New mode of operation inspired by the braid of long hair

Hana ALI-PACHA[1]*, Adda Belkacem ALI-PACHA[2], Naima HADJ-SAID[3]

[1] ETIS laboratory, ENSEA, 6 Av. Ponceau Cergy-Pontoise, France

[2, 3] LACOSI laboratory, University of Sciences and Technologies of Oran, Mohamed Boudiaf, Algeria

hana.ali-pacha@ensea.fr*, a.alipacha@gmail.com, naima.hadjsaid@univ-usto.dz

***Corresponding author:** Hana ALI-PACHA
hana.ali-pacha@ensea.fr

Abstract: In cryptography, a mode of operation is the way of processing plaintext and encrypted text blocks within a block cipher algorithm, or it is the presentation of a method of chaining blocks in a block cipher. Several models exist with their strengths, some are more vulnerable than others, and some combine authentication and security concepts. In this paper, a new mode of operation is proposed, inspired by the braid of long hair which we call mode CBLCH (Cipher Braided Long Hair Chaining). The HILL cipher will be used to validate it and to compare it with ECB (Electronic Code-Book: code dictionary) and CBC mode (Cipher Block Chaining: sequence of blocks) by the influence of a pixel change on the plaint-image and the encrypted image.

Keywords: Cryptography, Operators Modes, Electronic Code Book, Cipher Block Chaining, Logistic Map, Hill cipher.

1. Introduction

The definition of block ciphers induces a natural way to encrypt fixed-size blocks (Blazhevski et.al., 2013; Bujari & Aribas, 2017; Dworkin, 2018; Rogaway, 2011). There are however different ways to use these primitives to encrypt messages of any size, called modes of operation.

An operating procedure consists of a detailed description of the actions necessary to obtain a result (Hadj-Said et al., 2011). It usually describes the detailed sequence of operations performed on a fixed station, but it can also describe the sequence of operations from station to station. An operating mode describing the operational sequences from workstation to workstation makes it possible to define:

- all the operational stations involved in the production of a product, an elementary part;
- the expected (allocated) transit times for each station;
- the logical order of intervention of each station (machine, or manual station);
- the conditions for chaining, triggering, and successive operations;
- the transfer methods from post to post.

Historically, in cryptography, modes of operation have been extensively studied (Bujari & Aribas, 2017; Dworkin, 2018; Rogaway, 2011) for their error propagation properties during various data modification scenarios during encryption.

The most natural mode is to split the message into n-bit blocks and apply the encryption function to each of these blocks with the encryption key K. This mode is called ECB (Electronic Code Book). It should not be used, as the encrypted messages obtained leak information on the corresponding clear messages. Indeed, two identical blocks of light lead to two blocks of identical numbers, which is why it is recommended to use the CBC mode (Cipher Block Chaining) which is more suitable to fill this weakness.

In this paper, a new mode of operation is proposed, more efficient than the CBC mode. This is inspired by the long hair braid (Figure 1) called CBLCH (Cipher Braided Long Hair Chaining) mode.

https://doi.org/10.33436/v33i4y202302

Figure 1. Braided long hair

The HILL cipher will be used to validate and compare it with the ECB mode (Electronic Code Book) and the CBC mode (Cipher Block Chaining: sequence of blocks). The choice of the HILL algorithm is motivated by the simplicity of the description, in this paper, of the principles of encryption and decryption of the algorithm.

2. Hill encryption Hill cipher

Lester Hill (1891-1961) was a mathematician cryptographer (Lester, 1929) published in 1929 in the journal American Mathematical Monthly an article entitled: "Cryptography in an algebraic alphabet", where he details a new type of encryption algorithm.

It is a polygraph cipher (Lester, 1929; Smart, 2004), that is to say, the letters are not encrypted one after the other, but in packets. Let's study in this paper the bi-graphic version that is to say that our group the letters two by two.

In the first encryption phase, each pixel to be encrypted is replaced by its numerical value between 0 and 255. The numbers thus obtained are grouped by 2. The pixels P$_k$ and P$_{k+1}$ of the plaintext image will be encrypted C$_k$ and C$_{k+1}$ with the formula below:

$$\begin{pmatrix} c_k \\ c_{k+1} \end{pmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} . \begin{pmatrix} p_k \\ p_{k+1} \end{pmatrix} .\mathrm{mod}(256) \tag{1}$$

This means, that the first two pixels of the clear image (P$_1$ and P$_2$) will be encrypted (C$_1$ and C$_2$) according to the following two Equations:

$$\begin{cases} c_1 = a.p_1 + b.p_2 .\mathrm{mod}(256) \\ c_2 = c.p_1 + d.p_2 .\mathrm{mod}(256) \end{cases} \tag{2}$$

where, a, b, c, and d, are integers, C$_1$ and C$_2$ will also be integers. The choice of the key here corresponds to the choice of linear combinations to be made (they are always the same block to block).

To decrypt, the principle is the same as for encryption: the encrypted values are used two by two, and then they are multiplied by the inverse matrix.

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} . \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} .\mathrm{mod}(256) \tag{3}$$

Ordinary, the inverse of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is (Easttom, 2016):

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}.\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.\text{mod}(256) \tag{4}$$

With the condition that: $ad - bc \neq 0$

3. Modes of operation

Block ciphering (Bujari & Aribas, 2017; Dworkin, 2018; Smart, 2004) comes from cutting data into blocks of generally fixed size (often a power of two between 32 and 512 bits). The blocks are then encrypted one after the other using a special block-chaining method (mode of operation). Several modes exist (Bujari & Aribas, 2017; Dworkin, 2018; Rogaway, 2011; Smart, 2004) with their assets.

1. Electronic CodeBook (ECB).
2. Cipher Block Chaining (CBC).
3. Cipher Feedback (CFB).
4. Output Feedback (OFB).
5. Counter Mode (CTR).

ECB mode is used for transmitting a single value insecure manner, the CBC mode is used for encrypting blocks of text authentication, the CFB mode is used for transmitting an encrypted stream of data authentication, the OFB mode is used for transmitting an encrypted stream of data, the CTR mode is used for transmitting blocks-oriented applications.

In the following, only the two modes of operation will be used in this study: ECB mode and CBC mode.

We assume that the encryption function is denoted E, the decryption function is denoted D and the encryption/decryption key is denoted k (in the case of the secret key cryptosystem).

3.1. Electronic Code Book (ECB)

This mode, code dictionary, is the simplest. Each block is encrypted independently of the others. A random order of the blocks can be introduced to be encrypted, but in return, this mode is very vulnerable to attacks. It can, also, be used for pipelining hardware. The basic diagram will be as in Figure 2 for cipher and as in Figure 3 for decipher, and its cipher (decipher) Equation is in Equation 5.

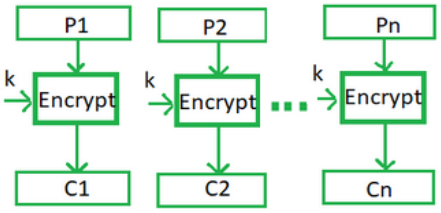


Figure 2. ECB Mode: Encryption Processes

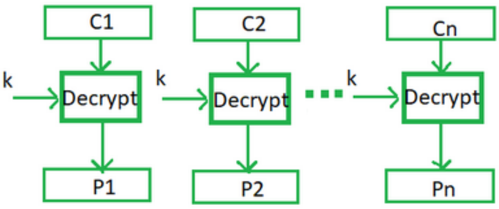


Figure 3. ECB Mode: Decryption Processes

$$\begin{cases} c_j = E_k(p_j) \\ p_j = D_k(c_j) \end{cases} \quad \text{For j= 1…N} \tag{5}$$

This mode is sensitive to “repetitive attacks”: which consist of re-injecting into the system, identical data that was previously intercepted. The goal is to modify the behaviour of the system or repeat actions. For these reasons, this mode is not used in cryptographic applications. The unique advantage of this mode is that it provides quick access to any area of the encrypted text and, the ability to decrypt only part of the data.

3.2. Cipher Block Chaining (CBC)

CBC mode (block sequencing) is the most widely used encryption mode (Ehrsam et al., 1976).

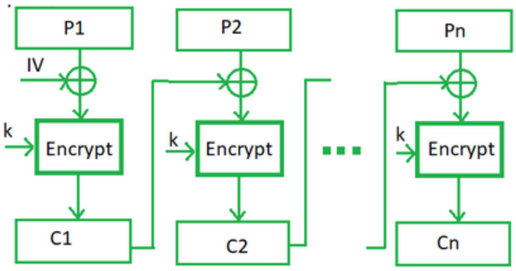


Figure 4. CBC Mode: Encryption Processes

$$\begin{cases} c_1 = E_k(p_1 \oplus IV) \\ c_j = E_k(p_j \oplus c_{j-1}) \end{cases} \quad \text{For } j=2\ldots N \tag{6a}$$

It consists in encrypting a block ***i*** previously combined by or exclusively with the encrypted block of the previous block, the basic diagram will be as Figure 4 for cipher and as in Figure 5 for decipher, and its cipher (decipher) Equation is in Equation 6.

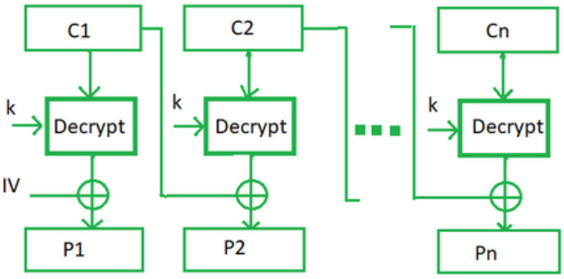


Figure 5. CBC Mode: Decryption Processes

$$\begin{cases} p_1 = D_k(p_1) \oplus IV \\ p_j = D_k(p_j) \oplus c_{j-1} \end{cases} \quad \text{For } j=2\ldots N \tag{6b}$$

Where IV designates an initialization vector. It is a random data block, which allows you to start encrypting the first block and thus provides a random form, independent of the document to encrypt. It does not need to be encrypted itself during transmission, but it must never be re-used with the same key. In this mode, each block is applied an exclusive OR with the encryption of the previous block before it is encrypted itself. In addition, to make each message unique, an initialization vector (IV) is used. One of the recommendations is that the initialization vector changes with each session, and must be transmitted to the recipient, so it is not necessary to encrypt it before sending it; it may be known to the opponent. CBC mode introduces a dependency between two encryption cycles: the cipher obtained at rank (i-1) is used to obtain the cipher of rank (i). Concretely; this c(i-1) cipher is xored (XOR) with block P(i).

3.3. Cipher Braided Long Hair Chaining Chaining Mode (CBLCH)

To mix the data well with each other, we have proposed this new CBLCH mode. In this type of mode, each block I is divided into two parts, the left part and another the right part, the encryption produces in its side a block of two parts left part and right part. The left part is left as the first cryptogram, and a new block (i+1) is formed to be encrypted by two parts, by injecting the right part of the cryptogram i of the previous block into the left part of the block (i+1) and, the right part of the block (i+1) is taken from the plaintext message. The basic diagram will be as

Figure 6 for cipher and as in Figure 7 for decipher, and its cipher (decipher) Equation is in Equation 7.

$$\begin{cases} P_i=(P_{i,1},P_{i,2})Pla\operatorname{int}ext\_value \\ C_i=(C_{i,1},C_{i,2})Cipher\_value \\ I_i=(I_{i,1},I_{i,2})Intermidate\_E.value \\ d_i=(d_{i,1},d_{i,2})Intermidate\_D.value \end{cases}$$

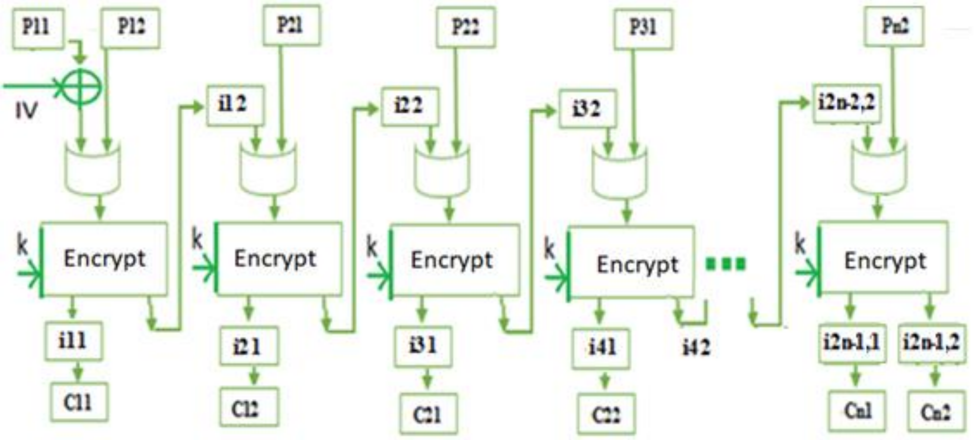


Figure 6. CBLCH mode: Encryption Processes

$$\begin{cases}(I_{1,1},I_{1,2})=E_k(P_{1,1}\oplus IV,P_{1,2})\rightarrow C_{1,1}=I_{1,1}\\ (I_{2,1},I_{2,2})=E_k(I_{1,2}\oplus IV,P_{2,1})\rightarrow C_{1,2}=I_{2,1}\end{cases} \tag{7a}$$

$$(I_{2j-1,1},I_{2j-1,2})=E_k(I_{2j-2,2},I_{j,1})\rightarrow C_{j,1}=I_{2j-1,1}$$
$$(I_{2j,1},I_{2j,2})=E_k(I_{2j-1,2},P_{j,2})\rightarrow C_{j,2}=I_{2j,1} \quad \text{For j=2…N-1}$$

$$(I_{2N-1,1},I_{2N-1,2})=E_k(I_{2N-2,2},I_{N,1})\rightarrow (C_{N,1},C_{N,2})=(I_{2N-1,1},I_{2N-1,2})$$

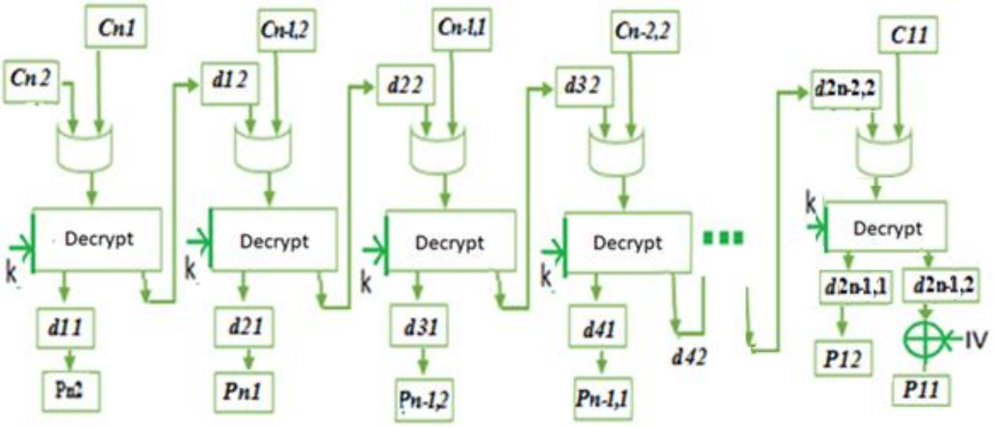


Figure 7. CBLCH mode: Decryption Processes

$$\begin{cases}(d_{1,1},d_{1,2})=D_k(C_{N,2},C_{N,1})\rightarrow P_{N,2}=d_{1,1}\\ (d_{2,1},d_{2,2})=D_k(d_{1,2},C_{N-1,2})\rightarrow P_{N,1}=d_{2,1}\end{cases}$$

$$\begin{cases} (d_{2j-1,1}, d_{2j-1,2}) = D_k(d_{2j-2,2}, C_{N-j+1,2}) \rightarrow P_{N-j+1,2} = d_{2j-1,1} & \text{For j=2…N-1} \\ (d_{2j,1}, d_{2j,2}) = D_k(d_{2j-1,2}, C_{N-j+1,1}) \rightarrow P_{N-j+1,1} = d_{2j,1} & \end{cases} \quad (7b)$$

$$(d_{2N-1,1}, d_{2N-1,2}) = D_k(d_{2N-2,2}, C_{1,1}) \rightarrow (P_{1,1}, P_{1,2}) = (d_{2N-1,2} \oplus IV, d_{2N-1,1})$$

The encryption of a block will be linked to the previous encrypted block. The CBLCH mode introduces a dependency between the encryption cycles: the cipher obtained at rank i-1 is injected in half to obtain the cipher of rank i. concretely, this cipher of c_{i-1} keeps a half for itself and injects the second half block m_i to constitute the c_i cipher of c_{i-1}.

The main feature of this mode is the decryption of the data that is performed from the end of the data to the beginning of the data (First In Last Out of the encrypted data), as if to untie the long hair braid.

4. Validating the CBLCH mode

To validate a cryptographic system, it must pass certain tests successfully (Ali-Pacha et.al., 2020; Chen et. al., 2004).

4.1. Entropy

Claude Shannon brought in Entropy as a mathematical function that corresponds to the quantity of information contained (or delivered) by a source of information.

For a source, which has a discrete random variable Xn symbols, each symbol x_i having a probability P_i of appearing, the entropy H of the source X is defined as:

$$\begin{cases} H(x) = -\sum_{i=1}^{n} p_i.\log_2(p_i) \\ p_i = \frac{k_i}{n} \end{cases} \quad (8)$$

With, i varies from 0 to 255, and n is the number of values generated (n=256*256=65536), k_i corresponds to the frequency of each number i.

A logarithm based on 2 is generally used because the entropy then has the bit/symbol units. The symbols represent the possible achievements of the random variable X.

Consider a source consisting of an alphabet of 256 characters. If these characters are equiprobable, the entropy associated with each character is **$\log_2(256) = \log_2(2^8) = 8$ bits**, which means that it takes 8 bits to transmit a character. The ideal is that the entropy of the encrypted image approaches a source which delivers equiprobable characters.

4.2. Image histogram

For a monochrome image which has a single component, the histogram is defined as a discrete function associating with each intensity value, the number of pixels taking this value. The histogram is therefore determined by counting the number of pixels for each intensity of the image. The histogram can then be seen as a probability density. Histograms are resistant to several transformations in the image (Ali-Pacha et.al., 2020; Chen et.al., 2004). They are invariant to rotations and translations and a lesser extent to changes in perspective and scale.

4.3. Correlation between adjacent pixels

In probability and statistics, studying the correlation between two random variables amounts to studying the intensity of the link that may exist between these variables. In the best case, the link sought is an affine relationship, it is a linear regression. For example, if you want to calculate the correlation coefficient between two series of the same length (typical case: a regression), with the following hypotheses: X:(x_1, ..., x_n) and Y(y_1, ..., y_n) and for each of the two series. **The linear Bravais-Pearson correlation coefficient** (Ali-Pacha et.al., 2020; Chen et.al., 2004) provides a measure of this correlation. The following formula calculates the correlation coefficient linking these two series:

$$coef(X,Y) = \frac{\mathrm{cov}(X,Y)}{\sqrt{D(X)}.\sqrt{D(Y)}} \tag{9}$$

The covariance between x and y is given as follows:

$$\mathrm{cov}(X,Y) = \frac{1}{N}.\sum_{i=1}^{N}((X_i - E(X)).(Y_i - E(Y))) \tag{10}$$

The mean of X : $$E(X) = \frac{1}{N}.\sum_{i=1}^{N} X_i \tag{11a}$$

The mean of Y is : $$E(Y) = \frac{1}{N}.\sum_{i=1}^{N} Y_i \tag{11b}$$

The standard deviation of X is :

$$D(X) = \frac{1}{N}.\sum_{i=1}^{N}\left(X_i - E(X)\right)^2 \tag{12a}$$

The standard deviation of Y is :

$$D(Y) = \frac{1}{N}.\sum_{i=1}^{N}\left(Y_i - E(Y)\right)^2 \tag{12b}$$

The correlation coefficient is included in the Interval [-1, +1]. The intermediate values provide information on the degree of linear dependence between the two variables, the closer the coefficient in absolute value is 1, the correlation between the variables is strong; the closer the coefficient is to the value 0, the correlation between the variables is weak. A correlation equal to 0 means that the variables are not correlated.

1500 pairs of adjacent pixels are randomly chosen both for the plaintext image and the encrypted image, then the two correlation coefficients are calculated from the plaintext image and for its encrypted.

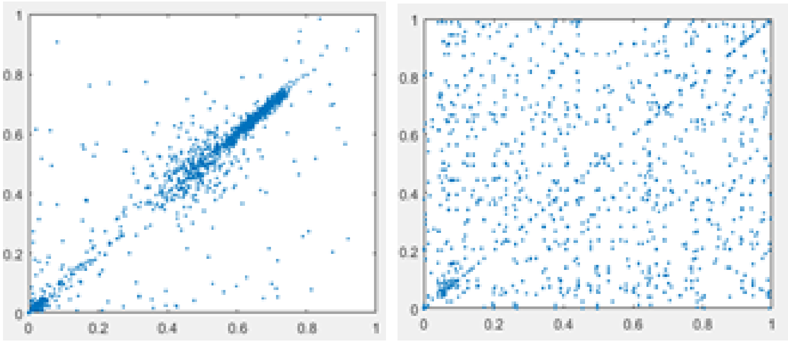


Figure 8a. Plaintext Image **Figure 8b.** Encrypted Image

Figure 8. Correlation between horizontally adjacent pixels

4.4. UACI and NPCR

The NPCR and UACI tests (Wu & Noonan, 2011) make it possible to analyse the resistance of encryption to differential attacks for image encryption. The NPCR and UACI are designed to test the number of changing pixels and the average number of changed intensities between encrypted images that are derived from two same near-plaintext images that differ from each other, usually by a single pixel. These two tests are compactly defined and easy to calculate, the test results are difficult to interpret. For example, the upper limit of the NPCR score is 100%, this means that the NPCR score of a secure cipher should be very close to this limit.

To test the influence of a pixel, change on the image plaint and the encrypted image (Wu & Noonan, 2011), two communes' measurements can be used: number of pixels changed rate (NPCR) and unified changing average intensity.

(UACI). Consider two images, including the corresponding unencrypted (I_o) and encrypted images (I_{enc}), to be noted by I_o and I_{enc}. A bipolar array, D with the same size as the (Io) and (Ienc) images is defined. Then, D(i, j) is determined by I_o(i, j) and I_{enc}(i, j), namely, whether:

$$\begin{cases} I_0(i,j) = I_{enc}(i,j) \rightarrow D(i,j) = 0 \\ I_0(i,j) \neq I_{enc}(i,j) \rightarrow D(i,j) = 1 \end{cases} \tag{13}$$

NPCR is defined as :

$$NPCR = \frac{100\%}{M.N} . \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \tag{14}$$

The NPCR measures the percentage of different pixel numbers between the single image and the encrypted image. UACI is defined as:

$$UACI = \frac{100\%}{M.N} . \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{I_0(i,j) - I_{enc}(i,j)}{255} \tag{15}$$

5. Results and interpretations

Plaintext images and encrypted images of Lena and Cameraman and, with IV=0. will be used.

5.1. Results using Lena image

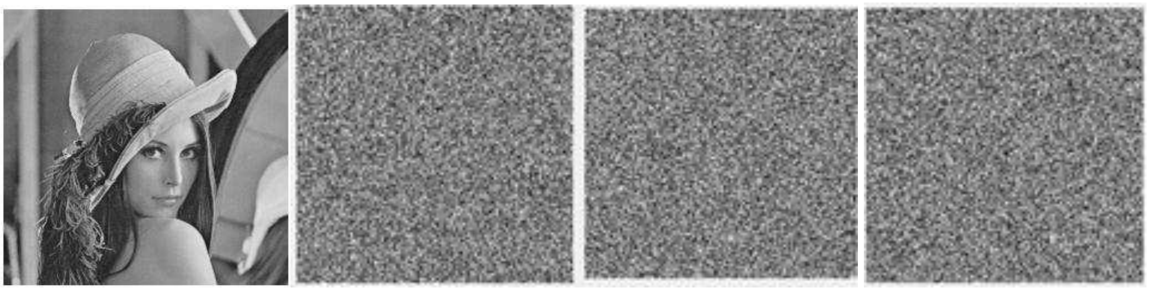


Figure 9a. Lena's Image **Figure 9b.** EBC **Figure 9c.** CBC **Figure 9d.** CBLCH

Figure 9. Lena's image and her encrypted image respectively for different operator modes

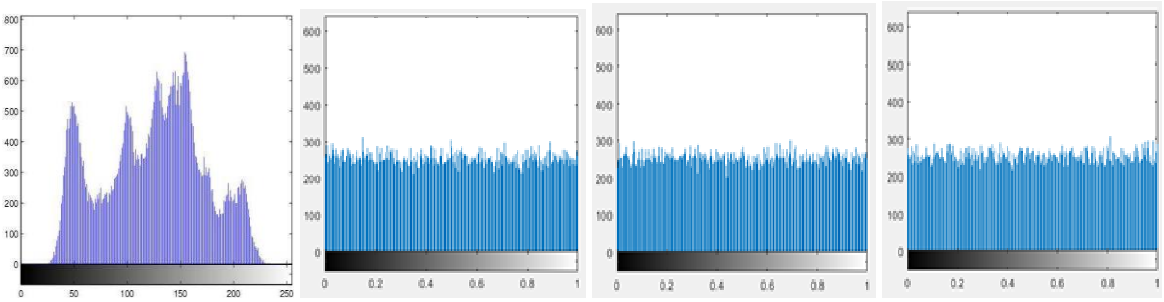
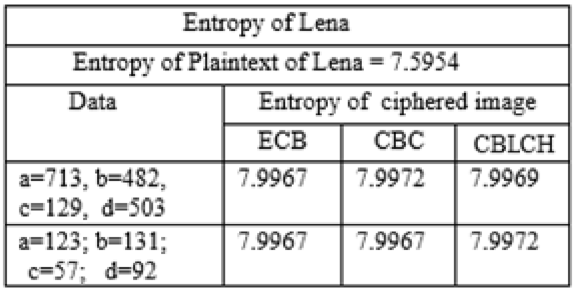


Figure 10a. Lena's histogram **Figure 10b.** EBC **Figure 10c.** CBC **Figure 10d.** CBLCH

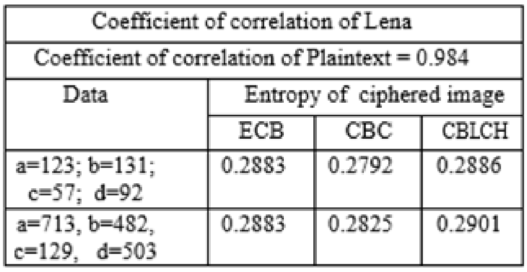
Figure 10. Histogram of Lena's image and its histogram of the encrypted image for different operator modes

Table 1. Entropy of Lena's image and entropies of the encrypted image respectively by ECB, CBC, and CBLCH modes



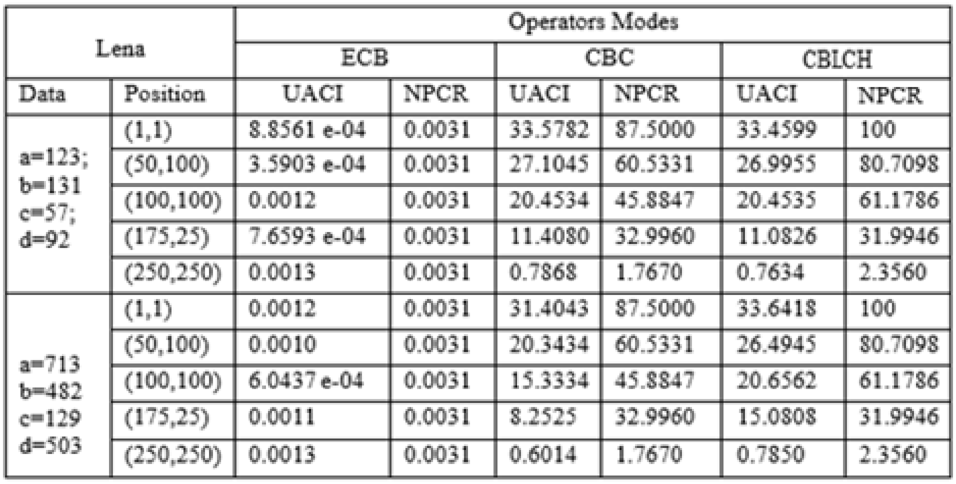
Entropy of Lena			
Entropy of Plaintext of Lena = 7.5954			
Data	Entropy of ciphered image		
	ECB	CBC	CBLCH
a=713, b=482, c=129, d=503	7.9967	7.9972	7.9969
a=123; b=131; c=57; d=92	7.9967	7.9967	7.9972

Table 2. correlation coefficients of Lena's image and the correlation coefficients of the encrypted image by ECB, CBC, and CBLCH modes respectively



Coefficient of correlation of Lena			
Coefficient of correlation of Plaintext = 0.984			
Data	Entropy of ciphered image		
	ECB	CBC	CBLCH
a=123; b=131; c=57; d=92	0.2883	0.2792	0.2886
a=713, b=482, c=129, d=503	0.2883	0.2825	0.2901

Table 3. UACI/NPCR of the Lena image and UACI/NPCR of the encrypted image by ECB, CBC, and CBLCH modes respectively



Lena		Operators Modes					
		ECB		CBC		CBLCH	
Data	Position	UACI	NPCR	UACI	NPCR	UACI	NPCR
a=123; b=131 c=57; d=92	(1,1)	8.8561 e-04	0.0031	33.5782	87.5000	33.4599	100
	(50,100)	3.5903 e-04	0.0031	27.1045	60.5331	26.9955	80.7098
	(100,100)	0.0012	0.0031	20.4534	45.8847	20.4535	61.1786
	(175,25)	7.6593 e-04	0.0031	11.4080	32.9960	11.0826	31.9946
	(250,250)	0.0013	0.0031	0.7868	1.7670	0.7634	2.3560
a=713 b=482 c=129 d=503	(1,1)	0.0012	0.0031	31.4043	87.5000	33.6418	100
	(50,100)	0.0010	0.0031	20.3434	60.5331	26.4945	80.7098
	(100,100)	6.0437 e-04	0.0031	15.3334	45.8847	20.6562	61.1786
	(175,25)	0.0011	0.0031	8.2525	32.9960	15.0808	31.9946
	(250,250)	0.0013	0.0031	0.6014	1.7670	0.7850	2.3560

5.2. Results using cameraman image

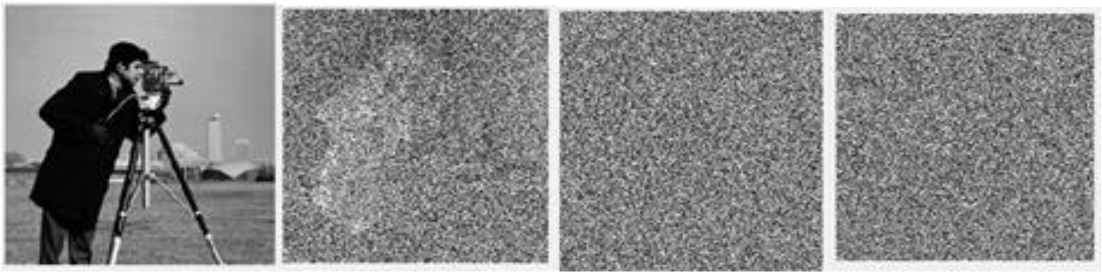


Figure 11a. Cameraman's Image **Figure 11b.** EBC **Figure 11c.** CBC **Figure 11d.** CBLCH

Figure 11. Cameraman image and its encrypted image respectively for different operator modes

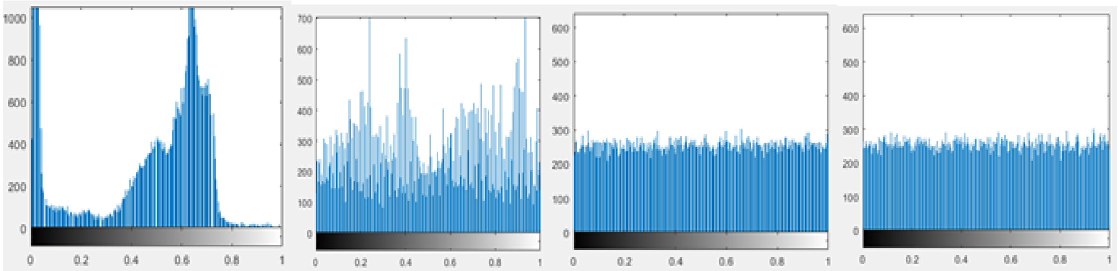
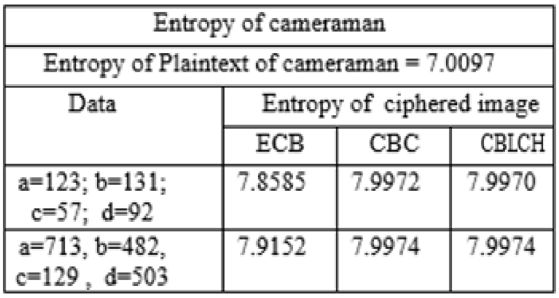


Figure 12a. Cameraman's Histogram **Figure 12b.** EBC **Figure 12c.** CBC **Figure 12d.** CBLCH

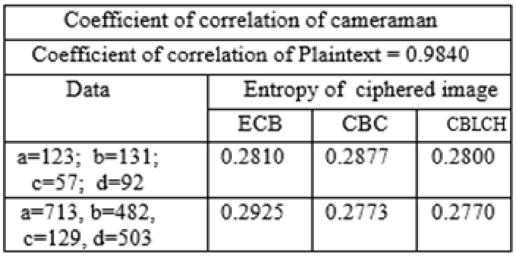
Figure 12. Histogram of the Cameraman image and its histogram of the image encrypted respectively for different operator modes

Table 4. Entropy of the Cameraman image and entropies of the encrypted image respectively by EBC, CBC, and CBLCH modes



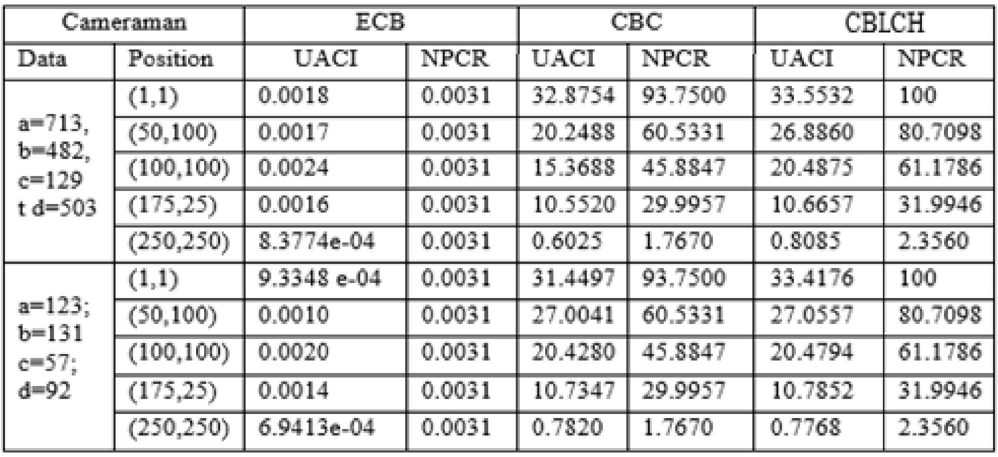
Entropy of cameraman			
Entropy of Plaintext of cameraman = 7.0097			
Data	Entropy of ciphered image		
	ECB	CBC	CBLCH
a=123; b=131; c=57; d=92	7.8585	7.9972	7.9970
a=713, b=482, c=129 , d=503	7.9152	7.9974	7.9974

Table 5. correlation coefficients of the Cameraman image and the correlation coefficients of the quantized image respectively by the EBC, CBC, and CBLCH modes



Coefficient of correlation of cameraman			
Coefficient of correlation of Plaintext = 0.9840			
Data	Entropy of ciphered image		
	ECB	CBC	CBLCH
a=123; b=131; c=57; d=92	0.2810	0.2877	0.2800
a=713, b=482, c=129, d=503	0.2925	0.2773	0.2770

Table 6. UACI/NPCR of the Cameraman image and UACI/NPCR of the encrypted image by ECB, CBC, and CBLCH modes respectively



Cameraman		ECB		CBC		CBLCH	
Data	Position	UACI	NPCR	UACI	NPCR	UACI	NPCR
a=713, b=482, c=129 t d=503	(1,1)	0.0018	0.0031	32.8754	93.7500	33.5532	100
	(50,100)	0.0017	0.0031	20.2488	60.5331	26.8860	80.7098
	(100,100)	0.0024	0.0031	15.3688	45.8847	20.4875	61.1786
	(175,25)	0.0016	0.0031	10.5520	29.9957	10.6657	31.9946
	(250,250)	8.3774e-04	0.0031	0.6025	1.7670	0.8085	2.3560
a=123; b=131 c=57; d=92	(1,1)	9.3348 e-04	0.0031	31.4497	93.7500	33.4176	100
	(50,100)	0.0010	0.0031	27.0041	60.5331	27.0557	80.7098
	(100,100)	0.0020	0.0031	20.4280	45.8847	20.4794	61.1786
	(175,25)	0.0014	0.0031	10.7347	29.9957	10.7852	31.9946
	(250,250)	6.9413e-04	0.0031	0.7820	1.7670	0.7768	2.3560

5.3. Interpretation of the results

Based on the results obtained, it can be said that, the ECB, CBC and CBLCH modes met the following requirements:

1. Referring to the results obtained, the plaintext image in figure 9a and in figure 11a differs significantly from the corresponding encrypted image in figure 9 (b, c and d) and in figure 11 (b, c and d).
2. The histograms of the plaintext images (figure 10a, figure12a) and their encrypted images (figure 10d, figure 12d) show that, the CBLCH mode works correctly. In addition, the histogram of the encrypted images in figure 10 (b, c and d) and, in figure 12 (b, c and d) is uniform which makes it difficult to extract the statistical nature pixels from the simple image.
3. The entropy test from Table 1 and Table 4 suggests that these modes are equivalent uniform (will only be considered CBC and CBLCH modes). The obtained value is very close to the theoretical one (**99.96%).**
4. Table 2 and Table 5 show the correlation between two horizontally adjacent pixels of the plaintext image and its encrypted. It is observed that the neighbouring pixels in the plaintext image correlate (**coeff = 0.984**), while in the encrypted will have one little correlation (**coeff = 0.29**). This low correlation between two neighbouring pixels in the encrypted image makes the attack of the cryptosystem difficult. According to Table 2 and Table 5, the conclusion is that these modes are equivalent.
5. Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks, from Table 3 and Table 6 it is clear that the CBLCH mode is better than the other modes.
6. The graphs in Figure 8 represent the correlation between two horizontally adjacent pixels

of the clear and quantized image. It is observed that the neighbouring pixels in Lena's plaintext image (quantize the values a=713, b=482, c=129 and d=503 and the CBLCH mode) have a strong correlation **(coeff = 0.9844)**, while in the cipher there is some correlation **(coeff = 0.2901.** This low correlation between neighbouring pixels two in the encrypted image makes it difficult to attack our cryptography system. Moreover, it is clear that in the clear image, several straight lines can be fitted to this cloud of points; but among all these lines the one which is an affine line of the form (Y = aX + b) can be retained, thus representing **a linear correlation**.

7. Referring to the all results obtained, show that, the Hill cipher with CBLCH mode works correctly.
8. For a message of N blocks the encryption/decryption with the BHLCH mode takes (2N-1) of times. However, the encryption/decryption with the other two modes EBC and CBC take (N) times.

6. Conclusion

A new mode of operation that can be used in block ciphering. was proposed. This mode is inspired by a **Braided Long Hair braid**. This mode was validated with Hill encryption. The choice of the HILL algorithm is motivated by the simplicity of the description, in this paper, of the principles of encryption and decryption of the algorithm. The DES algorithm was already used in this draft paper, unfortunately, it has a very large number of pages, even with a brief description of the DES, and the same conclusions have been found.

The CBLCH mode introduces additional complexity into the encryption process by creating a dependency between successive blocks that is; the encryption of a block will be "somehow" linked to the previous block(s)/encryption. In addition, the encrypted data are processed in First In Last Out, i.e. to decrypt an image one must start processing the data that arrived last in the first place.

In addition, it was compared to the EBC and CBC modes, which showed that it is robust against differential attacks better than the CBC.

REFERENCES

Ali-Pacha, H., Hadj-Said, N. & Ali-Pacha, A. B. (2020) Data Security based on Homographic Function. *Pattern Recognition Letters*. 129, 240-246. doi:10.1016/j.patrec.2019.10.032.

Blazhevski, A. Bozhinovski, Stojchevska, B. & V. Pachovski, V. (2013) Modes of Operation of the AES Algorithm. *The 10th Conference for Informatics and Information Technology (CIIT 2013)*. https://ciit.finki.ukim.mk/data/papers/10CiiT/10CiiT-46.pdf [Accessed December 08, 2023].

Bujari & Aribas, E. (2017) Comparative Analysis of Block Cipher Modes of Operation. *International Advanced Researches & Engineering Congress, 16-18 November 2017, Osmaniye, Turkey*. http://iarec.osma- niye.edu.tr/ [Accessed December 08, 2023].

Chen, G., Mao, G. Y. & Chui, C. K. (2004) (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*. 21, 749–76. doi: 10.1016/j.chaos.2003.12.022

Dworkin, N. (2018) Recommendation for Block Cipher Modes of Operation, Methods and Techniques. *NIST Special Publication*. 800-38A. U.S. Government Printing Office Washington, Edition 2001. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38a.pdf [Accessed December 08, 2023].

Easttom, C. (2016) *Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education, 505 p.

Ehrsam, W. F., Meyer, C. H. W., Smith, J. L .& Tuchman, W. L. (1976) Message verification and transmission error detection by block chaining. US 4074066A.

Hadj-Said, N., Ali-Pacha, A. B., Ali-Pacha, M. S., Haouas, A. (2011) New Mode of Operation for Cryptography. *RIST Review*. 19(2), 33-48. https://www.ajol.info/index.php/rist/article/view/171247 [Accessed December 08, 2023].

Lester, H. S. (1929) Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*. 36(6), 306-312. doi: 10.1080/00029890.1929.11986963.

Rogaway, P. (2011) Evaluation of Some Blockcipher Modes of Operation. *Cryptography Research and Evaluation Committees (CRYPTREC)*. https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf. [Accessed December 08, 2023].

Smart, N. P. (2004) *Cryptography: An Introduction*. 433 p. McGraw-Hill College, December 30, 2004.

Wu, Y., Noonan, J. P. (2011) NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology. *Journal of Selected Areas in Telecommunications (JSAT)*. 31-38.

Hana ALI-PACHA, has a PhD in Telecommunication option Cryptography and Data Security from, University of Sciences and Technology of Oran Mohamed Boudiaf (USTOMB), Algeria in April 2021. She received the diploma of Master II of Cryptography and Data Security in June 2016. Her research interests are in cryptography, wireless networks and systems security.

Adda Belkacem ALI-PACHA was born in Algeria. He received an engineering degree in telecommunications from the National Institute of Telecommunications and Information and Communication Technologies of Oran - Algeria (NITICTO) in 1986. Also, he got a university degree in mathematics in 1986 and a magister in signal processing in November 1993. Later he obtained a Ph.D. in safety data in 2004. He is a Full Professor in the Electronics Institute at the University of Sciences and Technology of Oran Mohamed Boudiaf (USTOMB), Algeria. The Telecommunication domains are his favourite interest fields research, his other research interests are coding, cryptography and security, and FPGA.

Naima HADJ-SAID was born in Algeria. She received an engineering degree in telecommunications from the National Institute of Telecommunications and Information and Communication Technologies of Oran - Algeria (NITICTO) in 1986, a magister degree from NITICTO in (1992) and a PhD from the University of Sciences and Technology of Oran Mohamed Boudiaf (USTOMB), Algeria in 2005. Now, she is a Full Professor at the Computer Sciences Department of the University of Sciences and Technology of Oran Mohamed Boudiaf (USTOMB), Algeria. Her interest research is in the area of Digital Communications, and cryptography, her other research interests are coding, and security.