14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASIP

ASYMMETRIC CRYPTOGRAPHY AS SUBSET OF DIGITAL HOLOGRAM WATERMARKING

Michele De Santis and Giuseppe Schirripa Spagnolo

Department of Electronic Engineering, Università degli Studi "Roma Tre"
Via della Vasca Navale n.84, 00146 Roma, Italy
phone: + (39) 06 55177046, fax: + (39) 06 5579078, email: schirrip@.uniroma3.it

ABSTRACT

In this paper we propose an asymmetric cryptography as subset of digital hologram watermarking, which is able to detect malicious tampering while tolerating some incidental distortions. It is a fragile watermark; in fact the mark is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation. The proposed technique could be applied to Color Images as well as to Gray Scale ones. Using digital hologram watermarking, the embedded mark could be easily recovered by means of a Fourier Transform. Due to this fact the host image can be tampered and watermarked with the same holographic pattern. To avoid this possibility we have introduced an encryption method using an asymmetric Cryptography. The proposed scheme is based on the knowledge of original mark from the Authentication Entity, for applying Image Correlation between this and the extracted one.

1. INTRODUCTION

The past few years have witnessed an increasing use of digitally stored information and the development of new multimedia digital servers. Digital images are gradually replacing their classic analogue counterparts. It is well known that digital images can be altered or manipulated with ease. Furthermore, it is generally impossible to tell whether a given image is authentic or has been altered subsequently to capture by some readily available digital image processing tools. This is an important issue in, for example, legal application, news reporting, medical and medical archiving, where we want to be sure that the digital image in question truly reflects what the scene looked like at the time capture [1].

Digital watermarking techniques have been developed to meet the needs of the growing concern caused by digital copyright protection and data security. There have been different types of watermarks proposed in the literature, designed for different applications [2]. Digital watermarking can be classified into two major categories based on their application domains. The two categories are robust and fragile.

Robust watermarks are intended for copyright protection. It has been a common view that the mark inserted should be resistant to destruction under image processing operations, which involve pixel value manipulation. On the other hand, a "fragile" invisible watermark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarks is in content authentication. A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation [3, 4]. Fragile marks are not suited for enforcing copyright ownership of digital images; an attacker would attempt to destroy the embedded mark and fragile marks are, by definition, easily destroyed. The sensitivity of fragile marks to modification leads to their use in image authentication.

In the security community, an integrity service is unambiguously defined as one which insures that the sent data and received data are identical. This binary definition can also be applicable to images; however it is too strict and not well adapted to this type of digital document. Indeed, in real life situations, images will be transformed. Their pixel values will therefore be modified but not the actual semantic meaning of the image. In other words, the problem of image authentication concerns the image content, for example, when modifications of the document may change its meaning or visually degrade it. In order to provide an authentication service for still images, it is important to distinguish between malicious manipulations, which consist of changing the content of the original image such as captions or faces, and manipulations related to the use of an image, such as format conversion, compression, filtering, and so on. Unfortunately this distinction is not always clear, it partly depends on the type of image and its use. Indeed the integrity criteria of an artistic masterpiece and a medical image will not be the same. In the first case, a JPEG compression will not affect the perception of the image, whereas in the second case it may discard some of the fine details which would render the image totally useless [5].

The scope of this paper is to present a fragile invisible watermarking for digital image authentication. In this paper, we extend the secret key verification watermarking, proposed in [6, 7], into a public key scheme so that the integrity and ownership of the image can be verified using a public key. In such a system, the owner of the image inserts a watermark using a private key SK. In the watermark extraction procedure, any person can use the public key PK (corresponding to the private key SK).

A possible schema to encode the watermark is shown in Figure 1a.

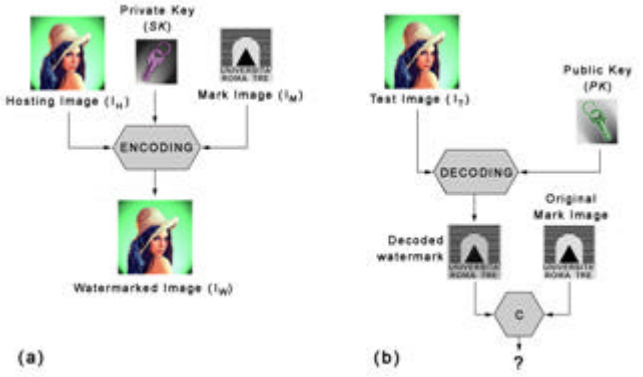

Figure 1 - Encoding, decoding, and comparing embedded watermarks in a digital image. In the encoding process (a), a content creator/owner inserts a mark into an original digital image. In the decoding process (b), a content owner checks a test image trying to recover a mark, and then compares the recovered image with the original inserted one.

In the encoding process a content creator/owner inserts a watermark into an original image. When a user receives a test image, he uses the detector to evaluate the authenticity of the received image. The detection process requires knowledge of "side information". The side information is the public key and image of the mark. A possible scheme to decode a watermark is shown in Figure 1b.

To compare the recovered watermark to the original insert one, generally, statistical tests are used. In this work we use the correlation coefficient as statistic test.

In this paper we propose Digital Hologram code techniques, adopted and designed to detect any unauthorized modification for the purpose of image authentication.

This paper is organized as follows. In Section 2, we briefly introduce the method used for the construction of the Digital Hologram (DH), the embedding watermark processes and the detecting watermark method. Section 3 discusses the cryptographic enhancement. Experimental results are given in Section 4. Finally, Section 5 contains our conclusions and future prospective.

2. CONSTRUCTION OF THE DIGITAL HOLOGRAM

Digital Hologram (DH) is a holographic technique in which the diffraction pattern to be used as a hologram is numerically generated by a computer and then the image is numerically reconstructed. The DH, of a mark image, can be considered as a pseudo-noise mask which will be the input data of the watermarking algorithm.

In our work, we used a binary mark: the "ROMA TRE" logo. First of all, the image of the mark is resized to a fourth of the dimensions of the hosting image. Subsequently, it is duplicated and positioned inside a structure with the same dimensions as the image which must be marked, as like that as shown in Figure 2a. The mark image, so modified, is elaborated, using appropriate mathematical transformations and coding algorithms, to generate the grayscale diffuse-type Fourier-transformed hologram (DH) of it (see Figure 2b). We made this manipulation for simulating an off-axis holography. The scope of this paper is not to explain the realization of such type as DH, for which references can be found in literature [8-15].

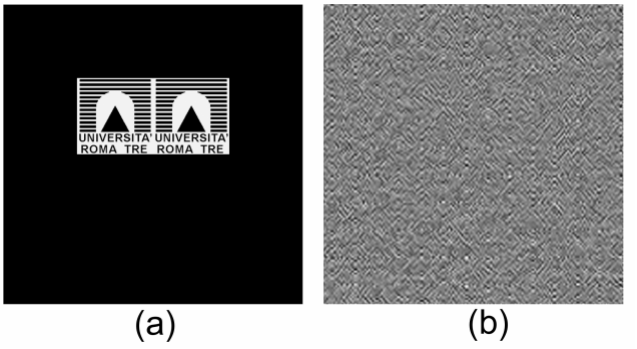

Figure 2 - Resizing and zero padding of the "ROMA TRE" logo (a) and related diffuse-type Fourier transformed hologram (b)

In the reconstruction phase we obtain four copies of the mark image positioned to the four corners of the frame (see figure 3). These four copies are due to the Twin Image Effect, which reproduces, in the reconstruction phase, two copies, symmetrically respectful to the center of the image, for each image presents into the original mark.

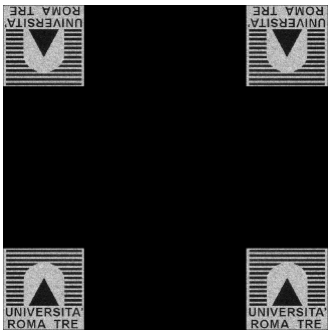

Figure 3 - Mark reconstructed from the hologram shown in figure 2(b)

The DH of the mark image is embedded into the hosting image, resulting in the content fragile watermarking.

Before embedding the CGH, a suitable lowpass filter, in frequency domain [16], is applied to the hosting image. In this way all high frequency information is eliminated from the hosting image.

This operation is necessary because the watermarking schema foresees that the mark can be extracted from the marked image spectra. For this reason the spectra of the obtained filtered image and the spectra of the DH (i.e. the original mark) have to be spatially separated. By means of the high frequency filtering the image spectra is concentrated only in the low and medium frequencies, whereas the DH spectrum is only in high frequency.

3. CRYPTOGRAPHICAL ENHANCEMENT

For creating a Fragile Watermarking scheme useful for image authentication, we have encrypted the mark with an appropriate cryptographic method. Because an asymmetric cryptosystem is used, we not only can verify that the image has not been tampered with, we can also identify the origination of the image.

The used cryptographic technique is derived from the AES [17] and from RSA cryptosystem [18].

Using a pseudo-random number generator we create two different vectors (one for rows and one for columns), called $\mathbf{Rand}_{ROW}$ and $\mathbf{Rand}_{COL}$, with dimensions equal to the number of rows and columns of the mark image respectively. After applying a shift rotation operation to each pixel of each row, using as offset the related $\mathbf{Rand}_{ROW}$ element value (i.e. for shifting the i-th row pixels, we use the i-th $\mathbf{Rand}_{ROW}$ element). The same approach is repeated also for each pixels of each column, using the other random vector, $\mathbf{Rand}_{COL}$.

In following Figure 5 the complete path applied to a 6x6 matrix is shown.

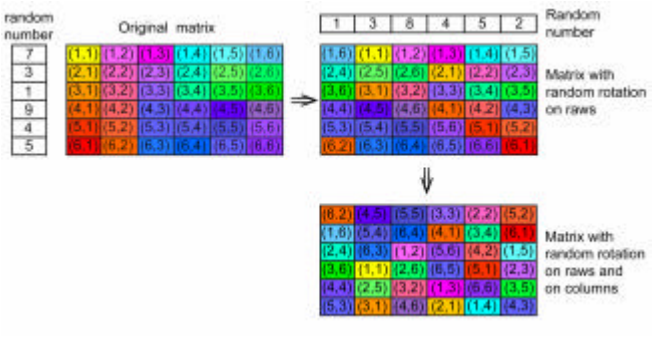

Figure 5 - Example of complete encryption path applied to a 6x6 Image. The resulting Image is completely similar to random noise.

To make the cryptosystem, we have applied, to the $\mathbf{Rand}_{ROW}$ and $\mathbf{Rand}_{COL}$ vectors, an asymmetric cryptographic algorithm (RSA algorithm). In asymmetric cryptography, the key for the encryption is not the same as the key for the decryption. Each user has two keys: a Public Key (PK), which is known to all, and Private Key (SK), which is kept secret (private).

With this vector we realize the encryption of the mark. The cipher mark is inserted, in the hosting image, using a appropriate weight value. In this way, we realize the CGH watermarking. Subsequently, sender (Alice) encrypts $Rand_{ROW}$ and $Rand_{COL}$ vectors with the secret key of RSA algorithm obtaining two new vectors E_Rand_{ROW} and E_Rand_{COL}(the data are partitioned into blocks, the number of the vector, and the encryption is applied to those blocks sequentially so that lost of ending blocks will not affect the blocks before them; losing a block would mean to lose only a row or a column of the mark). In this way Alice digitally signs document, establishing she is document owner/creator. When recipient (Bob) gets the signed document extracts the mark, embedded in the watermarking image, by means of a appropriate FFT technique. This mark must be decrypted by means of $\mathbf{Rand}_{ROW}$ and $\mathbf{Rand}_{COL}$ vectors. The $\mathbf{Rand}_{ROW}$ and $\mathbf{Rand}_{COL}$ vectors can be obtained from $\mathbf{E\_Rand}_{ROW}$ and $\mathbf{E\_Rand}_{COL}$ using the public key of Alice. Bob obtains $\mathbf{Rand}_{ROW}$ and $\mathbf{Rand}_{COL}$ vectors signed by Alice by applying Alices's public key to $\mathbf{E\_Rand}_{ROW}$ and $\mathbf{E\_Rand}_{COL}$.

$$\underbrace{\left.\begin{aligned}\mathbf{E\_Rand}_{ROW} &= \left(\mathbf{Rand}_{ROW}\right)^{d} \bmod (n)\\ \mathbf{E\_Rand}_{COL} &= \left(\mathbf{Rand}_{COL}\right)^{d} \bmod (n)\end{aligned}\right\}}_{Alice}$$

$$\Downarrow \text{ sending to Bob}$$

$$\Rightarrow \underbrace{\left\{\begin{aligned}\mathbf{Rand}_{ROW} &= \left(\mathbf{E\_Rand}_{ROW}\right)^{e} \bmod (n)\\ \mathbf{Rand}_{COL} &= \left(\mathbf{E\_Rand}_{COL}\right)^{e} \bmod (n)\end{aligned}\right.}_{Bob} \quad . \qquad (1)$$

$$\text{Alice's key} \begin{cases}(n,e) \text{ public}\\ (n,d) \text{ private}\end{cases}$$

Therefore Bob can prove to someone that Alice, and no one else (including Bob), must have signed document .

The Figure 6 shows the complete scheme of CGH watermarking.

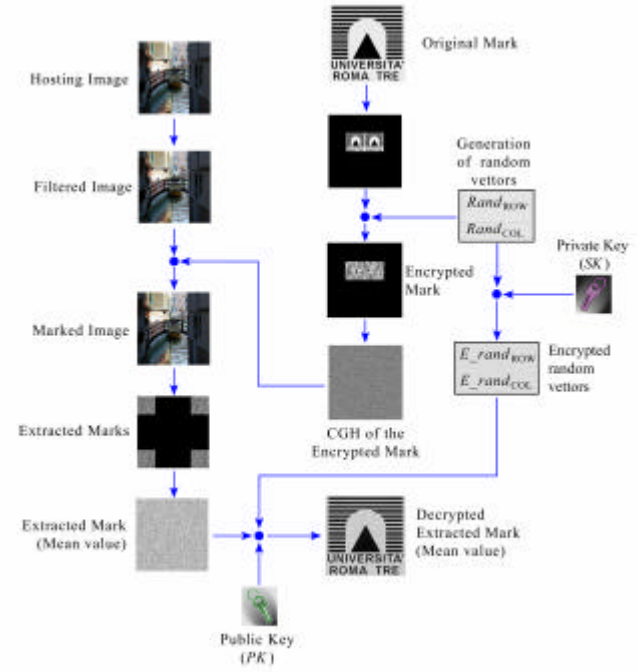

Figure 6 - The images show the entire algorithm sequence

The considered holographic technique sticks a speckle noise into the mark, once inserted into the host image. This added noise avoids the possibility of forging watermarked image, by simply copying the watermark from a watermarked image to any arbitrary image with the same size, without leaving a trace of it. In fact, forging an image, in this way, would bring

the recovered mark to have a very low cross-correlation (this is because the mark has been inserted twice and this brings to add the speckle noise twice into the recovered mark). So, using one not re-editing image, as a picture, this copying watermarking is not practicable.

4. EXPERIMENTAL RESULTS

In our tests, we have used hosting images (both color and gray level) with dimension 1024 x 1024 pixels. Each one has been filtered for allowing the correct mark insertion. The used mark was the B/W "ROMA TRE" logo with dimensions 256 x 256 pixels. It has to be underlined that we have no limitation in image and mark dimensions; in fact we resize the mark to 1/4 of the width and 1/4 of the height of the hosting image. In our schema we do not use the mark as it is, but the hosting image is marked by means of the encrypted version of it. To compare the recovered watermark to the originally inserted one, and then verify the presence of forgery and/or tampering, the correlation coefficient is used as a statistic test.

The invisible fragile watermarking technique, described in previous paragraphs, allows the detection of any change to a watermarked image.

Figure 7(a) shows a hosting image and figure 7(b) shows an image with an invisible watermark added using a weigh α=0.008. It clearly demonstrates that the watermark is invisible.

Figure 7 - (a) Hosting image. (b) An invisible watermarking added to the hosting image. (c) Extracted watermarking

If one uses the correct keys in the watermark extraction procedure shown in figure 7(b), he can obtain the output image shown in figure 7(c), indicating the presence of a proper watermark.

An important advantage, of the proposed method, is that, it is robust to the possible loss of bits in the transmission of the digital signature (transmission of $\mathbf{E\_Rand}_{ROW}$ and $\mathbf{E\_Rand}_{COL}$ vectors). In fact, the method is able to correctly recover, the hidden mark, even with a loss of data more than 1/100 bits. Figure 8(a) shows an image marked with "ROMA TRE" logo (using an α=0.004). Figure 8(b) shows the mark extracted in presence of a loss of equal data to 6 bits on 512.

Figure 8 - (a) Image marked with "ROMA TRE" logo. (b) Extracted watermarking in presence of a loss of equal data to 6 bits on 512. (coefficient of correlation 0.90 – without loss of data the coefficient of correlation is 0.96)

Another important property is that, if one changes a certain number of pixels in the watermarked image, the procedure returns a noisy mark and lowers the correlation coefficient. Figure 9(a) shows a picture of Venice marked with "ROMA TRE" logo. In this case we have used an α=0.004. Figure 9(b) shows a modification of the Figure 9(a). Figure 9(c) shows the mark extract by the picture without modification and Figure 9(d) the mark extract after modification.

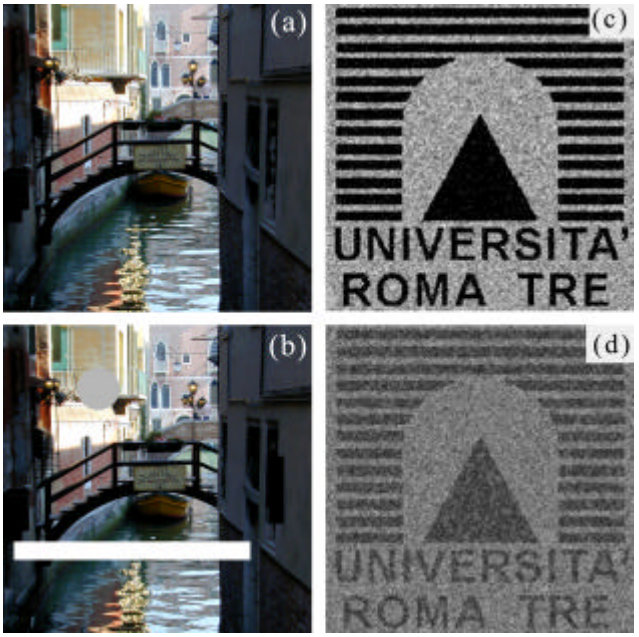

Figure 9 - (a) An invisible watermarking added to the picture of Venice. (b) Picture of Venice with modification. (c) Extracted watermarking from image without modification (coefficient of correlation 0.96). (d) Extracted watermarking from image with modification (coefficient of correlation 0.64). Structure of an all-optical packet router.

5. CONCLUSIONS AND FUTURE PROSPECTIVE

In the CGH watermarking proposed in literature, we have the problem of the impossibility to apply a cryptographic approach with a pure substitution method. In fact, in CGH watermarking, the reconstructed mark image is similar, but not equal to the embedded one. For this reason it is impossible, using a substitution table, such as direct AES or RSA methods, to substitute the encrypted CGH amplitude values with a different value (e.g. if the i-th pixel has value 125 and we substitute this value with 56, we have the necessity to extract in reconstruction phase exactly the value 56, but in our solution we can extract, for instance, the value 78, so the decoding is not possible).

In this paper, we have presented an enhanced version of the CGH Watermarking, based on a newly cryptographic approach based on an Asymmetric Key algorithm. The proposed method consents to use the CGH watermarking as digital signature. Therefore, it is suitable for marking images, such as the ones of medical databases or a database of fingerprints, to avoid fraudulent tampering. Unfortunately, the method is not suitable for the authentication of images exchanged by Internet. In fact, in the transmission on the net, image distorted by common image processing, such as JPEG "lossy compression", should be accepted. In our method, when the watermarked images undergo a JPEG compression the watermark is destroyed.

In relation to other fragile watermarking methods, the proposed method introduces the concept of public key cryptography, necessary for assuring the correct creator's authentication. In addition this method has the advantages, for the field of interest, to be cropping-resistant and to be resistant also to the lost transmission data.

Besides, further studies must be begun to make the system even suitable for the authentication of images exchanged over the Internet.

REFERENCES

[1] P.W. Wong, N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification," *IEEE Trans. Image Processing* vol. 10(10), pp. 1593-1601, 2001.

[2] N. Memon, P.W. Wong, "Protecting digital media content: Watermarks for copyrighting and authentication," *Commun. ACM*, vol. 41, pp. 35-43, 1998.

[3] M.M. Yeung, F.C. Mintzer, "Invisible watermarking for image verification," *J. Electronic Imaging*, vol. 7(3), pp. 578-591, 1998.

[4] E. T. Lin, E. J. Delp, "A Review of Fragile Image Watermarks," *Proc. of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents*, Orlando, FL, October 1999, Orlando, FL, pp. 25-29.

[5] C. Rey, J.L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication," *EURASIP Journal on Applied Signal Processing*, vol. 6, pp. 613–621, 2002.

[6] G. Schirripa, C. Simonetti and L. Cozzella, "Fragile Digital Watermarking by Synthetic Holograms," Proc. SPIE vol. 5615 European Symposium on Optics/Fotonics in security & Defence, London, UK, 25-28 October 2004, pp. 173-182.

[7] G. Schirripa Spagnolo, C. Simonetti, L. Cozzella, "Content fragile watermarking based on computer generated hologram coding technique," *J. Opt. A: Pure Appl. Opt*., vol. 7(7), pp. 333-342, 2005.

[8] W. R. Lee, "Sampled Fourier transform hologram generated by computer," Appl. Opt., vol. 9(3), pp. 639- 643, 1970.

[9] W. R. Lee, Computer Generated Holograms: techniques and applications, Progress in Optics 16 (1974) 121-231.

[10] Y. Aoki, Watermarking Technique Using Computer-Generated Holograms, *Electronics and Communications in Japan*, Part 3, vol. 84(1), pp. 21-31, 2001.

[11] L. Croce Ferri, Visualization of 3D information with digital holography using laser printers, *Computers & Graphics* vol. 25(2) pp. 309-321, 2001.

[12] J. Dittmann, L. Croce Ferri, C. Vielhauer, "Hologram Watermarks for Document Authentications," *IEEE International Conference on Information Technology: Coding and Computing*, IEEE Computer Society, Las Vegas, NV, USA, 2-4 April 2001, pp. 60-64.

[13] L. Croce Ferri, A. Mayerhöfer, M. Frank, C. Vielhauer, R. Steinmetz, "Biometric Authentication for ID Cards with Hologram Watermarks," *Proc. SPIE* vol. 4675, Photonic West, Security and Watermarking of multimedia contents IV, San Jose, CA, 19-25 January 2002, pp. 629-640.

[14] N. Takai and Y. Mifune, "Digital watermarking by a holographic technique," *Appl. Opt*., vol. 41(5), pp. 865-873, 2002.

[15] X. Zhou, L. Chen, J. Shao, "Investigation of digital hologram watermarking with double binary phase encoding," *Optical Engineering*, vol. 44(6), pp. (067007)1–25, June 2005.

[16] R.W. Ramirez, *The FFT Fundamentals and Concepts*, Prentice Hall, Englewood Cliffs, NJ, 1985, Chapter 7, pp. 137-143.

[17] NIST FIPS 197 – Advanced Encryption Standard, 26 Nov 2001.

[18] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM 21(3) (1978) 120-126, 1978.