Applied Mathematical Sciences, Vol. 7, 2013, no. 42, 2093 - 2102
HIKARI Ltd, www.m-hikari.com

Encryption of Ultrasound Images Using the Permutation on the ($\mathbb{Z}/p\mathbb{Z}$) Fields

[1] Y. Benlcouiri, [3] M. C. Ismaili, [4] A. Azizi

[1, 3, 4] Laboratory of Arithmetic, Scientific Computing and Applications,
Faculty of Science, Mohamed First University
Oujda, Morocco.
[1] benlcouiriy@yahoo.fr, [3] mcismaili@yahoo.fr, [4] abdelmalekazizi@yahoo.fr

[2] M. Benabdellah

[2] Laboratory of Economic and Management of Organizations,
Faculty of Law, Economics and Social Sciences, Mohamed First University,
Oujda, Morocco.
[2] med_benabdellah@yahoo.fr

Abstract

Encryption methods include transposition by rearranging the data to be encrypted so as to make them unintelligible. For example, it rearranges geometrically the data to make them visually unusable. In this paper, we propose a new encryption method of still images based on the affine encryption principle to achieve a transposition and perform some manipulations to reduce the quantity of bits to be processed on an image. The application of this method on the still images, gave us a high degree of safety laws after a security measure introduced by Shannon and a minimum processing time is proportional to the number of pixels, while operations encryption and decryption. The comparison of this approach with the encryption method using injection of noise on the architecture of artificial neural networks, showed its good performance.

Keywords: Congruence, Affine Encryption, Puzzle, Transposition, Modular Arithmetic

1 Introduction

The most methods of encryption based on two principles: substitution and transposition. Substitution means that replacing some letters by symbols or others. Transposition means that permuting the letters of the message to make it unintelligible. Over the centuries, many systems of cryptographic TMIS have developed more perfection more clever. [7]

The symmetric cryptography is very used and characterized by high speed (Encryption on the fly), as well as software implementations (Kryptozone, Software Firewalls such Firewall-1 and VPN-1 checkpoint) that hardware (Cards dedicated, Crypto processor 8 to 32 bits, wired algorithms,…) which significantly accelerates the flow and allows its widespread use. This type of cryptography usually works in two different processes; the encryption by block and encryption "stream" (in continuous state). [8]

The image encryption is not possible with asymmetric methods because this type of system requires the use of large numbers to ensure a high level of security which increases the amount of data to be processed, while the symmetric encryption standards such as DES and AES despite their advantage (number of encrypted bits = number of clear bits) are very slow to respond to the compromise by providing decryption to consumption time more than encryption block mode has drawbacks because of homogeneous areas of an all identical image blocks, after encrypting, are also implying that the entropy of the image processing is not maximum, and an error caused by noise on an encrypted bit propagates the error on all the current block. [5, 6, 9]

The cryptography by transposition seems to be suitable to this type of problems; it reorganizes the locations of the elements of the message (text, pixel…) by ways to limited access. On the first methods of this time is the "SCYTALE" where encryption based on the modification of the original message by the inclusion of unnecessary symbols disappeared when the message was wrapped around the stick predefined length and thickness. In this case, security is not based on the technical used, but on the exact dimensions of the "SCYTALE" where the length and the size of it were the key of the system. To give an idea of its power, we choose the simple case of transposition of three abstractly characters, the method is as follows: when one character is selected in the first place on the three possible positions, we have two characters as they may be positioned in different ways, a total of 3×2=6 combinations. In the case of a longer message, 10 characters, for example, the number of possible combinations is then (10!) for a total of 3.628.800, is generally (n) characters there are (n!) ways to reorganize. Thus a reasonable message of 40 characters globalizes a number of combinations which becomes totally unthinkable to check them all.[3]

In this sense, and in order to optimize and secure transposition and storage of fixed images, we propose a new transposition approach to implement the principles of using affine encryption. The main advantages of this approach are flexibility and reduction of processing time, which is proportional to the number of pixels during the operation of encryption and decryption. Indeed, through this method we can vary the processing time depending on the desired level of security.

First of all, we will discuss the affine encryption procedure and some notions of congruence. Then, we describe the subdivision process image in puzzle. After that, we will describe in detail the principles of our approach and results obtained after its implementation comparing it with the encryption method using injection of noise on the architecture of artificial neural networks. Finally, we conclude our article by introducing some perspectives.

2 Methods

2.1 Affine cryptography

2.1.1 Definition of congruence

For u, v in $\mathbb{Z}$ and n an integer ≥ 2, the notation u≡ v(n) reads u congruent to v modulo n and means that u-v is divisible by n which is equivalent to say that u and v have the same retained when divided by n, for example 17 = 5 (3) but also -1 = 1 (2). [1]

u, v, r, s belong to $\mathbb{Z}$ and n an integer ≥ 2,

if u ≡ v (n) and r ≡ s(n) so:

u + r ≡ v + s(n); u - r ≡ v - s(n); u × r ≡ v × s(n);

and for all k Є $\mathbb{Z}$ we have u ≡ v + kn(n)

if u and v are two integers belonging to {0;1;2;…;n-1}

so u ≡ v(n) implies u ≡ v

2.1.2 Affine encryption

Noting that E = {0; 1; 2;…;25}
a and b are integers selected from E. Coding is affine, after numbered from 0 to 25 letters of the alphabet, to encode a letter (called source) number x by the letter number y, where y is the remainder of the division of ax+b by 26. The encoding function associated affine associated with the coefficients a and b is the function f from E to E in which x matches to f (x) = y. f(x) is the only element of the set E = {0, 1, 2, ..., 25} which is congruent to ax+b modulo 26, f (x) ≡ ax+b (26).[1]

For example if a=17 and b=5 the letters a, b, c are respectively encoded by f, w, n. in fact, the number of a is 0 so the letter a is encoded by the letter of number f(0)≡ 17×0+5=5 so f(0)=5 be the letter f; the number of b is 1 so the letter b is encoded by the letter of number f(1)≡ 17×1+5=22 so f(1)=22 be the letter w; the number of c is 2 so the letter c is encoded by the letter of number f(2)≡ 17×2+5=39 (26), and since f(2) must be in E (it is the remained of devising 39 by 26) f(2)=13 be the letter n.[1]

In theory it is not necessary to take *a* and *b* in E, but they are not, considering their remains in the division by 26, we are back immediately: 35x-15≡9x+11 (26). [1]

Jules César used an affine code: *f(x) ≡ x+3 (26)* in fact the encoding of the from *f(x)≡ x+3 (26)*; are back to a circular permutation of the letters. For example for *b=13 : a->d, b->e, c->f,....x->a, y->b, z->c.* [1]

It is obviously necessary that a condition for a coding function is that 2 separate letters have to be encoded in different way, otherwise it will be impossible to decode the message exactly. That is what interest us here? This condition is fulfilled only if *a* and 26 are coprime, it means that if *a* and 26 are 1 as the only common positive divisor. [1]

By checking this condition the only values of a are: 1; 3; 5; 7; 9; 11; 15; 17; 19; 21; 23; 25. In the sequel, when we speak about an affine coding function, it will be understood that *a* is one of the 12 numbers. [1]

2.3 Puzzle

The invention of puzzle is attributed to John Pillsbury, a London mapmaker and engraver. In 1760 he had the idea to cut cards representing different countries of the world and sell them as funny way to learn geography. [2]

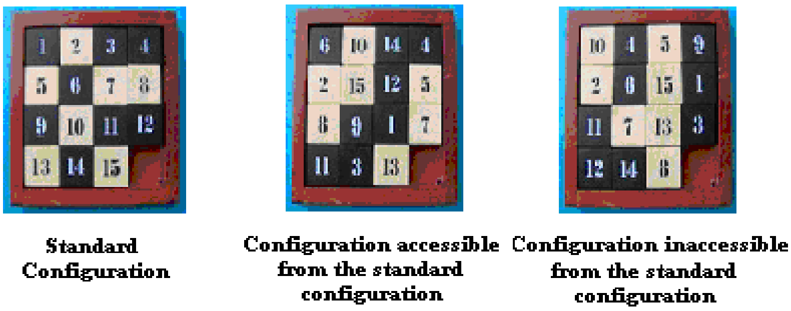
In the same year, when Turing’s death in 1954, an article was released “solvable and unsolvable problems” which presents in an elementary way, a number of results concerning the theory of computability. Although it is rather from a business extension, it carries with it a rigorous proof of the undesirability of the halting problem. But the approach is very different from the seminal work of 1936, and inflections that Turing did to earlier work are particularly instructive. [4]

The problem of the article refers to problems. But the term refers only decision problems. Indeed, Turing scrupulously distinguishes these puzzles for which are sought decision procedures. The same problem leads us to translate “puzzle” with “enigma” (sometimes “puzzle”) rather than “problem”. [4]

A problem is an application form: is there any decision procedure to solve this puzzle? And an insoluble problem is an enigma for which the decision problem is not soluble (i.e there is no decision procedure to resolve). Therefore, the whole about Turing is based on two concepts, which should be clarified before anything else: the notion of enigma and effective procedure. However, these will themselves defined as enigmas that meet a number of conditions. This is the notion of enigma (puzzle), which plays a central role and must be specified first. [2, 4]

- ✓ At first Turing meant to familiarize the reader with this notion by giving examples of enigmas. In a sense, it shows to the reader that this notion is already familiar. Because it is not a coincidence that Turing opens his inventory with a game that certainly is not marketed until now, but that is not less popular to already know the cheeky. As we shall see, this puzzle which is well known to children, plays an almost paradigmatic in this first step in the process of Turing. [4]

✓ As marketed, the reader looks like a square divided into sixteen squares (sometimes less, sometimes more, in variants in which we are not interested here), fifteen among them are occupied by mobile edge numbered from 1 to 15, the sixteenth is empty. The game is to place the edges in a given configuration, knowing that we cannot move the edges only one by one, and sliding in the empty box a square adjacent to it. (See Figure 1).



Standard Configuration

Configuration accessible from the standard configuration

Configuration inaccessible from the standard configuration

Figure 1: Different configurations of teasing..

It should stop at the first example, which shows particularly the essential characteristics enigmas: [4]

1) We have configurations, all of which are arrangements of a specified number of pieces – in the case of cheeky; we have 16 possible configurations in principle.

2) These pieces can be moved in accordance with specified rules that allow some shots and prohibit others, for example, the cheeky (teasing), you can remove the game!

3) Moving the pieces, we move from one configuration to another. The goal is to get some final configuration from an initial configuration.

4) At each step, we have the choice between a finite number of possible moves. Thus, in the teasing there are only two, three or four possible moves at each step, depending on the position of the blank.

This last point is important because the nature itself of the enigmatic riddle, it is precisely in this need to make the right choice. This is what wants who need to undertake solving the riddle of teasing. It is the nature of the movements to be performed for each step. He would have an implementation plan that eliminates all hesitations at each stage, may deviate from the goal.

3. Proposed method

Our method is to use the principles of an affine encryption not on the ring $\mathbb{Z}/_{26}\mathbb{Z}$ but on field type $\mathbb{Z}/p\mathbb{Z}$ married to the results of modular arithmetic and the problem of the puzzle to complete the transposition on these elements.

The generation's keys generation our method is divided into three parts:

- Choose a prime number p to work on the $\mathbb{Z}/p\mathbb{Z}$ field, in which all elements are invertible.
- Subdivide the image processing into *(p-1)* puzzle pieces (square, triangle…) with *(n×m)* blocks size according to the required security level.
- Select a pair of elements (a, b) in $[(\mathbb{Z}/p\mathbb{Z})^*,(\mathbb{Z}/p\mathbb{Z})]$.
- the encryption key is threefold:

[p; (a, b) ; (n, m)]

➢ ***Encryption step***

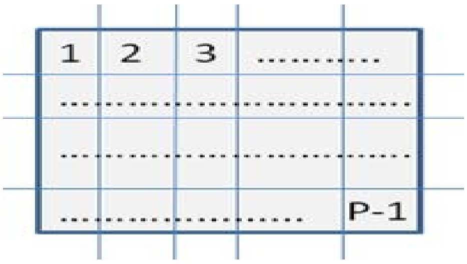


Figure 2:Original image divided into (p-1) elements.

After subdividing the image as shown in the figure above, in *(p-1)* macro-blocks numbered from *1* to *p-1*, we proceed as following:

Let f be the mapping defined as follows:

$$f: (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})$$
$$: \quad x \quad \rightarrow \quad ax+b(p)$$

The transpose function is defined as follows:

$$g : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$$
$$: x \longrightarrow \begin{cases} g(x)=b & \text{if } f(x)=0 \\ g(x)=f(x) & \text{else} \end{cases}$$

To change the location of each macro-block of image processing, we apply the function *g* to its indices.

$$\{g(1),g(2),g(3)\ldots,g(p-1)\} = \{5, 10\ldots, (p-1),\ldots 3\}_{transpose}$$

Reorganize the results after applying the function *g* on the indices of macro-blocks conducted a transposition.

Encryption algorithm

```
[p; (a, b) ; (n, m)] : Encrytion key
Tab [p-1] : Images into macroblocks
Tab_crypte [p-1] : Image after transposition
Beginning
    Variable i, temp ;
        for (i=1; i<p; i++)
            temp= g(i);
                if(temp=0)
                    Tab_crypte [i] = Tab[b]
                else
                    Tab_crypte [i] = Tab[temp]
                end if
        end for
Back ( Tab_crypte )
End
```

The encrypted image is shown in the figure below.

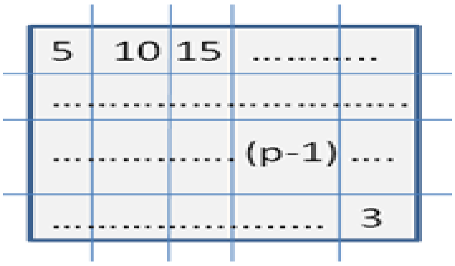


Figure 3: Encrypted image after transposition of (p-1) blocks.

- ***Decryption step***

The encryption key and the decryption key are equal to *[p ; (a,b) ; (n,m)];*
As the encryption method, after dividing the image into *(p-1)* macro-blocks, whose size is *(n×m)* pixels, this time we set the application g for the reconstruction of the original image as follows:

Decryption algorithm

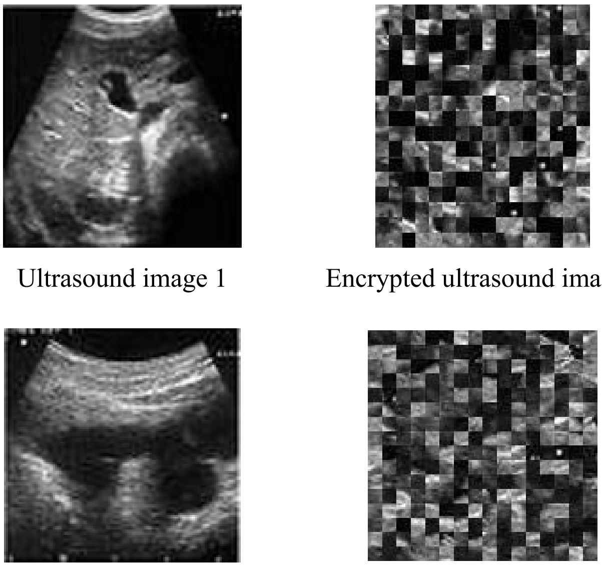
```
[p; (a, b) ; (n, m)] : Decryption key
Tab_crypte [p-1] : Encrypted image into macroblocks
Tab [p-1] : Reorganized image
Beginning
    Variable i, temp ;
        for (i=1 ; i<p; i++)
            temp= g(i);
            if(temp=0){
                Tab [b] = Tab_crypte [i] }
              else{
                Tab [temp]=Tab_crypte [i] }
        end for
Back ( Tab)
End
```

Whose application on the elements of the sequence already transposed, bring us back to the original.

4. Applications and results

We apply the proposed method to image in grayscale such that the size is 128×128 pixels. For this reason we start with:

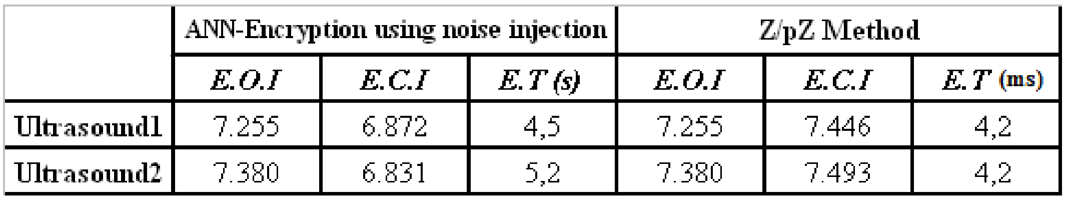
1) The choice of a prime number, in our case p = 257 (We will work on the field $\mathbb{Z}/p\mathbb{Z}=\mathbb{Z}/257^*\mathbb{Z}$)
2) Then we divide the image into (p-1) = 256 elements each of size *(n×m)* where *n* = 8 and *m* = 8.
3) We randomly chosen in $\mathbb{Z}/257^*\mathbb{Z}$; a = 33 and b = 0. We get the following cryptosystem keys:
   The encryption key is: *[257; (33,0) ; (8×8)]*



Ultrasound image 1 Encrypted ultrasound image1

Ultrasound image 2 Encrypted image 2

Figure 4: Results after applying our method to ultrasound images 1 and 2.



	ANN-Encryption using noise injection			Z/pZ Method		
	E.O.I	*E.C.I*	*E.T (s)*	*E.O.I*	*E.C.I*	*E.T* (ms)
Ultrasound1	7.255	6.872	4,5	7.255	7.446	4,2
Ultrasound2	7.380	6.831	5,2	7.380	7.493	4,2

Table 1. Comparison between the encryption method that uses the permutation on the ($\mathbb{Z}$/p$\mathbb{Z}$) fields and the method based on the ANN and the Encryption using noise injection. E.O.I: Entropy of Original Image, E.C.I: Entropy of encrypted Image, E.T: Encryption Time.

The subdivision of the image into 256 macro-blocks allows us, on encryption, to make a calculation codes into 8 bits and we got a minimum processing time. The entropy of the original image is equal to that of the encrypted image which provides a high degree of safety according to security measure law that are introduced by Shannon in information theory.

In the method "ANN-Encryption using noise injection" [10], the neural networks compression provides a compression ratio quite interesting even if it is costly in terms of time required to adjust the weights appropriate to the neural networks that are responsible for the visual quality of the image processing, as well as part of the compression asymmetric compression coefficients are not those of the decompression and the codomain presented on the hidden layer can be demonstrably injective. Moreover, this algorithm provides a transmission with interlace (progressive transmission), which reduces the burden of bandwidth. As regards the time necessary for the operations of dissimilation, it may vary depending on the degree of security.

The complexity introduced by our algorithm computes the number of possible keys which equals [p*(p-1)] is the number of combinations available on the (p-1)! total combinations. The reapplication of this algorithm on the results of one of the [p*(p-1)] key gives access to other combinations that are not available in a single application because $g_{(a,b)} \circ g_{(a_1,b)_1} \neq g_{(a*a_1,a*b_1+b)}$ such that $g_{(a,b)} = ax + b$.

The cryptanalysis of our method with an exhaustive attack demands the course of (256)! possible cases to induce the original image which requires a human factor which validated the original image among the cases, and the analysis frequency can not bring anything since it is not a substitution for nothing been replaced by something else, but the locations of block that was changed. Time encryption proves its superiority and stability for images of the same size.

5. Conclusion

We introduced a method of cryptography of fixed images based on the affine encryption to produce a method of transposition on field type ($\mathbb{Z}$/p$\mathbb{Z}$) which allows us to 312 possible tests on the affine encryption of [(p-1)!] tests that the use of the principle of the puzzle allows to reduce the amount of pixels processed the results obtained from our application, shows that the complexity can produce such a system of transposition.

Then we wish to apply this method on the video to produce a crypto-system which is appropriate to this type of document knowing its encryption speed and the degree of security that provides.

Acknowledgements. Supported by the Hassan II Academy of science and technology of Morocco.

References

[1] A. Azizi, ”Cour de cryptographie”, Master Ingénierie Informatique, FSO, Université Mohamed Premier, Oujda, Maroc, 2011.

[2] Antoine Bello, ”Éloge de la pièce manquante”, Coll. La Noire, Éd. Gallimard, 1998.

[3] Juan Gomez, ”Mathématiques, espionnage et piratage informatique : Codage et cryptographie”, ISBN/ISSN/EAN 978-2-8152-0237-4, RBA Coleccionables, Barcelone, Espagne, 2011.

[4] Lény Oumraou, ”Algorithmes et puzzles : une ultime approche de Turing ”, Docteur agrégé de philosophie - Universite Paris I, France.

[5] M. Benabdellah, M. Gharbi, N. Zahid, F. Regragui, E. H. Bouyakhf, ”Encryption-Compression Method of Images”, International Journal on Computer Science and Information Systems (IJCSIS) Vol. 4: No 1. pp. 30-41 February, 2009.

[6] M. Benabdellah, F. Regragui, E. H. Bouyakhf, ”Hybrid Methods of Image Compression-Encryption”, J. of Commun. & Comput. Eng. ISSN 2090-6234, Volume 1, Issue 1-2, pp. 1-11, 2011.

[7] Schneier B., ”Cryptographie Appliquée”, Vuibert, Wiley and International Thomson Publishing, NY, 2nd edition, 1997.

[8] T. Ebrahimi, F. Leprevost and B. Warusfeld Ed., ”Cryptographie et Securité des systèmes et réseaux”, Lavoisier-Hermes, 2006.

[9] Y. Benlcouiri, M. Benabdellah, M. C. Ismaili and A. Azizi, Crypto-Compression of Images Based on The ANNs and The AES, J. of Commun. & Comput. Eng. ISSN 2090-6234, volume 2, Issue 3, pp 1: 6, 2012.

[10] Y. Benlcouiri , M. Benabdellah, M. C. Ismaili and A. Azizi, Securing Images by Secret Key Steganography, Applied Mathematical Sciences, Vol. 6, 2012, no. 111, 5513 – 5523.

Received: December 3, 2012