Journal of Computer Science

Original Research Paper

Crypto-Watermarking of Images based on the Permutation on Z/pZ and the Wavelet Decompositions of Legall 5/3

[1]Younes Benlcouiri, [1]Moulay Chrif Ismaili, [1]Abdelmalek Azizi and [2]Mohammed Benabdellah

[1]Laboratory of Arithmetic, Scientific Computing and Applications,
Faculty of Science, Mohamed First University, Oujda, Morocco
[2]Laboratory of Economic and Management of Organizations,
Faculty of Law, Economics and Social Sciences, Mohamed First University, Oujda, Morocco

Article history
Received: 02-10-2018
Revised: 16-11-2018
Accepted: 08-06-2019

Corresponding Author:
Younes Benlcouiri
Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University. Oujda, Morocco
Email: y.benlcouiri@gmail.com

Abstract: In this work, we are interested in the insertion of the watermarking of digital images in the frequency domain. The algorithm proposed uses the transformed into wavelet Legall 5/3 on an image encrypted by swapping on the Z/pZ field, to perform the watermarking. By consequence, this introduces the concept of keys to the traditional methods of non-blind watermarking. The results of the application of this method on the fixed image (presented in the section: Application and results show well its performance.

Keywords: Crypto-Watermarking, Still Images, Wavelet Decompositions of Legall 5/3, Transposition Z/pZ, Modular Arithmetic

Introduction

The important development of digital networks has revealed the problem of the protection of the intellectual property of the documents, which has motivated many research in digital watermarking. This technique is to insert, at the inside of a digital document, an invisible mark, containing a code, robust to any attack that might change the given watermarked. Many algorithms of watermarking have been proposed seeking to optimize compromise robustness and invisibility. However, none of them meets the specifications ideal. Currently, no functional model of universal watermarking has been defined (Inoue *et al*., 2002; Awad *et al*., 2009).

The watermarking image is governed by three different principles: In the first case, we only have the image watermarked, from what we must extract the signature in order to know its owner. In the second case, we have the image watermarked and of the signature, therefore we are seeking, in this case, to confirm the presence of the signature in the medium treaty. The last case concerned the watermarking not blind. We have the original image, as well as the image watermarked and signature inserted. The third case will be our subject for study in this work (Antoine, 1998).

The watermarking image is divided into two parts; the first represents the Insert phase of the brand, while the second represents the phase of its detection.

The wavelet transformation is the form of the major compression new standard form such as JPEG2000 there, the watermarking in its domain is guaranteed exceeds degradation type problem of compression (Benabdellah *et al*., 2009). More the multi-resolution domain guaranteed that too, such as Legall transformation (Wang *et al*., 2002).

The cryptography is the whole of the locking process aimed to protect access to some data in order to make them incomprehensible to non-authorized persons. Cryptographic technologies are thus recognized as essential tools of data security, confidence in the communications and electronic commerce (Daubechies and Sweldens, 1998; Oumraou, 2009).

Most of the methods of encryption are based on two essential principles: The substitution and transposition. Substitute means that it replaces certain letters by others, or by symbols. The transposition means that we exchange presents the letters of the message in order to make unintelligible. Over the centuries, many cryptographic systems have been developed, more and more sophisticated, more and more astute (Benlcouiri *et al*., 2012a).

In this sense and in order to ensure the optimization and the securing of transmission and storage of still images, we propose an approach to watermarking non-blind which is based, not on the original image for the extraction of the mark, but on its encrypted version. The main advantages of the approach are the

introduction of the concept of the keys in the watermarking not blind. The flexibility and the reduction of the time of encryption are proportional to the number of pixels, at the time of encryption and decryption operations. In effect, by this method, we can vary the processing time in the function of the desired level of security (Wang *et al*., 2002).

In what follows, we are going to talk about the wavelet decompositions of Legall 5/3 and the encryption procedure by transposition on the fields Z/pZ, next, we describe in detail, the principles of our method, as well as the results obtained. Finally, before concluding, we will talk about the prospects.

Methods

Wavelet Decompositions of Legall 5/3

JPEG 2000 uses a transformed separable to perform a dyadic decomposition of the whole image into sub-frequency bands (Benlcouiri *et al*., 2012b) (Fig. 1).

Thus the rows and columns are successively broken down following the recursive algorithm of Mallat, which gives as many sub-bands BB (low horizontal and vertical frequencies), BH (low frequencies and horizontal high vertical frequencies), HB (high horizontal frequencies and low vertical frequencies) and HH (high horizontal and vertical frequencies) that there is of levels of decompositions (Benlcouiri *et al*., 2012a).

The filters allowed are: Either the pair (9.7) irreversible of Daubechies or the pair (5.3) reversible of the Gall. The first defines a low-pass filter to 9 coefficients and a high-pass filter to 7 coefficients, all two to irrational coefficients. On the other hand, the pair (5.3) of low-pass and high-pass filters is to rational coefficients. As a general rule, the first allows compression rates higher for a given level of quality, but only the second is usable to compress without loss. The wavelet decompositions of Legall 5/3 allow the passage of the field of space to the domain multi resolution. It is a function of integers to integers (Wang *et al*., 2002).

The transformed into wavelet decompositions of Legall 5/3 is ensured by a low pass filter with three coefficients and a high pass filter to five coefficients. The image resulting from such processing includes an image of approximation and three images of details. The next level is achieved by applying new processing on the matrix of approximation. This wavelet seems to give better performance for the compression without losses, it is the wavelet by default the standard JPEG 2000 for the reversible compression. Numeric values of the coefficients of the filters are presented in the following Table 1 (Wang *et al*., 2002).

The use of Multi Resolution Analysis (MRA) as a support for inserting the signature ensures a better robustness to screw screws of this compression standard JPEG2000. In addition, this transformation follows the model of the multi-channel system human psycho visual. The multi resolution domain allows a spatial localization and frequency. The transformation in this area is provided by the filters associated with the wavelet (Benlcouiri *et al*., 2012a).

Transposition on Z/pZ

This method is to use the principles of the affine cipher, not on the ring Z/26Z, but on the fields of type Z/pZ, married to the problem of the puzzle to achieve the transposition on these elements (Wang *et al*., 2002).

Table 1: Filters used for the wavelet decompositions of Legall 5/3

	0	±1	±2
h_a	6/8	2/8	-1/8
g_a	1	-1/2	
h_2	1	1/2	
g_2	6/8	-2/8	-1/8

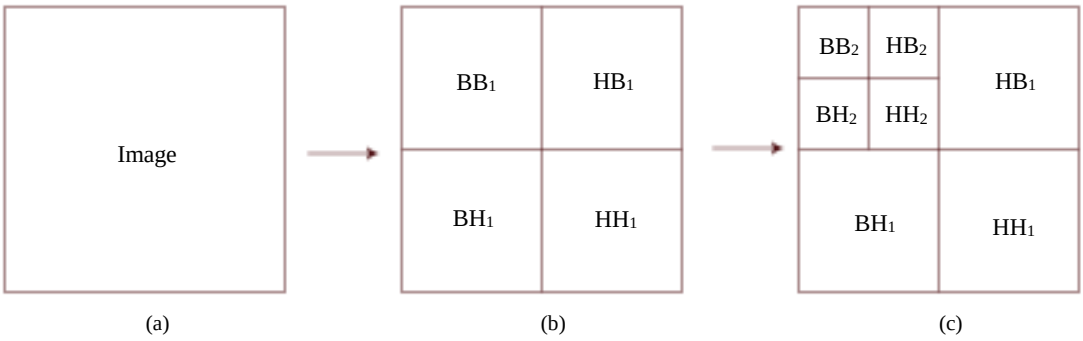

Fig. 1: Dyadic division of an image (a) in sub-bands of frequencies after a (b) and two (c) levels of decomposition

The generation of the keys to our method is broken down into three parts (Benlcouiri *et al*., 2012b):

1. Choose a prime number p for work on the body (Z/pZ) * whose all elements are reversal film
2. Subdivide the image in (P-1) pieces of puzzle (square, triangle etc…), note (n × m) the size of the blocks according to the appropriate level of safety
3. Choose a couple of elements (*a*,*b*) in ((Z/pZ)*, (Z/pZ)) and calculate the inverse of (a) using the algorithm of Euclid extended or:

$$a \times a^{-1} \equiv 1 \; mod(p)$$

The encryption key is the triple:

$$\left[P;(a,b);(n,m)\right];$$

The decryption key is misled directly because encryption is symmetric:

$$\left[P;\left(a^{-1},-b\right);(n,m)\right];$$

Process of Encryption

After the subdivision of image, as shown in the Fig. 2, in (P-1) macro-blocks numbered from 1 up to p-1, we proceed as follows.

Either *f* the application defined by:

$$f:(Z/pZ)^{*} \to (Z/pZ)^{*} \; x \to ax+b(p)$$

To change the location of each macro-block of the processed image, we apply the function f to its indices:

$$\left\{f(1), f(2), f(3)\ldots, f(p-1)\right\} = \left\{5,\ 10\ldots,(p-1)\ldots\ 3\right\}$$

Reorganize the results after the application of function *f* on the indices of the macro-blocks and this, in order to reconstruct the image whose macro-blocks have performed a transposition (Benlcouiri *et al*., 2012b).

The encrypted image will be the one shown on the Fig. 3:

Process of Decryption

The decryption key is the triple [*p*; (a^{-1}, -*b*); (*n*, *m*)];

As well as the encryption process, after having divided the image in (*p*-1) macro-blocks, whose size is (*n* × *m*) pixels, we define the application *f*-1 to reconstruct the original image by:

$$f^{-1}(Z/pZ)^{*} \to (Z/pZ)^{*}$$
$$x \to (x-b)\times a^{-1}(p)$$

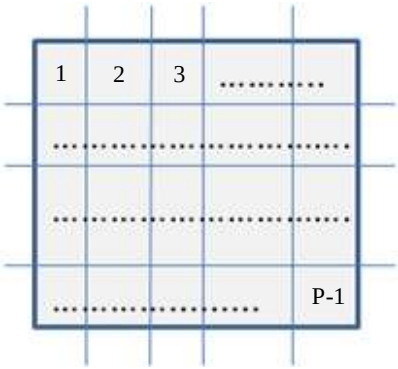

Fig. 2: Original Image divided into (*p*-1) elements

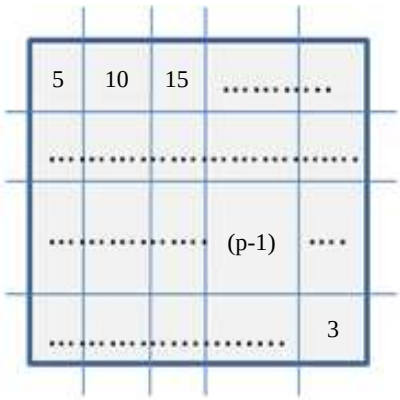

Fig. 3: Image encrypted after transposition of (p-1) blocks

The application of f^{-1} on the elements of the suite already transposed us back to the original image:

$$\left\{f^{-1}(1), f^{-1}(2), f^{-1}(3)\ldots f^{-1}(p-1)\right\} = \left\{1,\ 2,\ 3\ldots,\ (p-1)\right\}$$

The main advantage on *Z*/*pZ* field is the random space of the key that can be used in affine application. So, all *a* and *b* less than *p* are suitable as parameter in *f* application. Other way, the number of element that we can permute is *p*-1 for that the number of puzzle elements is suitable at *p*-1. Noting some other manipulation of images can be used for realize the streaming operation.

Proposed Method

The difference between the conventional methods of blind-watermarking and our new approach is the procedure of insertion and extraction of the mark which is done at the domain level transformed into wavelet decompositions of the encrypted image for introduce the key principle in this type of watermarking.

The mark is inserted on, the image of approximation of the second level after its

decomposition by the transformation of Legall 5/3, mentioned BB^2 in Fig. 1.

The insert function used is:

$$Y_i = X_i + a\, W_i ;$$

Where:

(X_i) = The value of pixel i in the second level of Legall transformation BB_2 of the encrypted original images
(α) = The coefficient of insert the mark
(W_i) = The value i of the original mark
(Y_i) = The value i in the second level of the Legall transformation BB_2 of marked image

To produce the marked image, we apply IDWT of Legell 5/3 in the original transformation after substitute BB_2 by Y_i.

The Insertion Process

This part consists of 5 steps, the Fig. 4 shows this decomposition.

The decryption step consists in rearranging each bloc x_i of crypto-watermarked image in the position $f^{-1}(i)$.

Extraction of the Mark

Unlike the classical case of extraction of the marking, our method requires the knowledge of encryption keys of the image watermarked and of the original image.

After encryption of the image watermarked and of the original image, we calculate the difference between the image crypto-watermarked and the encrypted of the original image in order to extract the mark, this is shown in the Fig. 5.

The main difference by the proposed method and (Mothi *et al*., 2013; Gurparkash *et al*., 2010; Elbasi *et al*., 2006; Awad *et al*., 2009;) is introduce the principle of keys by marking the encrypted image. The several attack on watermarking is delete it such as visible one and other, when the emplacement of the mark is known. In our method the emplacement of mark is relative to encrypt image (by permutation) there for the key of encryption is necessarily to this type of operation. Such as the degree of robustness guaranteed by wavelet-watermarking (Kalker *et al*., 2002) we can affirmed the distortion of mark added by our approach is relative to use all possible α in the equation of insertion on all pixel of image, then the distortion of mark in this proposed method is relative to lose the image information.

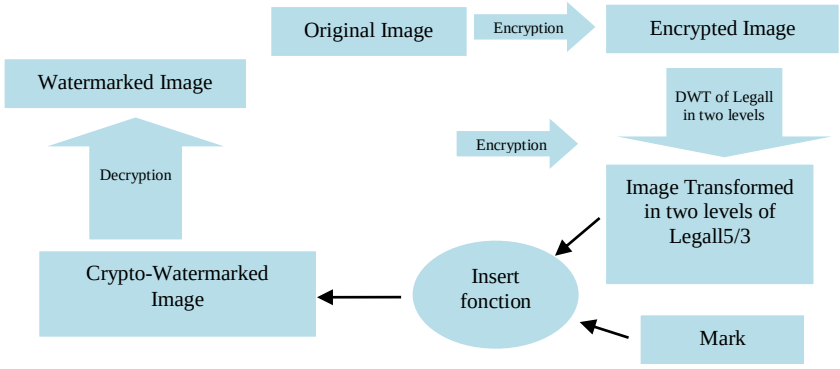

Fig. 4: iagram of the insert phase of the mark

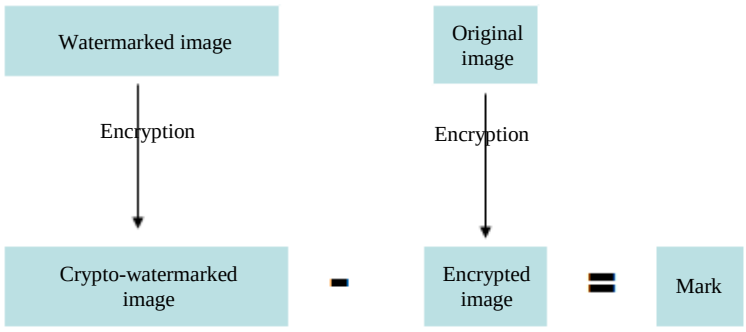

Fig. 5: Diagram of the extraction stage of the mark

Application and Results

The application of the proposed method is performed on images in gray level of size 128 ×128 pixels. Then we proceed as follows:

- We take p = 257 for work on the fields Z /pZ = Z/257Z
- Then, we also subdivide the image in (P-1) = 256 elements each of which have the size (n × m) with n = 8 and m = 8
- Finally, we choose randomly in Z/257 Z; a = 29, b = 0 and we calculate the inverse $(29)^{-1} \equiv 195\ (257)$

The keys of the crypto-system will be:
The encryption key is the triple:

$$\left[257;(29.0);(8\times 8)\right];$$

The decryption key is the triple:

$$\left[257;(195.0);(8\times 8)\right];$$

The application of our method, on the image Lena, gives us the following results:

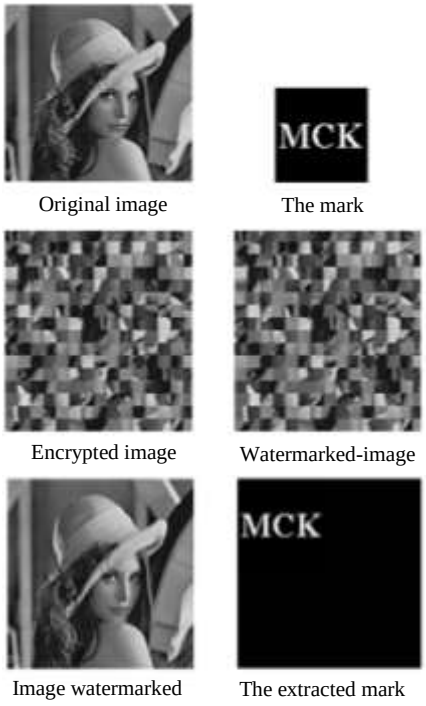

Fig. 6: Results after application of our method on the image Lena

Table 2: Results after application of our method on the image Lena. E.I.O: Entropy of the original image. E.I.R: Entropy of the encrypted image. T.C: Time of encryption

	E.I.O	E.I.C	T.C(s)
Image Lena	7.6464	7.6464	0.038

The Table 2 approuve the fixed entropy between original image and encrypted one. Then, the encryption process have any influence on the data domaine of insertion.

For the extraction of the mark, we calculate the difference between the two images watermarked and original one (Fig. 6).

We obtained the same entropy, by comparing the original image and the image encrypted, which offers a large degree of security according to the laws of security measure introduced by Shannon in information theory.

As any manipulation, the watermarking will cause a degradation of the image. This degradation must be minimized in order to ensure the imperceptibility of the mark. It constitutes a criterion for assessment of performance of the watermarking methods. In effect, in the conventional method, we carried the insert of the mark in the transformed from the original image, whereas in our case the insertion is carried on the transformed of the encrypted image, therefore the mark is not accessible if we don't know the key of permutation.

Conclusion

We have introduced a hybrid method of crypto-watermarking in still images based on the affine cipher, to produce a transposition on (Z/pZ) field and the watermarking by wavelet decompositions of Legall 5/3 in the frequency domain. This method has enabled to limit access to the watermarking even with the knowledge of the original image. The use of the principle of puzzle allows to reduce the amount of pixels to be processed and the results obtained clearly show the complexity that can produce such a system of transposition. View the speed of encryption that it has and the degree of security that it offers, we will want apply this method on the video.

Acknowledgment

This work was supported in part by the Hassan II Academy of Science and Technology of Morocco.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished results. The authors confirm no involved conflict of interest.

References

Antoine, B., 1998. Éloge De La Pièce Manquante. 1st Edn., La Noire - Gallimard, pp: 265.

Awad, K., F. Al-Asmari and A. Al-Enizi, 2009. A pyramid-based watermarking technique for digital color images copyright protection. Proceedings of the International Conference on Computing, Engineering and Information, Apr. 2-4, IEEE Xplore Press, Fullerton, CA, USA, pp: 44-47. DOI: 10.1109/ICC.2009.29

Benabdellah, M., M. Gharbi, N. Zahid, F. Regragui and H. Bouyakhf, 2009. Encryption-compression method of images. Int. J. Comput. Sci. Inform. Syst., 1: 30-41.

Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2012a. Crypto-compression of images based on the ANNS and the AES. J. Commun. Comput. Eng., 1: 1-6.

Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2012b. Securing Images by Secret Key Steganography. Int. J. Applied Math. Sci., 6: 5513-5523.

Daubechies, I. and W. Sweldens, 1998. Factoring wavelet transforms into lifting steps. J. Fourier Anal. Applic., 3: 247-269. DOI: 10.1007/BF02476026

Elbasi, E., E. Elbasi, M. Ahmet, A. Eskicioglu and M. Eskicioglu, 2006. A dwt-based robust semi-blind image watermarking algorithm using two bands. Proceeding of the Security, Steganography and Watermarking of Multimedia Contents VIII, Feb. 17-17, IEEE Xplore Press, California, USA, pp: 777-787. DOI: 10.1117/12.651154

Gurparkash, S.K., 2010. Blind digital image watermarking using adpative casting energy in different resolutions of wavelet transform. Proceedings of the International Conference on Computer and Communication Technology Allahabad, Sept. 17-19 IEEE Xplore Press, Uttar Pradesh, India, pp: 210-215. DOI: 10.1109/ICCCT.2010.5640527

Inoue, H., A. Miyazaki, A. Yamamoto and T. Katsura, 2002. A digital watermark based on the wavelet transform and its robustness on image compression. Proceedings of the International Conference on Image Processing, Oct. 7-7, IEEE Xplore Press, Chicago, IL, USA, pp: 391-395. DOI: 10.1109/ICIP.1998.723388

Kalker, T., 2002. Considerations on watermarking security. Proceeding of the IEEE 4th Workshop on Multimedia Signal Processing, Oct. 3-5, IEEE Xplore Press, Cannes, France, pp: 201-206. DOI: 10.1109/MMSP.2001.962734

Mothi, R. and M. Karthikeyan, 2013. A wavelet packet and fuzzy based digital image watermarking. Proceeding of the IEEE International Conference on Computational Intelligence and Computing Research, Dec. 26-28, IEEE Xplore Press, Enathi, India, pp: 1-5. DOI: 10.1109/ICCIC.2013.6724292

Oumraou, L., 2009. Algorithmes et puzzles: Une ultime approche de Turing. Docteur agrégé de philosophie - Universite Paris I, France.

Wang, Y., J.F. Doherty and R.E. Van Dyck, 2002. A wavelet-based watermarking algorithm for ownership verification of digital images. IEEE Trans. Image Process., 11: 77-88. DOI: 10.1109/83.982816