Crypto-Imagery

Image & Video

Y. Benlcouiri, M. C. Ismaili, A. Azizi

Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University, Oujda, Morocco.

(benlcouiriy, mcismaili, abdelmalekazizi)@yahoo.fr

Abstract. This paper is structured on securing of storage, transmission and the traceability of digital images. It consists in the design of the cryptographic algorithms appropriate to the case of fixed and moving images.
In this sense, we have introduced two approaches that is different in the synthesis of confusion and diffusion on using the principles of substitu-tion and/or transposition to secure JPEG and MPEG format.

1 Introduction

Before the emergence of the web and the expansion of the need for sharing of multimedia documents in many types of applications, namely, tele- medicine, IPTV, Video on Demand (VOD), video conferencing or private military ... the need for security became a major issue. To this effect, the computer security is called to its indispensable tool which is the crypto in order to guarantee those documents a secure in content.

The algorithms of modern cryptography such as AES, DES or RSA... Show all of the problems facing the image coding by loss of information. In effect, the loss of a single bit of an encrypted message during compression deteriorate the entire block when its decryption. Therefore, the encrypted images by these algorithms cannot undergo the procedures of irreversible compression, and have other problems of slow, even when it is to encrypt the images in their compressed form. In addition, the crypto in his native approach to encrypt all of the documents does not seem suited to the particular case of pictures and video, especially, when it comes to the applications in real time.

As well, to respond to these problems, we have proposed solutions that are based on linear applications of the type (ax+b), to perform operations of substitution and/or dissemination. What guarantee a processing time more optimal than the standards of encryptions, which are based on power calculations such as the RSA, EL-Gamal ¦ or those who clutter the numbers of rounds such as the DES, AES etc. On the other hand, for cohabitation between the crypto and compression algorithms by loss of information, in their format the most popular JPEG and MPEG. In this sense, we propose to retain only the operations of transposition on the blocks already processed by the JPEG algorithm. This leaves each of the algorithms operate independently of the processing space of the other. In effect, the JPEG performs loss of information at the block level, and then the algorithm that we propose does not affect their content. In addition, it changed their location. However, the transposition seems to be well suited to this type of problems, except that its security is not based only on the complexity of the algorithm used, but given on semantic vulnerabilities related to the reconstruction of a puzzle, without having recourse to the encryption algorithm and/or those of decryption.

To illustrate the solutions that we propose. In what follows, we sit in a first time, the preliminary mathematics needed for the construction of our two crypto-systems. And then, we will present the foundation of each of our two cryptographic applications and their implementation algorithmic. Then, we will describe their mode of use on images in the JPEG format and the MPEG video. As well as the results obtained after the application of each of them. Finally, we will conclude our chapter by a general balance on the different algorithms proposed.

2 The Affine-Crypto

Since all the operations in crypto manifest themselves as either a substitution is a transposition or a mix of the two, we present below one of the crypto-systems developed in the work of this thesis. These works are based on the affine application which allows you to carry out, at the time, substitution and permutation. The difference between these two operations resides in the space on which they operate.

While the substitution is restricted to the number of symbols in the space of the representation, transposition, as to it, is related to the length

of the message. We propose the application of these two operations on the images and video, using the applications following again:

2.1 The affine Substitution:

Buried since the early work of Al-Kindi by the analysis of the frequencies of the occurrence of the letters in the languages. The mono-substitution (substituting mono-alphabetic) no longer constituted that a problem of transcoding on the frequency of occurrence of the latter, even if we would have a chain of substitution from a true randomization. That said, in the case of images, is there a rule of the appearance of the colors? Without forgetting that the image is regarded as the universal language that can express his miles words in the different languages that exist... This observation led us to carry the principle of the affine encryption since the ring toward $\mathbb{Z}/26\mathbb{Z}$ the one in $\mathbb{Z}/256\mathbb{Z}$ order to adapt it to the case of the image.

Encryption:.

Either n the number of symbols in the space of the representation (all distinct). It is called substitution refines the application **S**, which at a x given, match an image $\overline{x}$. The function S is définie as follow:

$$\begin{array}{rccc} \mathbf{S}: & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x & \rightarrow & a \times x + b mod(n) \end{array}$$

Or: The pair (a, b) represents the key of the substitution such that a $\in$ $(\mathbb{Z}/n\mathbb{Z})^*$ and; b $\in$ $\mathbb{Z}/n\mathbb{Z}$

Then that x is the value of the plaintext message, which will be replaced by its corresponding $\overline{x} = S(x)$.

Decryption:.

The reverse proxy $\mathbf{S}^{-1}$ is an application that has to vacation to give each $\overline{x}$ its clear value x. OF or the formal definition of $\mathbf{S}^{-1}$ is:

$$\begin{array}{rccc} \mathbf{S}^{-1}: & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ & \overline{x} & \rightarrow & (\overline{x} - b) \times a^{-1} mod(n) \end{array}$$

Or: a^{-1} is the inverse of the a in $\mathbb{Z}/n\mathbb{Z}$, that was calculated by the algorithm of Euclid extended such that ,$(a \times a^{-1}) - (k \times n) = 1$ and the decryption key is the pair. (a^{-1}, b)

2.2 The Transposition affine:

It is based on the problem of the reconstruction of the puzzle, which belongs to the family point unresolveable, and the unconditional safety that can offer any system of transposition. In what follows, we will introduce the affine function on which rests our system of transposition.

Encryption.

Either n the length of the message, and the transposition affine is obtained by the application of the function defined T below on each of the indices of the initial vector $V = \{0,1,2 \dots n-1\}$to find its corresponding. $V' = \{T(0), T(1), T(2) \dots, T(n-1)\}$

$$\begin{array}{rccc} \mathbf{T}: & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x & \rightarrow & a \times x + b mod(n) \end{array}$$

Or: (a, b) is the key (encryption) transposition avecet, $a \in \mathbb{Z}/n\mathbb{Z}^* b \in \mathbb{Z}/n\mathbb{Z}$

And x is the index of a component of the message which will be rearranged in a new location. $T(x)$

Decryption.

The rearrangement (or decryption) of the message in its format non-noisy, is achieved by applying the transpose function reverse $\mathbf{T}^{-1}$ on each of the indices of the blocks of the encrypted message. This function is defined as follows:

$$\begin{array}{rccc} \mathbf{T}^{-1}: & \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x & \rightarrow & (x-b) \times a^{-1} mod(n) \end{array}$$

Or: a^{-1} is the inverse of a in$\mathbb{Z}/n\mathbb{Z}$, that was calculated by the algorithm of Euclid extended, such as:$(a \times a^{-1}) - (k \times n) = 1$ Thus the decryption key is the pair. (a^{-1}, b)

Key Space :

The key space is considered as one of the essential pillars on which rests the safety of crypto-symmetric systems. In this sense, the key space of each of the applications presented below is of possible keys $\varphi(n) \times n$ in the general case. In conclusion:

- The substitution: is an application that operates on a space of a fixed size $\mathbb{Z}/256\mathbb{Z}$ in the case of images. What rounded the number of keys to $\varphi(256) \times 256 =$
- The transposition: in se mode of operation the number of keys varies depending on the size of the message (or image) and remains in its general format$\varphi(n) \times n$, such as the number of n blocks in the message.
- Mixed=alternative+transposition: incorporate the two applications would lead to the multiplication of the number of keys in each of them either of $(\varphi(n) \times n) \times (\varphi(256) \times 256)$

These results do that condemn the dictated of Shannon in these work on the information theory, which considers that the substitution does not offer a good level of security, but may increase one of a system by transposition.

2.3 Affine Algorithm

In this section, we present the implementation of the mathematical concepts of the crypto-affine under algorithmic form. The algorithms of encryption and decryption are formulated as follows:

Encryption Algorithm:.

Variable:

- s =Number of symbol s in the space of the representatives,
- t =The length of the message ,
- $\overline{m}$ = The encrypted message ;

Entry:

- m =Message (or image),
- (a, b) =The surrogate key with $a \in \mathbb{Z}/s\mathbb{Z}^*$and,$b \in \mathbb{Z}/s\mathbb{Z}$
- (c, d) =The keyof permutation and$c \in \mathbb{Z}/t\mathbb{Z}^*$;$d \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

- For i=0 to not of 1 up to t
  // * Substitution & Transposition * //

$\overline{m}[(c \times i + d) mod(t)] = a \times m(i) + b \ mod\ (s)$

- End for

Finish.

The inverse algorithm which performs the phase of the decryption is of the following form:

Algorithm for decryption:.

Variable:

- s =Number of symbol s in the space of the representatives,
- t =The length of the message ,
- m = The encrypted message ;

Entry:

- $\overline{m}$ =Message (or image),
- (a^{-1}, b) =The surrogate key with $a \in \mathbb{Z}/s\mathbb{Z}^*$ and,$b \in \mathbb{Z}/s\mathbb{Z}$
- (c^{-1}, d) =The key to swap $c \in \mathbb{Z}/t\mathbb{Z}^*$ and;$d \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

- For i=0 to not of 1 up to t
  // * Substitution & Transposition * //
  $m[(i - d\ )a^{-1} mod(t)] = (\ \overline{m}(i) - b\ ) \times a^{-1}\ mod(26)$
- End for

Finish.

Complexity.

The complexity of each of the algorithms in terms of the speed of execution is of two multiplication operations and two other of addition (resp subtraction), more than a single assignment operation, which will turn the execution of our method in operations such as $5 \times tt$ is the size of the message. OF or the confirmation of the polynomial complexity of our algorithm which is in $(5 \times t) \in \theta(t)$.

However, the crypto-affine, seems to be well adapted to the particular case of pictures and video. In effect, the capacity of the data processing is the asset of the substitution in the color world. In addition, it remains

vulnerable to the number of combinations that can generate an application affine. In effect, this last is proportional to the number of possible keys either of keys $\varphi(n) \times n$.

Knowing that the number of possible combinations of a set n and. The question asked is: Is there an application that allows you to pull a combination among the $n!n!$ combinations that exist?

To answer this question, we have put in place a new solution based on the algebraic structure defined in the section that follows.

3 New form algebraic

To remedy the problems of the crypto-affine as regards the number of combinais he can offer, we have proposed a new function which is capable of generating all possible permutations on a set of n elements, either of combinations. $n!$ This function is defined on a structure of type $\mathbb{Z}/n\mathbb{Z} - \{0\}$ in which our function is constructed as follows:

$$\begin{array}{rccc} \boldsymbol{B}_{(a,b)}: & \mathbb{Z}/n\mathbb{Z} - \{0\} & \rightarrow & \mathbb{Z}/n\mathbb{Z} - \{0\} \\ & x & \rightarrow & \begin{cases} b & si \quad a \times x + b = 0 \; mod\; (n) \\ sinon & a \times x + b \; mod\; (n) \end{cases} \end{array}$$

Or the couple has$(a, b)$for conditions: $a \in \mathbb{Z}/n\mathbb{Z}^*$et.$b \in \mathbb{Z}/n\mathbb{Z}$

The number of possible keys on this function $\boldsymbol{B}_{(a,b)}$ is equal to that of a affine application, since the conditions on the parameters (or keys) (a, b) remain the same, or the $\varphi(n) \times n$ possible keys.

The major difference between this new function $\boldsymbol{B}_{(a,b)}$ and the applications affines presented in section crypto-affine, is evident in the fact that composed of , which $\boldsymbol{B}_{(a,b)} \circ \boldsymbol{B}_{(c,d)}$on the contrary applications affine or $S\ T$ whose composed always remains on the $\varphi(n) \times n$ case possibles. The function $\boldsymbol{B}_{(a,b)}$with respect to it, under certain conditions on the keys, allows us to go further to generate more that $\varphi(n) \times n$ permutations, see all the combinations of a set of n elements.

Therefore, there is a condition to satisfy on the keys, so that the result of the composed either:

$$\boldsymbol{B}_{(a,b)} \circ \boldsymbol{B}_{(c,d)} \neq \boldsymbol{B}_{(i,j)} \forall i\ , j\ tel\ que\ i \in \mathbb{Z}/n\mathbb{Z}^* \text{et}\ j \in \mathbb{Z}/n\mathbb{Z},$$

This means that the compound is outside the suites accessed by a single application. For this to be possible, the conditions to be respected on the k couples of keys (a_k, b_k) which are succeeding each other in a composition of the form $\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)} \ldots \circ \boldsymbol{B}_{(a_k,b_k)}$ are:

Either$(a_i, b_i) \in (\mathbb{Z}/n\mathbb{Z}^*, \mathbb{Z}/n\mathbb{Z})$ pour i = 1,2,3 …. k

$$\begin{cases} a_1 \neq a_{\mathrm{k}}^{-1} \text{and } a_i \neq a_{\mathrm{i+1}}^{-1} \text{ pour toute element i, tel que } i = 1,2 \ldots k-1 \\ -b_{i-1} \neq a_{\mathrm{i}}^{-1} b_i \text{ for } 1 < i \leq k \text{ and } -b_k \neq a_1^{-1} b_1 \end{cases}$$

Example of use on the body: $\mathbb{Z}/5\mathbb{Z} - \{0\}$

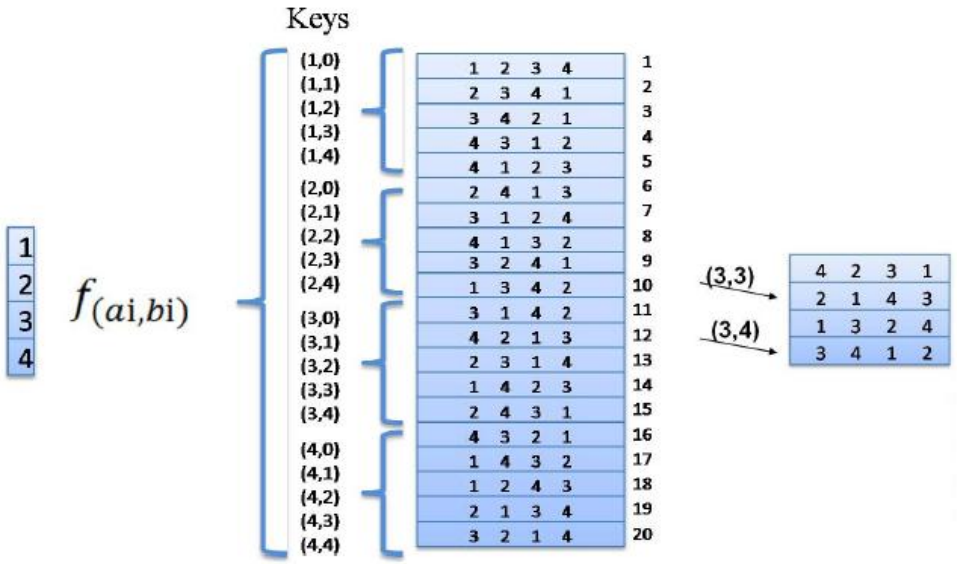


Fig. 1. Illustrative Example of the application of the function B to generate the (**4**!) permutations.

Key Space.

The difference between the space of keys on the applications further affine and the new application resides in the fact that, the applications further refinement (crypto-affine) are limited to the number of possible keys, whereas, on the method, the number of keys is relatively linked to r the number of composed of $\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)}$, if it assumes that:

$$(\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)})^r = \underbrace{\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)} \circ \dots (\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)} \circ (\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)}))}_{r\ fois},$$

With (a_1, b_1) and which satisfy (a_2, b_2) the conditions presented above. In this case the number of keys is of $(\varphi(n) \times n)^r$;

Has this fact, the number of keys can be input according to the number and type of compound used ; simple in the case $B^r_{(a_1,b_1)}$, or complex . $(\boldsymbol{B}_{(a_1,b_1)} \circ \boldsymbol{B}_{(a_2,b_2)})^r$ As well the number of keys can achieve the use of all the composite applications possible, either of $(\varphi(n) \times n)(\varphi(n) \times n)$ which is greater than $n!$. That said, the number of keys is greater than the number of possible messages. Thus, it highlights the conditions of a crypto-perfect system which satisfies the conditions of Shannon on a simple system of transposition (or broadcast). In effect, all systems of permutation are of unconditional safety (the entropy of the message clear = the entropy of the encrypted message). We add through the offered function the fact that the number of possible keys is greater than the number of possible messages.

After having justified the theoretical basis for this type of applications and demonstrated its usefulness on the example above. In what follows, we will present the algorithms that use this feature to build the same synthesis than that presented in crypto-affine, and which consists of operations of substitution and transposition.

3.1 Algorithm $\boldsymbol{B}_{(a,b)}$

The procedures for encryption and decryption that use the new construction $\boldsymbol{B}_{(a,b)}$ are formulated as follows:

Encryption Algorithm:

The algorithm provides, below, allows you to perform, at the time, the operations of substitution and transposition. The two couples of keys (a, b) and shall be used, respectively, to perform the substitution and transposition by the application of the function. The key neutral (1.0) can be used when one wants to ignore one of the two operations. (c, d) $\boldsymbol{B}_{(a,b)}$

Variable:

- $s =$ Number of symbol s in the space of the representatives**+1**,
- $t =$The length of the message**+1**,
- $\overline{m} =$ The encrypted message ;

Entry:

- $m =$Message (or image),
- $(a, b) =$The surrogate key with $a \in \mathbb{Z}/s\mathbb{Z}^*$ and,$b \in \mathbb{Z}/s\mathbb{Z}$
- $(c, d) =$The key to swap $c \in \mathbb{Z}/t\mathbb{Z}^*$ and;$d \in \mathbb{Z}/t\mathbb{Z}$

Beginning:

- For i=1 to not of 1 up to t
  // * Substitution & Transposition * //
  If ( )$a \times m(i) + b \ mod\ (s) == 0$
  Then
  If ( )$c \times i + d\ mod(t) == 0$
  $\overline{\mathrm{m}}[\mathrm{d}] = \mathrm{b}$
  Otherwise
  $\overline{\mathrm{m}}[(\mathrm{c} \times \mathrm{i} + \mathrm{d})\mathrm{mod}(\mathrm{t})] = \mathrm{b}$
  End of If
  Otherwise
  If ( )$\mathrm{c} \times \mathrm{i} + \mathrm{d}\ \mathrm{mod}(\mathrm{t}) == 0$
  Then $\overline{m}[d] = a \times m(i) + b \ mod\ (s)$
  Otherwise
  $\overline{m}[(c \times i + d)mod(t)] = a \times m(i) +$
  $b \ mod\ (s)$
  End of If
- End for

Finish.

Algorithm for decryption.

The inverse function of the encryption process is defined as follows :

$$B_{(a,b)}^{-1}: \quad \mathbb{Z}/n\mathbb{Z} - \{0\} \quad \rightarrow \quad \mathbb{Z}/n\mathbb{Z} - \{0\}$$

$$x \quad \rightarrow \quad \begin{cases} (-b)a^{-1} \quad si \quad (x-b) \times a^{-1} = 0 \; mod \; (n) \\ sinon \quad (x-b) \times a^{-1} mod \; (n) \end{cases}$$

Or: a^{-1} is the inverse of a that is calculated by the algorithm of Euclid extended.

Thus the pseudo code algorithmic of the function of decryption $B_{(a,b)}^{-1}$ is given as follows:

Variable:

- s =Number of symbols in the space of the representatives**+1**,
- t =The length of the message**+1**,
- m = The encrypted message ;

Entry:

- $\overline{m}$ =Message (or image),
- (a^{-1}, b) =The surrogate key with $a \in \mathbb{Z}/s\mathbb{Z}^*$ and,$b \in \mathbb{Z}/s\mathbb{Z}$
- (c^{-1}, d) =The key to swap $c \in \mathbb{Z}/t\mathbb{Z}^*$ and;$d \in \mathbb{Z}/t\mathbb{Z}$

Beginning:

- For i=1 to not of 1 up to t
  // * Substitution & Transposition * //
  If ( )$(\overline{m}(i) - b) \times a^{-1}) \; mod \; (s) == 0$
  Then
  If ( )$(i - d) \times c^{-1} mod(t) == 0$
  $m[(-d) \times c^{-1} mod(t)] = (-b) \times a^{-1} mod(s)$
  Otherwise
  $m\,[(i - d) \times c^{-1} mod(t)] = (-b) \times a^{-1} mod(s)$
  End of If
  Otherwise
  If ( )c × i + d mod(t) == 0
  Then
  $m\left[(-d) \times c^{-1} mod(t)\right] = a \times \overline{m}(i) + b \; mod \; (s)$S
  Otherwise

$$m\,[(i-d)\ \times c^{-1} mod(t)] = a \times \overline{m}(i) + b\ mod\ (s)$$

End of If

- End for

Finish.

We have just to illustrate the fundamental concepts of the general case of two crypto-systems developed during the work of this thesis. In the following, we will present the use cases appropriate for the image and to the video.

4 Algorithm & Application to the image

In their nature, the image and the video are sighted as puzzles of pixels. That said, the reorganization of parts (pixel) is returned directly to the problem of the puzzle. Therefore, we will use this fact to propose the algorithms of the crypto-affine and of the function B on this particular type of data. And then, after having shown the results of the application on different types of keys, we will be arranging a list of recommendations for the use of our two Crypto-systems on this type of documents.

4.1 Crypto-Image

The algorithms for encryption and decryption of the crypto-system affine and B, in their general form, can be applied directly on any data type. In the case image, it is sufficient for the present in the form of a vector of pixels to one of the crypto-systems affine, or the one that uses the function B. However, as we will see on the section dedicated to the presentation of the results, even if this mode of operation provides a run time reasonable enough (proportional to the size of the image), it calls into question all the problems of its predecessors AES, DES, etc. those linked to the loss of information during the compression phase, which leaves the use of our two crypto-systems, in the naive form (already presented), is limited to the case of documents which are being cut back without loss of information. To do this, we will propose another variant of the use of each of the applications further affine and the function B to meet the needs of the compression by loss of information and thus reduce the number of operations in encryption and decryption which will

be proportional to the number of elements in the new structure of the puzzle.

In this new form of use of affine functions and B, which is more adapted to the case image, we propose to omit the substitution operation. Thus the algorithms of encryption and decryption that use the synthesis of the puzzle are illustrated in the following sub-sections:

4.2 Algorithm of the Crypto-Image:

As already mentioned, the image is a puzzle of pixels. In based on this note we propose the algorithms of encryption and decryption that use the crypto-affine and the function B to transpose blocks of pixels in order to produce disorder on the puzzle in treatment. The two methods are flexible enough to choose if the transposition is done by fixing the size of blocks in the puzzle (for the needs of compression) or, to set the number of elements in the puzzle to guarantee an execution time fixed.

In what follows, we present the pseudo code of the algorithms for encryption and decryption of each of the two crypto-systems by omitting the substitution operations.

Algorithm of Cryptage-Affine -Image.

The encryption algorithm-affine, which operates on the pieces of the puzzle (image blocks) is defined as follows:

Algorithm:

Variable:

- t =The number of elements of the puzzle,
- $\overline{I}_{h,l}$ = The encrypted image ;
- V = The vector of elements of the puzzle
- $\overline{V}$ = The vector of elements of the puzzle in their form transposed

Entry:

- $I_{h,l}$ =Message (or image),
- (a, b) =The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and;$b \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

$V =$ Subdivide the image $I_{h,l}$ in t block ;

- For i=0 to not of 1 up to t
  // * Operation Transposition * //
  $\overline{V}[(a \times i + b) mod(t)] = V(i)$
- End for

$\overline{I}_{h,l} =$ Reconstruct the image by the vector $\overline{V}$;

Finish.

Algorithm for decryption .

The algorithm of decryption is to reorganize the image in its form not noisy. To do this, we find two different ways: The first uses the key inverse $(a, b)^{-1} = (a^{-1}, b)$ on the inverse function of the swap, while the second uses the same key to reassemble in the reverse of the transposition performed by the key(a, b). Thus the algorithm is defined as follows:

Algorithm:.

Variable:

- t =The number of elements of the puzzle ,
- $\overline{I}_{h,l}$ = The encrypted image ;
- $V =$ The vector of elements of the puzzle
- $\overline{V}$ = The vector of elements of the puzzle in their form transposed

Entry:

- $I_{h,l}$ =Message (or image),
- (a, b) =The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and;$b \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

$V =$ Subdivide the image $I_{h,l}$ in t block ;

- For i=0 to not of 1 up to t
  // * Operation Transposition with the key inverse * //
  $V[(x - b) \times a^{-1} mod(t)] = \overline{V}(i)$

// * Operation Transposition without reverse keys * //

$V(i) = \overline{V}\,[(a \times i + b) mod(t)]$

- End for

$\overline{\mathrm{I}}_{\mathrm{h,l}} =$ Reconstruct the image by the vector $\overline{V}$;

Finish.

The algorithm below present exploits the equivalence between the two instructions :

$$et \quad \begin{matrix} V[(x-b) \times a^{-1} mod(t)] = \overline{V}\,(i) \\ V(i) = \overline{V}\,[(a \times i + b) mod(t)] \end{matrix}$$

To do more to appeal to the calculation of inverse of a through the algorithm of Euclid:

Algorithm of the Crypto-B-Image :.

The algorithms of this crypto-system are similar to those of the crypto-affine in their synthesis preprocessing of images (transposition of the pieces of the puzzle). Nevertheless, the latter, as we have shown in its founding party, it can offer a equiprobable permutation on the set of possible combinations.

However we rewrite the algorithms of encryption and decryption of our crypto-system in the following form:

Encryption Algorithm.

Variable:

- t =The number of elements of the puzzle ,
- $\overline{I}_{h,l}$ = The encrypted image ;
- V = The vector of elements of the puzzle
- $\overline{V}$ = The vector of elements of the puzzle in their form transposed

Entry:

- $I_{h,l}$ =Message (or image),
- (a, b) =The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and;$b \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

$V =$ Subdivide the image $I_{h,l}$ in t block ;

- For i=1 to not of 1 up to t
  // * Operation of Transposition * //
  If ( )$a \times i + b\ mod(t) == 0$
  Then
  $\overline{V}[b] = V(i)$
  Otherwise
  $\overline{V}[a \times i + b \bmod(t)] = V(i)$
  End of If
- End for

$\overline{I}_{h,l} =$ Reconstruct the image by the vector $\overline{V}$;

Finish.

The encryption algorithm, present, executes only once the operations of the function B with the key (a,b), whereas, for cluttering up the level of security, it is sufficient to reiterate the algorithm with a key that is the same or not which verifies the conditions laid down in the fundamental part of application B. Thus the algorithm reverse the encryption process is:

Algorithm for decryption.

Variable:

- t =The number of elements of the puzzle,
- $\overline{I}_{h,l}$ = The encrypted image ;
- V = The vector of elements of the puzzle
- $\overline{V}$ = The vector of elements of the puzzle in their form transposed

Entry:

- $I_{h,l}$ =Message (or image),
- (a, b) =The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and;$b \in \mathbb{Z}/t\mathbb{Z}$

Beginning :

$V =$ Subdivide the image into blocks $I_{h,l}$ t ;

- For i=1 to not of 1 up to t
  // * Operation of Transposition Reverses * //
  If ( )$i - b\ mod(t) == 0$
  Then
  $V[(-b) \times a^{-1} mod(t)] = \overline{\mathrm{V}}(\mathrm{i})$
  Otherwise
  $V[(\mathrm{i} - \mathrm{b}) \times \mathrm{a}^{-1}\ \mathrm{mod(t)}] = \overline{\mathrm{V}}(\mathrm{i})$
  End of If
- End for

$\overline{\mathrm{I}}_{\mathrm{h,l}} =$ Reconstruct the image by the vector $\overline{V}$;

Finish.

Similarly that the encryption, the algorithm of decryption provided above, does not use the application B in the case composed. If the encryption was a composed of the function B with different keys (a,b) (c,d) … (y,z) (from left to right), the algorithm of decryption, as to him, must carry out the same operations in the reverse order, going from the right to the left (y,z) … (c,d) (a,b).

After having shown the appropriate algorithms to the implementation of each of our two crypto-systems. In the next section, we will present the results of the application of each of them on different images.

4.3 Results of the Applications of the crypto-images

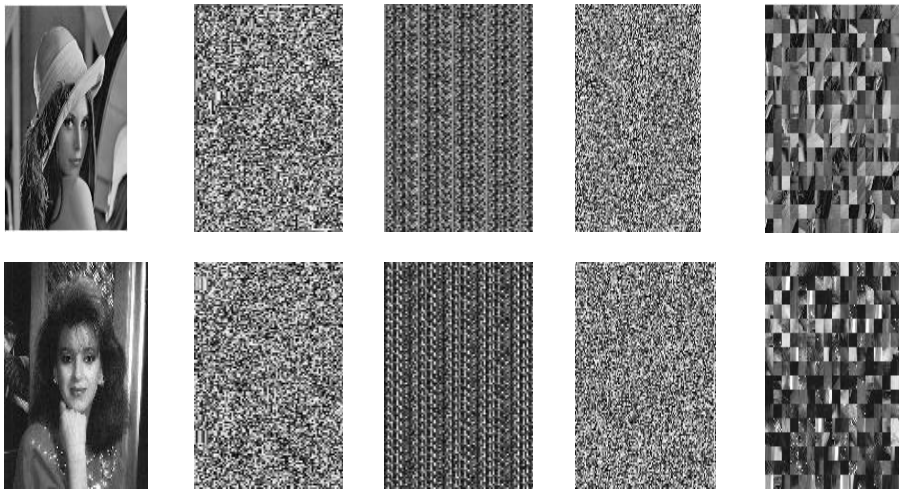
In this section, we present separately the results of the application of each of the crypto-systems proposed, on the different forms of algebraic $\mathbb{Z}/n\mathbb{Z}$. In effect, when n is a prime number, then $\mathbb{Z}/n\mathbb{Z}$ is a body. When n is a composite number, therefore, $\mathbb{Z}/n\mathbb{Z}$ is a ring. More particularly, if $\mathbb{Z}/(n = p)\mathbb{Z}$ and p a prime number, all the elements are reversal film except the zero, of this fact the choice of the key (a, b) on the two applications can be done randomly. It is the form of randomised our two crypto-systems. Otherwise, where n is a number composed the multiplicative part of the key, either $(a, b)a$ must satisfy the constraint. $a\text{^}n \equiv 1$

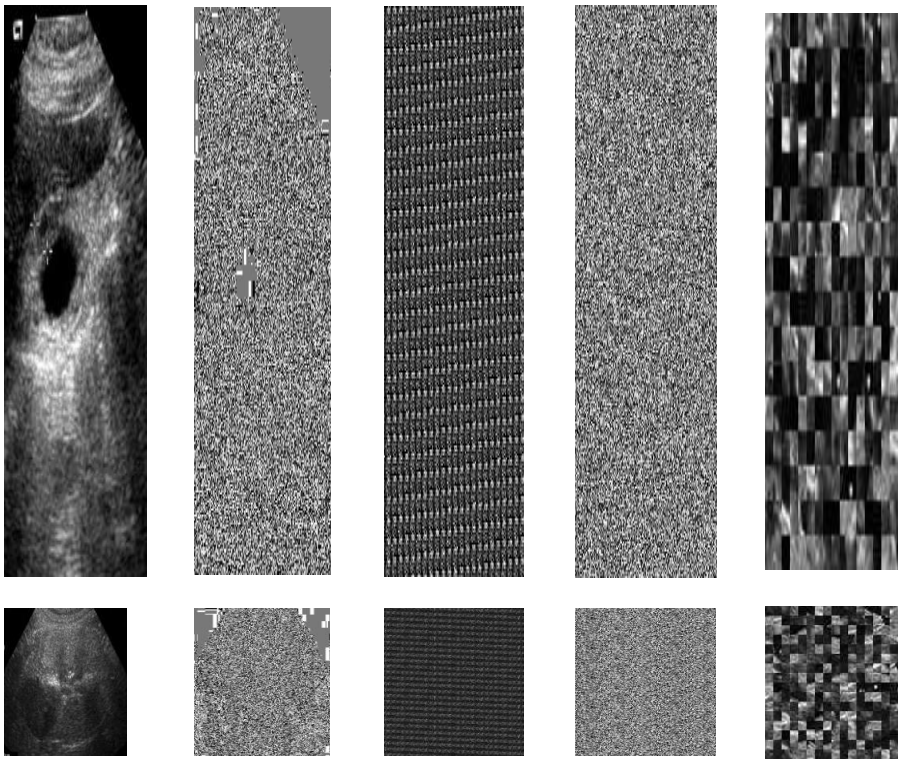
The images that we are presenting, below, are all similar, but differ in the application that it uses affine or B, to perform each of the crypto-

graphic operations, namely, the transposition, substitution or a joint between the two.

Results of the application of the affine crypto:.

We present here, the results obtained after the application of the algorithms that use the application affine on the images Lena and Betty of two different cases. The first case, is to treat the image as a puzzle of pixels (each pixel is a piece of the puzzle) and uses the structure $\mathbb{Z}/(n = 128 \times 128)\mathbb{Z}$, while the second case, imposed the number of parts in the puzzle and used the structure $\mathbb{Z}/(257)\mathbb{Z}$;





(A) *(B)* *(C)* *(D)* *(E)*

Figure 2. : The results obtained after application of chacuine of operations for transposition and substitution and those of their mixing, as well as those of the transposition of blocks of pixels by the keys (133 ; 120) and (155 ; 220) for the transposition by the application affine.

The images presented above, are the result of the application of the crypto-affine in these two approaches: the most naive (puzzle of pixel), which is to deal with the totality of the components of the image by the operations of substitution and(or) those of transposition. note that one of the two operations may be omitted in the use of the key (1.0) (the key neutral). Whereas the beeing aims to subdivide the image into a number of specific parts, to reduce the calculation time in function of the latter. The table below demonstrates the efficacy of the two approaches in calculation time and the keys used for each of the encrypted images.

Image	E. I. O	E. I. S	E. I. Tp	E. I. T-S	E. I. Tb	T. E (ms)			
						S	T	S+T	Tb

Lena(128 * 128)	7.6464	7.5515	7.6464	7.5515	7.6464	3	3	6	2
Betty(128 * 128)	7.3515	7.4386	7.3515	7.4386	7.3515	3	3	6	2
Echo-1	7.3319	7.3315	7.3319	7.3315	7.3319	1.3	0.9	3.2	2
Echo-2	6.7308	6.7308	6.7308	6.7308	6.7308	3.41	4.52	8.01	2

Figure 3. : Comparison between the original images Betty, Lena, Echo-1 and Echo-2 and their encrypted by the transposition and substitution. **E. I. O**: entropy of the Original Image. **E. I. R**: entropy of the Encrypted Image.**T. E:** Time threads in (ms) of the Substitution (**S**) ,Transposition (**T**), their joint (**S+T**) and Transposition by Block (Tb).

The main difference between the two modes of use of the crypto-affine, lies in the fact that the naive approach of the crypto-affine, even quite sure that the one who does that permutes the blocks, it prohibits any form of irreversible compression (with loss of information). While the one who uses blocks of pixels may well coexist with compression algorithms which operate on blocks, such as the JPEG algorithm when the blocks of the puzzle are of size 8×8.

Security.

The security of each of the two approaches based, first, on the cardinal of the key space, which is in $\varphi(n) \times n$ for each of the operations of transposition and substitution. The number of surrogate keys being fixed in $\mathbb{Z}/(256)\mathbb{Z}$ by the space of the representatives which is to values in (0 ,255). Whereas for the transposition, the number of keys is proportional to the number of elements of the puzzle. OF or the number of keys for each of the examples treated is in :

- Substitution: $\varphi(n) \times n = \varphi(256) \times 256 = 32768$;
- Transposition of a puzzle of pixel: $\varphi(n) \times n = \varphi(128^2) \times 128^2 = 8192 \times 16384 = 134217728$ such as $n = h \times l$;
- Transposition of blocks of pixel $\varphi(n) \times n = \varphi(257) \times 257 = 256 \times 257 = 65792.$

However, the naive algorithm, which treaty of the whole image, multiplied the number of keys of the substitution by the number of keys in the operations of the transposition. This offers opportunities to browse by the attacker who wants to reconstruct the image in question by crude force or by using the attacks of oracles alea. Then that for the one who

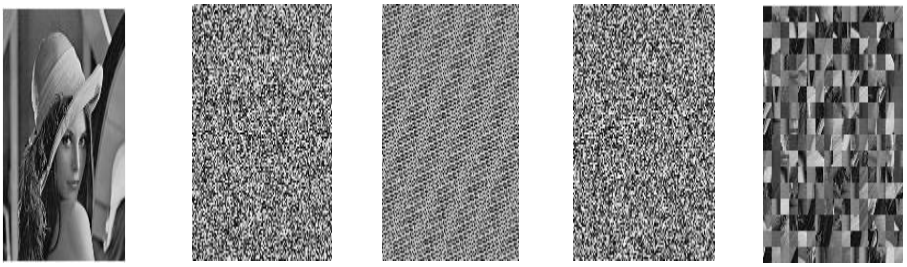
uses only the transposition of blocks of pixels, it is limited to the number of possible transpositions, which is in4398046511104 key 65792, which gives on the problem of semantic reconstruction of the puzzle without knowing its initial state.

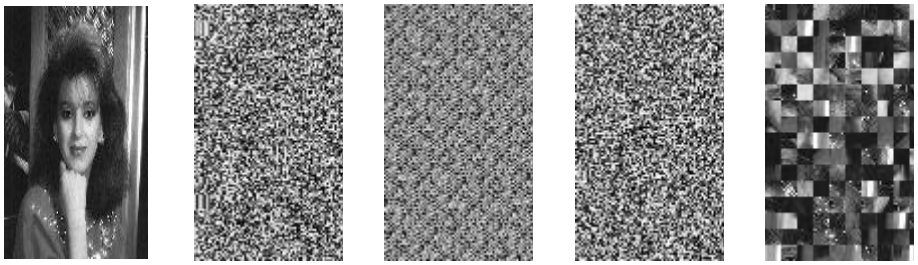
The application of the crypto-affine to images Lena and Betty demonstrates its flexibility to respond to the problems of the crypto-imaging, which focuses primarily on: the processing time, which is in some millisecond, and those linked to the loss of information in the process of irreversible compression. In this sense, and in order to meet the needs compression bandages with a higher level of security, we propose in this which follows the results of the application of the crypto-B on the same images.

Results of the application of the crypto B:.

In what follows, we will apply the function B already defined in section II, on the same algebraic structures used in the example of the affine application, namely $\mathbb{Z}/(n = 128 \times 128)\mathbb{Z}$ to transpose each pixel (puzzle of pixel), and the one $\mathbb{Z}/257\mathbb{Z}$ to perform the transposition of blocks as well as the substitution.

The results below show that they are quite similar to those presented in affine application. However, the latter operates the number of combinations that can be generated by the application B. In fact, the number of combinations is at the time relative to the length (number of parts of the puzzle) of the image and the number of compound used in the function B by following the conditions proposed in its basic definition.





(A) (B) (C) (D) (E)

Figure 4. : The results obtained after application of each of the operations of transposition and substitution and those of their mixing, as well as those of the transposition of the blocks of pixel by the function B.

The table below presents the different keys, measures of quality and the ratio related to each of the processed images above:

Image	E. I. O	E. I. S	E. I. Tp	E. I. T-S	E. I. Tb	T. E			
						S	T	S-T	Tb
Lena	7.6464	7.5515	7.6464	7.5515	7.6464	3	3	6	2
Betty	7.3515	7.4386	7.3515	7.4386	7.3515	3	3	6	2

Figure 5. : Comparison between the original image (Image Betty and Image Lena)and their encrypted by the transposition and substitution. E. I. O: entropy of the Original Image. E. I. R: entropy of the Encrypted Image.T. E: Time threads in Substitution,Transposition, their joint(S-T) and the transposition by blocks.

The results of the last table are the same as the results of the application further affine, the only difference lies in the execution time, which is relative to the number of composed of application B. Even if it appears long enough to cause the number of composed by comparison to that of the affine application. The latter may well be performed in off-line mode (regardless of the message) to thus offer the same treatment time that its previous which meets the needs of the real-time.

Security .

It is this security setting which makes the difference between the application further affine and the new application B. being linked to the number of keys, the safety of this application, as regards the operations

of substitution and those of transposition in the images in treatment (Lena & Betty), is presented as follows:

- Substitution: $\varphi(n) \times n = \varphi(257) \times 257 = 256 \times 257 = 65792$
- Transposition of a puzzle of pixel: $\varphi(n) \times n = \varphi(128^2) \times 128^2 = 134217728$ such as $n = h \times l$
- Transposition of blocks of pixel $\varphi(n) \times n = \varphi(257) \times 257 = 256 \times 257 = 65792$

The number of keys, each of these operations can be increased by powers according to the degree of security research, and which can go up to meet the conditions laid down by Shannon. Especially, if the number of combinations of keys is higher than that of possible messages, then, the attacks by random oracle are impaired.

In the case of the transposition by block of pixels, the degree of security remains the same as that of the affine applications face to all semantic attacks which aim rebuild the puzzle without having recourse to the encryption algorithms and(or) for decryption.

After having presented the results of the application of each of our two crypto-systems, and shows the strengths of each of them in terms of processing time, as well as to cohabit with the algorithms of JPEG compression, or in their randomized aspect which leaves change the key in FTAA. In what follows we will expand the application of these two crypto-systems in the case of video (animated image).

5 The Crypto-video:

Given the real-time processing of images which has our algorithms. In this section we propose to extend the use of our crypto-systems on the case of the video in its most popular format the MPEG. Or, we propose two different approaches: The first is to encrypt the primary image (image Intra) of each group of pictures (GoP structure) of the scene MPEG in treatment. With regard to this second approach, it uses the fact that there is no restriction on the Intra frame in the MPEG algorithm, to assign the role of the latter to one of Predictive images (image-P) of the same GoP.

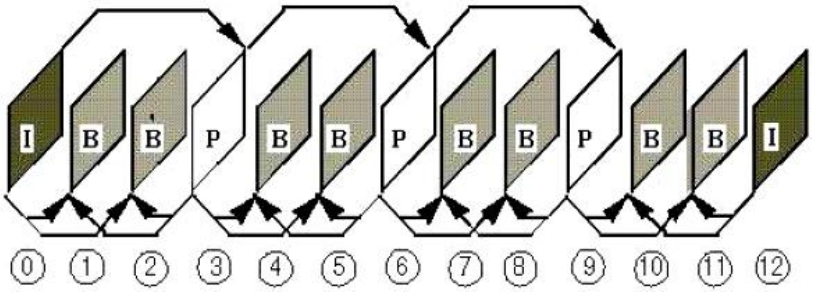


Figure 6. : Diagram of the construction of a GOP in the MPEG algorithm

In what follows, we illustrate the principles and algorithms of encryption and decryption of each of the two proposed approaches, leaving the choice open for the use of one of the two applications affine or B.

5.1 Crypto-video-MPEG

The MPEG format, as it has been presented in chapter I, is a succession of a set of groups of images in english (Group of Pictures). Each GoP rests on a single image called intra to reconstruct the 12 images that the succession. However, we are proposing in our algorithm to encrypt that the intra frame of each GoP. In addition, knowing that the Intra Frame is compressed by the JPEG algorithm and that the latter represents of 40to60% of the size of the GoP, we demand that the parts of the jigsaw are of size $(8 \times 8)$for does not affect the rate of compression of the JPEG algorithm as well as to the quality of the scene treated.

The difference between the algorithms, already presented and the latter, lies in the fact that the imposed upon him the size of the pieces of the puzzle, whereas in the algorithms already presented that were the number of parts. That said, the number of operations is proportional to the number of blocks of size (8×8) on the image. In this case the algorithms for encryption and decryption of the MPEG video of each of our methods are as follows :

Encryption Algorithm.

Variable:

- t =The number of blocks of size in the image (8×8) Intra ;
- $I_{h,l}$ = The Intra frame,

- $\overline{I}_{h,l}$ = The image Intra encoded ;
- V = A vector of blocks ;
- $\overline{V}$ = The vector of blocks in their form transposede
- $\overline{M}_m$ = MPEG Video encryptse ;
- GoP = A vector of group of image ;

Entry:

- (a, b) = The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and;$b \in \mathbb{Z}/t\mathbb{Z}$
- $M_{\{(h,l);m\}}$ = MPEG Video such as h and l are respectively the height and width of the images in the video and m the number of GoP ;

Beginning:

GoP = Extract the m GoP of $M_m$the video presented in betweene ;

- For each GoP(i)
  $I_{h,l}$ = Extract the image Intra of The GoP stock ;
  V = Subdivide the image into blocks of $I_{h,l}$size
  - For i=1 to not of 1 up to t
    // * Operation of Transposition * //
    If ( )$a \times i + b \bmod(t) == 0$
    Then
    $\overline{V}[b] = V(i)$
    Otherwise
    $\overline{V}[a \times i + b \bmod(t)] = V(i)$
    End of If
  - End For
  $\overline{I}_{h,l}$ = Reconstruct the image by the vector $\overline{V}$;
  GoP = Put the image $\overline{I}_{h,l}$ in place of the true Intra $I_{h,l}$;
- End For

Finish.

Thus, a non-authorized user, who does not have the key, will reconstruct the scene of the GoP using the encrypted image, which causes the sound effects of the scene a whole. While those allowed will use the key to (a^{-1}, b) proceed as follows:

Algorithm for decryption.

Variable:

- t =The number of blocks of size in the image (8×8) Intra ;
- $I_{h,l}$ = The Intra frame,
- $\overline{I}_{h,l}$ = The image Intra encoded ;
- V = A vector of blocks ;
- $\overline{V}$ = The vector of blocks in their form transposede
- GoP = A vector of group of images ;

Entry:

- (a^{-1}, b) = The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and; $b \in \mathbb{Z}/t\mathbb{Z}$
- $\overline{M}_m$ = MPEG Video encrypts ;

Output:

- $M_{\{(h,l);m\}}$ = MPEG Video such as h and l are respectively the height and width of the images in the video and m the number of GoP ;

Beginning:

GoP = Extract the m GoP of $\overline{M}_m$Ihas video presents in between ;

- For each GoP(i)
  $\overline{I}_{h,l}$ = = Extract the image Intra of The GoP stock ;
  $\overline{\mathrm{V}}$ = Subdivide the image into blocks of $\mathrm{I_{h,l}}$size
  - For i=1 to not of 1 up to t
    // * Operation of Transposition Reverses * //
    // * Operation of Transposition * //
    If ( )$\mathrm{i} - \mathrm{b} \bmod(\mathrm{t}) == 0$
    Then
    $\mathrm{V}[(-\mathrm{b}) \times \mathrm{a}^{-1} \bmod(\mathrm{t})] = \overline{\mathrm{V}}(\mathrm{i})$
    Otherwise
    $\mathrm{V}[(\mathrm{i} - \mathrm{b}) \times \mathrm{a}^{-1} \bmod(\mathrm{t})] = \overline{\mathrm{V}}(\mathrm{i})$
    End of If
  - End for
  $I_{h,l}$ = Reconstruct the image by the vector V;
  GoP = Put the image $\overline{\mathrm{I}}_{\mathrm{h,l}}$ in place of the true Intra $\mathrm{I_{h,l}}$;

- End For

Finish.

The algorithms listed-present, retain all the properties of those in the party who treaty still images, with one difference. Zn fact, those used here (on the case of the MPEG format) must at once omit the phase of substitution and operate on the puzzle pieces of size 8 * 8, such that operates the JPEG mode. To ensure the perfect reconstruction of the image-I on which is based the whole of the GOP.

The fact that the MPEG algorithm does not present any restriction on the image which must play the role of the pillar of the reconstruction of the GOP (image-I). We find that, we can assign the role of the latter to another of the same GoP. This allows cluttering the degree of security of the method below presented by the number of images that are in competition . In this context, we prefer to base this choice, not on random number generators , but on the compression method introduced by Benabdelleh and al, which offers, at the same time, the possibility to choose one of the images most optimal and a process pseudo-random basis on the content. This is the approach of crypto-compression that we will treat in the section that follows.

5.2 Crypto-compression-of the MPEG format

In this sub-section, we present the use of the same synthesis of encryption already proposed for the video, but which operates on the GoP who have undergoes changes in structure. This change in structure based on the research of the image the best possible among the four images: the Image-I and the other three images-P of the same GoP. The method presented above allows, at the same time, to reduce the size of the GoP when this is possible and cluttering the degree of security of its previous.

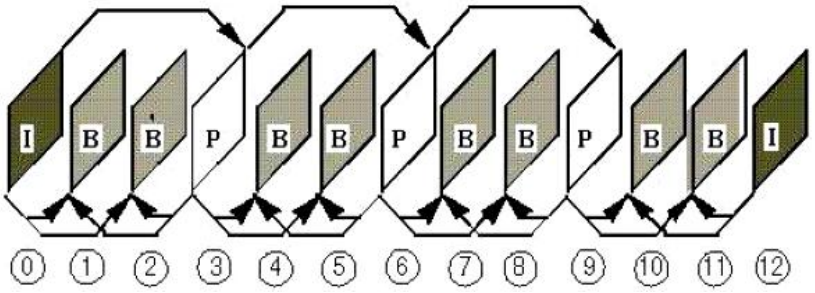


Figure 7. : Diagram of the construction of a GoP after the modification of the reference image of the MPEG algorithm

The criterion for the choice of the reference image of a GoP used on our system of crypto-compression was introduced by Benabdelah and al, where they propose to compare the coefficients of the transformed into wavelet Fabert-Sauder of each of the images: Intra and those who play the role of predictive images on the same GoP, for thus choose the most optimal. The comparison is performed on the coefficients of the transformed into wavelet Fabert-Sauder , she took advantage of the aspect of the multi-resolution of this last for compromising the quality perceptible to the scene which is going to be reconstructed.

Accordingly, the process proposed by the authors is to:

1. Extract the image-I and the images-P
2. Apply the TFM on each of the images
3. Subtract the coefficients of each of the images to all other images.
4. Criterion of choice

   If the results of step (3) only include separate points,

   Then they choose the one that contains the minimum of points

   Otherwise the results contain points in the form of linear curve and other non-linear

   Then they choose the image that holds the minimum distance between the different curves.
5. Reconstruction of the GOP in the new structure to formalize the vectors responsible for new predictive images

After having recalled the process of choice of reference images in the MPEG format. In what follows, we will be arranging a approach of a system of crypto-compression, or the algorithms of encryption and de-

cryption are differentiated from their predecessors (presented in the section), by the keys used. Because on this new approach, it is assumed that the index of the image-I remains secret. Having said that, it is added to the set of keys the index of the reference image chosen by the process of Benabdelah et al. The implementation algorithm is given as follows:

Algorithm of crypo-compression:.

Variable:

- t =The number of blocks of size in the image (8×8) Intra ;
- $I_{h,l}$ = The image Intra,
- $\overline{I}_{h,l}$ = The image Intra encoded ;
- V = A vector of blocks ;
- $\overline{V}$ = The vector of blocks in their form transposed
- V_{indice} = A vector containing the indices of the image-I in the new structure;
- $\overline{M}_m$ = Video MPEG encoded ;
- GoP = A vector of group of images ;

Entry:

- (a, b) = The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and; note that k the index of the new image intra $b \in \mathbb{Z}/t\mathbb{Z}$
- $M_{\{(h,l);m\}}$ = MPEG Video such as h and l are respectively the height and width of the images in the video and m the number of GoP ;

Beginning :

GoP = Extract the m GoP of $M_m$the video presented as input;

- For each GoP(i)
  $V_{indice}(i)$ = Algorithme_de_Benabdelah_et_all
  $I_{h,l}$ = Extract l'ima
  GE $V_{indice}(i)$ of The GoP stock ;
  V = Subdivide the image $I_{h,l}$in block sof size (8×8)
  - For i=1 to not of 1 up to t
    // * Operation of Transposition * //
    If ( )$a \times i + b \bmod(t) == 0$
    Then

$\overline{V}[b] = V(i)$

Otherwise

$\overline{V}[a \times i + b \bmod(t)] = V(i)$

End of If

- End For

$\overline{I}_{h,l} =$ *Reconstruct the image by the vector* $\overline{V}$ *;*

$GoP =$ *Put the image* $\overline{I}_{h,l}$ *in place of the true Intra* $I_{h,l}$*;*

- End For

Finish.

Thus, the user must wait for the end of the process of Benabdelah and al, to know what is the index of the image-I that it will encrypt and add to the key. The new key of each GoP is of the form (a,b,c) or the (a,b) is the key for transposition, and c motionne the location that must take the image-I. The introduction of the index of the image-I, is raise the degree of safety of users who would prefer encrypt all the GoP with the same key. In effect, an attacker who has been unable to break the system of transposition will face problems of synchronization of images in time, since it does not have the location that must take the image-I. In addition, the key used in the decryption process must mention the location that should take the image decrypted, so to rebuild the GoP. The decryption key will become (a-1, b, c] that we used on the following algorithm:

Decoding Algorithm crypto-wound:.

Variable:

- t =The number of blocks of size in the image (8×8) Intra ;
- $I_{h,l}$ = The image Intra,
- $\overline{I}_{h,l}$ = The image Intra encoded ;
- V = A vector of blocks ;
- $\overline{V}$ = The vector of blocks in their form transposed
- V_{indice} = A vector containing the indices of images-I in the new structure;
- $\overline{M}_m$ = Video MPEG encoded ;
- GoP = A vector of group of image ;

Entry:

- $(a, b) =$ The key to swap $a \in \mathbb{Z}/t\mathbb{Z}^*$ and; note that k the index of the new image intra $b \in \mathbb{Z}/t\mathbb{Z}$
- $M_{\{(h,l);m\}} =$ MPEG Video such as h and l are respectively the height and width of the images in the video and m the number of GoP ;

Beginning :

$GoP =$ Extract the m GoP of M_m the video presented as input;

- For each GoP(i)
  $V_{indice}(i) =$ Algorithme_de_Benabdelah_et_all
  $I_{h,l} =$ Extract l'ima
  GE $V_{indice}(i)$ of The GoP stock ;
  $V =$ Subdivide the image $I_{h,l}$ in block sof size (8×8)
  - For i=1 to not of 1 up to t
    // * Operation of Transposition * //
    If ( )$a \times i + b \bmod(t) == 0$
    Then
    $\overline{V}[b] = V(i)$
    Otherwise
    $\overline{V}[a \times i + b \bmod(t)] = V(i)$
    End of If
  - End For
  $\overline{I}_{h,l} =$ *Reconstruct the image by the vector* $\overline{V}$ *;*
  $GoP =$ *Put the image* $\overline{I}_{h,l}$ *in place of the true Intra* $I_{h,l}$*;*
- End For

The decrypters having knowledge of the key of permutation and of the location or it must install the bend of the GOP (image-I), may as well build the image-P of the GOP (see the preceding one and(or) that which the successor) as illustrated in the diagram of the process Benabdellah considers et al.

In what is to come, we will present the results of the application of each of the algorithms of the two proposed approaches.

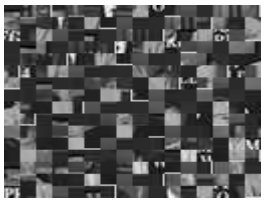
5.3 Application & Results

We present below, separately, the results of the application of each of the algorithms proposed for the encryption of the MPEG format and those of its crypto-compression. The video sequences used contain images of size $(h, l) = (128 \times 128)$. This gives about 256 parts (blocks) of puzzle of size (8×8). OF or, we use the algebraic structure $\mathbb{Z}/257\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ that allows you to design the randomized aspect for the two application examples shown below.

Encryption of the MPEG.

The results of the playback of a video encrypted by a user who does not have the key (resp the one who has) are as follows:

Intra Image


Encrypted Intra Image

Predicted Image (P1)


Encrypted Predicted Image (P1)

Bidirectional Image (B1)


Encrypted Bidirectional Image (B1)

Bidirectional Image (B2)

Encrypted Bidirectional Image (B2)

Figure 8. : The images decrypted (resp originals) and the effects of encryption of the intra frame on its predecessor (P) and (B) on the same GOP(1: 12) for an unwanted user.

The images (P) and (B) shown above have not undergone treatment of encryption. Because of this, the time of encryption of a GOP in the MPEG format focuses on the encryption of the image-I. Either of two images per second. The table below shows exactly the time of permutation of 256 blocks of puzzle and the entropy measures of each of the original images (resp decrypted) and those who are rebuilding themselves during a reading without malicious key. (Case of user non-permit)

GOP(1:12)	Our method		
	E.O.I	E.E.I	E.T(ms)
Intra image	7.0005	7.0005	5.2
Predicted image (P1)	6.9285	7.1651	0
Bidirectional image (B1)	6.9199	7.2486	0
Bidirectional image (B2)	6.9263	7.2489	0

Figure 9. : The results of the application of our synthesis on the Intra frame of the GOP (1: 12). E. I. O: Entropies of the Original Image, E. I. E: Entropies of the Encrypted Image, T. E: Time of Encryption (ms).

The results obtained, are only approve the cohabitation of our method with the algorithm of JPEG compression, when it comes to the puzzle pieces that are of size (8.8). In addition, the flexibility in execution time, which the problem is converted to the number of parts to swap. Either of 256 operations in the example in progress. Thus, the run time may well be reduced depending on the size of the used blocks which must respond to the constraint of the JPEG compression, in order to en-

sure the quality of the documents at the time of the reconstruction. What makes that the blocks can be increasingly large (8.16), (16.8), (16.16) or other ... according to the time of treatment research (reps to the degree of security semantics).

The randomized aspect of the structure, offered by the example treaty, leaves change randomly the keys of a moment to the other. An asset which can well serve on several use cases which we will come back in the last section of this chapter.

Security:

The algorithm proposed reported the problem of encryption of MPEG video to the encryption of a single image in each of its GoP. In addition, the security of the latter uses the same synthesis applied to the fixed image. Which leaves carry all properties already presented for still images, with the case of the video in its MPEG format.

The semantic security of the crypto-system is based, essentially, on the reconstruction of the puzzle without knowing its initial state, which is quite relative to the size and number of parts in the puzzle.

Application Crypto-compression:.

In this section, we present the results of the application of our approach to crypto-compression on the same GoP presented in the results of the previous application. The images presented below are the results of three cases of reading. In effect, the first is that of an original sequence (reps decrypted). As to the second, it presents the case of a sequence due to a reading malicious. While the last, is that of an attacker who has corrupted the system of encryption, but does not know the correct location of the image-I.

Image Intra

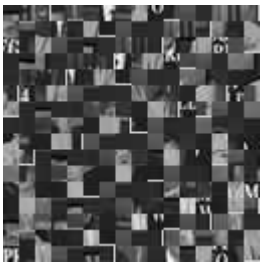
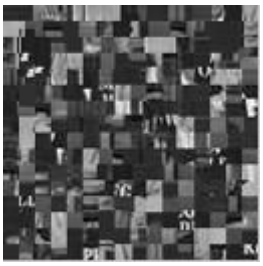


Image Encrypted Intra

Encrypted Intra Image

Predictive Image (P1)



Predictive Image Encrypted (P1)

Encrypted Image Predictive (P1)

Image Biderictionelle (B1)

Image Biderictionelle Encrypted (B1)

Image Biderictionelle Encrypted (B1)

Image Biderictionelle (B2)

Image Biderictionelle Encrypted (B2)

Image Biderictionelle Encrypted (B2)

Figure 10. : The images decrypted (resp originals) in column (a), those of the effects of encryption of the intra frame on its predecessors (P) and (B) on the same GOP(1: 12) and .in column (c) a reconstruction of an image-I evil is crooked or is positioned incorrectly.

Figure 11.

The table below address the set of measures related to the new structure of the GOP and the encryption keys (reps decryption) used.

GOP (1:12)	E. O. I	E. F. I	E. T (MS)	MCO (Kb)	ERM (Kb)

Intra image	7.0005	7.0005	5.22	4.44	4.41
Predicted image (P1)	6.9285	7.1651	0.00		
Bidirectional image (B1)	6.9199	7.2486	0.00		
Bidirectional image (B2)	6.9263	7.2489	0.00		

Figure 12. : The results of the application of our synthesis on the Intra frame of the GOP (1: 12). E. I. O: Entropies of the Original Image, E. I. E: Entropies of the Encrypted Image, T. E: Time of Encryption (ms).

The application of the algorithm of Benabdelah and al, has allowed us to choose the image-P3 as being the most optimal. As well, P3 offers the decrease of the memory space occupied by the GOP in treatment, and played the role of the picture-I on the MPEG algorithm. In addition, it is the image which will be encrypted. Consequently, the reconstruction of the structure of the GOP is done as shown in the figure below:

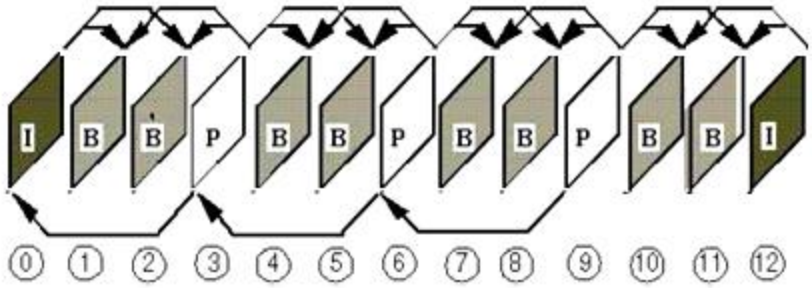


Figure 13. : Diagram of the construction of the GoP of the presented example

The image-P3, having become the pillar of the GoP, it will serve to reconstruct the image-P2 which the successor. And then, it is this last (image-P2) which will reconstruct the image-P1, which, in turn, is responsible for the reconstruction of the image-I. That said, the new architecture of the reconstruction of the structure of the GOP is in the inverse direction of the MPEG standard. To this effect, the vectors of reconstruction of images-P undergo changes, and are no longer the same as those of the MPEG algorithm whereas those of images-B, do not need. In effect, it is assumed that the choices made by the MPEG algorithm are most suitable.

In addition, the receiver (or decrypteur) is not very interested to changes that has could not undergo the architecture of the reconstruction of the

GOP. In fact, given that it knows the decryption key which contains the location of the image-I, and that it receives the GoP in its storage structure of IPBBPBBPBB…BB, it can decrypt the image-I and set to the appropriate location. That is to say that of the image-P3. Then, it is used to reconstruct the image-P2, and so on until all the images-Pi of the GoP are reconstructed according to the diagram of the algorithm Benabdelah et al.

The criterion for the choice of the reference image (image-I) allows you to perform the compression when there is an image more optimal than those used by the standard algorithm of the MPEG format (the first image of the sequence GoP). In addition, it offered a pseudo randomized based on the content for the choice of the image-I.

Thus, an attacker who stole the encryption system is faced with problems of synchronization of images in time. What causes the "wham of the reconstructed scene entire as shown in the figure(x) column(c). In addition, the attacker must try all possible locations, either of 4 possibilities, in the worst case, that he checked with the naked eye to award what is the right scene. A stain which could last a whole day, see more for a DVD movie or other type of document etc. as well, the proposed method seems to be well adapted to the transmission in direct. However, the latter cause a small problem of synchronizations, because the reconstruction of the last two images-B of the GOP in the MPEG algorithm uses the image-I of the GoP in succession. As a consequence, our approach requires the systematic reconstruction of two GoP which succeed one another, so to allow the reading of the first GoP.

Security:.

The security of our system of crypto-compression added to that of the approach presented in the section (IV. 4.1.1) (which aims to encrypt the image-I of the classic algorithm for the MPEG) of semantic problems. Because, this one replayed on the structure offered by the algorithm of Benabdelah and al, to hide the location of the image-I (added to the keys). Which poses the attackers before problems of synchronization of image in time (to synthesize the movement). It is the inky blackness of a feiutoscope in disorder. Who is 4 possibilities in the case of our method since the images which between competing in the algorithm proposed Benabdelah and al are: the image-I and the three Images-P of the same GoP.

Given that the choice of the pillar of the GOP is based on its content, it is an aspect of choice pseudo randomized controlled trial based on the content, which leaves us believing that the prediction of the location that must take the image-I will be more difficult to attackers, and clutter up its stain in the verification of all possible locations to the naked eye (attack by force gross).

The algorithms of the proposed approaches on the video, show their effectiveness in term of: execution time, the degrees of configurable security and the cohabitation with compression algorithms with loss of information.

6 Conclusion

In this chapter, we have presented the whole of the solutions proposed for the crypto-securing of pictures and video, or we have clearly shown that we have been able to identify all the challenges related to this theme (crypto-imaging). Passing by, the treatment time or our algorithms require only a few milliseconds of execution and, by, the cohabitation with one of the compression algorithms the most used that ca either JPEG or video in its MPEG format. Then, the security of the function B which comes up to reinstall to table the conditions posed by Shannon for a crypto-perfect system.

7 References

1. Barni M., F. Bartolini, V. Cappellini, A. Lippi, and A. Piva. A dwt-based technique for spatio-frequency masking of digital signatures. In Security and Watermarking of Multimedia Contents I, volume 3657, pages 31{39. SPIE, 1999.
2. Benabdellah, M, Gharbi, M., Regragui F. and Bouyakhf E.H., 2005. A method for choosing reference images based on edge detection for video compression. Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 3(7): 33-39.
3. Benabdellah, M, Gharbi, M., Regragui F. and Bouyakhf E.H., 2007. Choice of reference images for video compression, Int. J. Applied Math. Sci., 1: 2187-2201.
4. Benlcouiri, Y., Benabdellah, M., Ismaili M.C. and Azizi, A., 2013. Affine cipher extended to (Z/pZ) and it's application in images. Proceedings of the 20th International Conference on Telecommunications (ICT) May. 6-8, IEEE Xplore Press. DOI: 10.1109/ICTEL.2013.6632106
5. C. -F. Chen and K. K. Pang, "The Optimal Transform of Motion-Compensated Frame Difference Images in a Hybrid Coding", IEEE Trans. Circuits and Systems - II: Analog and

Digital Signal Processing, pp. 289 -296 1963

6. Choo, E., J. Lee, H. Lee and G. Nam, 2007. SRMT: A lightweight encryption scheme for secure real-time multimedia transmission. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering, Apr. 26-28, IEEE Xplore Press, Seoul, pp: 60-65. DOI: 10.1109/MUE.2007.194

7. Choon, L.S., 2004. Lightweight and cost-effective MPEG video encryption. Proceedings of the International Conference on Information and Communication Technologies: From Theory to Applications, Apr. 19-23, IEEE Xplore Press, pp: 525-526. DOI: 10.1109/ICTTA.2004.1307863

8. Cox Ingemar J., Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spreadspectrum watermarking for multimedia. IEEE Transactions on Image Processing,6(12) :1673:1687, 1997.

9. Ellinas, J. N. ; Sangriotis, M.S. "Stereo video coding based on quad-tree decomposition of Bâ€ "P frames by motion and disparity interpolation", IEE Proceedings - Vision Image and Signal Processing, Volume.152, Issue.5, pp. 639, 2005.

10. Error sensitivity data structures and retransmission strategies for robust JPEG 2000 wireless imaging Published in: Consumer Electronics, IEEE Transactions (Volume:49 , Results: 4) Date of Publication: Nov. 2003 Page(s): 872 - 882.

11. Hassen Seddik, Mounir Sayadi, and Farhat Fnaiech. Nouveau schéma de tatouage par substitution s'appliquant aux techniques spatiales robuste aux attaques asynchrones. In International Conference : Sciences of Electronic, Technologies of Information and Telecommunications, 2005.

12. Hu, Yu-Chen "Predictive time preserving block truncation coding for gray-level image compression", Journal of Electronic Imaging,Volume.13, Issue.4, pp. 871, 2004, ISSN: 10179909.

13. Huffman, D. A. "A method for the construction of minimum redundancy codes", In Proceedings IRE, vol. 40, 1962, pp. 1098-1101.

14. JPEG Still Image Data Compression Standard Pennebaker, William B. , Mitchell, Joan L. ,1993.

15. K. R. Rao and J. J. Hwang, "Techniques, standards for Image, video, and Audio Coding", 1996.

16. Kundur, D. and D. Hatzinakos. Digital watermarking using multiresolution waveletdecomposition. In IEEE ICASSP'98, volume 1, pages 2659{2662. IEEE, 1998.

17. Kundur, D.and D. Hatzinakos. A robust digital image watermarking scheme using the wavelet based function. In IEEE International Conference on Image Processing, volume 1, pages 544-547. IEEE, 1997.

18. Lightweight, A. "Implementations of fast discrete cosine transform for full color videotex services and terminals", In Proceedings of the IEEE Global Telecommunications Conference, IEEE Communications Society (1984), page(s). 333-337.

19. M. Maes and C. van Overveld. Digital watermarking by geometric warping. In IEEE International Conference on Image Processing, volume 2, pages 424:429. IEEE,1998.

20. Mitchell D. Swanson, Bin Zhu, and Ahmed H. Tewk. Transparent robust image watermarking. In IEEE International Conference on Image Processing, pages 211:214, 1996.

21. MPEG digital audio coding Signal Processing Magazine, IEEE (Volume:14 , Results: 5) , 1997, Page(s): 59 - 81.

22. MPEG digital video-coding standards, Signal Processing Magazine, Volume:14 Issue:5.

23. Muzaffar, Tanzeem; Choi, Tae-Sun "Video data reduction with error resilience based on macroblock reorder" ,Journal of Electronic Imaging,Volume.14, Issue.1, 2005, ISSN: 10179909.

24. Patrick Bas, Jean M. Chassery, , and Franck Davoine. A geometrical and frequential watermarking scheme using similarities. In Security and Watermarking of Multimedia Contents, pages 264:272. SPIE, 1999.

25. Pennebaker, W. B. , JPEG Tech. Specification, Revision 8. Informal working paper JPEG-8-R8, Aug. 1990.

26. Piva.A, M. Barni, F. Bartolini, , and V. Capellini. Dct based watermark recovering without resorting to the uncorrupted original image. In IEEE International Conference on Image Processing, pages 520{523. IEEE, 1997.

27.

28. Shannon, C.E., 1949. Communication Theory of Secrecy Systems. Bell System Technical Journal, 28: 656-715.

29. T. Naveen and J. W. Woods, "Motion Compensated Multiresolution Transmission of High Definition Video", IEEE Trans. Circ. And metric. Video Tech., vol. 4, Pages:29-41, 1994.

30. Tang, L., 1996. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the 4th ACM International Conference on Multimedia, Nov. 18-22, Boston, MA, USA, pp: 219-229. DOI: 10.1145/244130.244209

31. The JPEG 2000 still image compression standard Signal Processing Magazine, IEEE (Volume:18 , Results: 5),2001 Page(s) :36 - 58.

32. The JPEG still picture compression standard Published in:Consumer Electronics, IEEE Transactions (Volume:38 , Results: 1) ,Feb 1992, 10.1109 /30.125072 .

33. W. Zhu, Z. Xiong, , and Y. Zhang. Multiresolution watermarking for images and video : a united approach. In IEEE International Conference on Image Processing, volume 1, pages 465-469. IEEE, 1998.

34. Xia, C. Boncelet, and C. Arce. A multiresolution watermark for digital images.In IEEE International Conference on Image Processing, volume 1, pages 548:551.IEEE, 1997.

35. Zeghid, M.., Machhout, M.., Khriji, L. and Baganne, A., 2007. A modified AES based algorithm for image encryption. International Journal of Computer Science and Engineering 1(1): 70–75.

36. Zeng, W. and S. Lei, 2002. Efficient frequency domain selective scrambling of digital video. IEEE Trans. Mult., 5: 118-219.

37. Zhao, J. and E. Koch. Embedding robust labels into images for copyright protection.In International Congress on Intellectual Property Rights for Specialized Information,Knowledge

and New Technologies - KnowRight'95, volume 82, pages 242:251,