& 2008 631-640

[2] U.Patidar.M.Parek.G.Purolit.K.ud optics communication 254 (2011) 4331-4339

[3] A.Jarjar« Improvement of hill' sclassical method in image cryptography » International Journal of Statistics and Applied Mathematics 2017, Volume 2 Issue 3, Part A

[4] Imam Saputra, Mesran, Nelly Astuti Hasibuan3, "Vigenere Cipher Algorithm with Grayscale Image Key Generator for Secure Text File" International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue 01, January-2017

[5] Vaka Vamshi Krishna Reddy, Sreedhar Bhukya 2, "ENCRYPT AND DECRYPT IMAGE USING VIGENERE CIPHER", International Journal of Pure and Applied Mathematics, Volume 118 No. 24 2018

[6] Quist-Aphetsi Kester, « A cryptosystem based on Vigenère cipher with varying key", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012

[7] I Gede Arya Putra Dewangga, Tito Waluyo Purboyo, Ratna Astuti Nugrahaeni," A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography" International Journal of Applied Engineering Research, Volume 12, Number 21 (2017) pp. 10626-10636

[8] Md. Khalid Imam Rahmani, Neeta Wadhwa, Vaibhav Malhotra, "ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER", Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012

[9] Mohamed Boussif, Noureddine Aloui, Adnene Cherif , » Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher" ", IET DIGITAL LABRERY? 28/01/2020

---

[10]. Jun Peng, Xiaofeng Liao, and Zhongfu Wu, "Digital image secure communication using Chebyshev map chaotic sequences," IEEE secure communication, pp. 492-496, 2002

[11]. Hraoui.S.; Gmira.F.; Jarar,A.O.; Satori.K.; Saaidi.A: Benchmarking AES and chaos based logistic map for image encryption. Computer Systems and Applications (AICCSA), 2013 ACS International Conference

[12] M. Francois, T. Grosges, D. Barchiesi and R. Erra, "A New Image Encryption Scheme Based on Chaotic Function" in Signal Processing-Image Communication Elsevier, (2011), pp. 249-259.

[13] Ashish Shah » Enhancing Security of Vignere Cipher using Modified RC4" International Journal of Computer Applications (0975 – 8887) Volume 136 – No.5, February 2016

[14] H Li, Y Wang, Z Zuo - Optics and Lasers in Engineering, 2019 "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms" Volume 115, April 2019, Pages 197-207

[15] Rongjun Ge all « A Novel Chaos-Based Symmetric Image Encryption Using Bit-Pair Level Process" July 8, 2019, date of current version August 7, 2019.

[16] Mohamed JarJar "Further improvement of the HILL method applied in image encryption" Procedia computer sciences 00(2019)000-000

[17] Shams Mahmoud Abd Ali » Novel Encryption Algorithm for Securing Sensitive Information Based on Feistel Cipher”Test engeenering managenment Page Number: 10 - 16 Publication Issue:19 Volume: 80 September-October 2019