International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:11, 2008

Computer Generated Hologram for SemiFragile Watermarking with Encrypted Images

G. Schirripa Spagnolo, M. De Santis

Abstract**—**The protection of the contents of digital products is referred to as content authentication. In some applications, to be able to authenticate a digital product could be extremely essential. For example, if a digital product is used as a piece of evidence in the court, its integrity could mean life or death of the accused. Generally, the problem of content authentication can be solved using semi-fragile digital watermarking techniques. Recently many authors have proposed Computer Generated Hologram Watermarking (CGH-Watermarking) techniques. Starting from these studies, in this paper a semi-fragile Computer Generated Hologram coding technique is proposed, which is able to detect malicious tampering while tolerating some incidental distortions. The proposed technique uses as watermark an encrypted image, and it is well suitable for digital image authentication.

Keywords**—**Asymmetric cryptography, Semi-Fragile watermarking, Image authentication, Hologram watermark, Public-Key Cryptography, RSA.

I. Introduction

RECENTLY many authors have proposed Computer Generated Hologram Watermarking (CGH Watermarking) [1-5]. From these works, the potentiality emerges about the possibility to use the CGH watermarking as semi-fragile watermarking for images authentication [6, 7].

The specific interest in semi-fragile watermarking algorithms arises from the multitude of practical and commercial applications where contents need to be strictly protected, but the exact representation during exchange and storage need not be guaranteed.

Digital images are gradually replacing their classical analog 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 applications, news reporting, medical archiving, where people want to be sure that the digital image in question truly reflects what the scene looked like at the time of capture [8]. In particular, for medical images are very important the "Integrity" (the information has not been modified by non-authorized people), and the "Authentication" (a proof that the information belongs indeed to the correct patient and was issued from the correct source).

In this work an application of CHG Watermarking is presented, as semi-fragile watermarking for monitoring the integrity of the content of the image.

A semi-fragile watermarking monitors the integrity of the content of the image but not its numerical representation. Therefore the watermark is designed so that the integrity is proven if the content of the image has not been tampered. However if parts of the image are replaced, the watermark information should indicate evidence of forgery.

The sensitivity of fragile marks to modification leads to their use in digital image authentication. That is, it may be of interest for parties to verify that a digital image has not been edited, damaged, or altered since it was marked. Image authentication systems have applicability in law, commerce, defense, and journalism [9-13].

The paper presents a complete schema, based on digital watermarking, to allow the verification of originality of the digital image. To have a better security, the proposed method uses a secret key. A possible schema to encode the watermark is shown in Figure 1a.

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 the "side information". The side information is the secret key and the image of the mark. A possible schema to decode a watermark is shown in Figure 1b. To compare the recovered watermark to the original insert watermark, generally, statistical tests are used. In this work the correlation coefficient is used as test statistic.

The proposed technique has some advantages and disadvantages compared to other schemas. First of all it is cropping resistant, due to the particular intrinsic characteristics of the used CGH watermarking. In addition, the proposed cryptographic schema allows to have a secure watermarking resistant to data loss; in fact it is possible to extract mark information also from a watermarked image, transmitted on a noise channel, in which the two random key vector could be degraded (i.e. some element could be lost).

Manuscript received April 19, 2007.

G. Schirripa Spagnolo is with the Università degli Studi "Roma Tre", Dipartimento di Ingegneria Elettronica, Via Della Vasca Navale 84, I-00146, Roma (Italy) (corresponding author to provide phone: +39 0655177046; fax: +39 065579078; e-mailschirrip@uniroma3.it).

M. De Santis is with the Università degli Studi "Roma Tre", Dipartimento di Ingegneria Elettronica, Via Della Vasca Navale 84, I-00146, Roma (Italy).

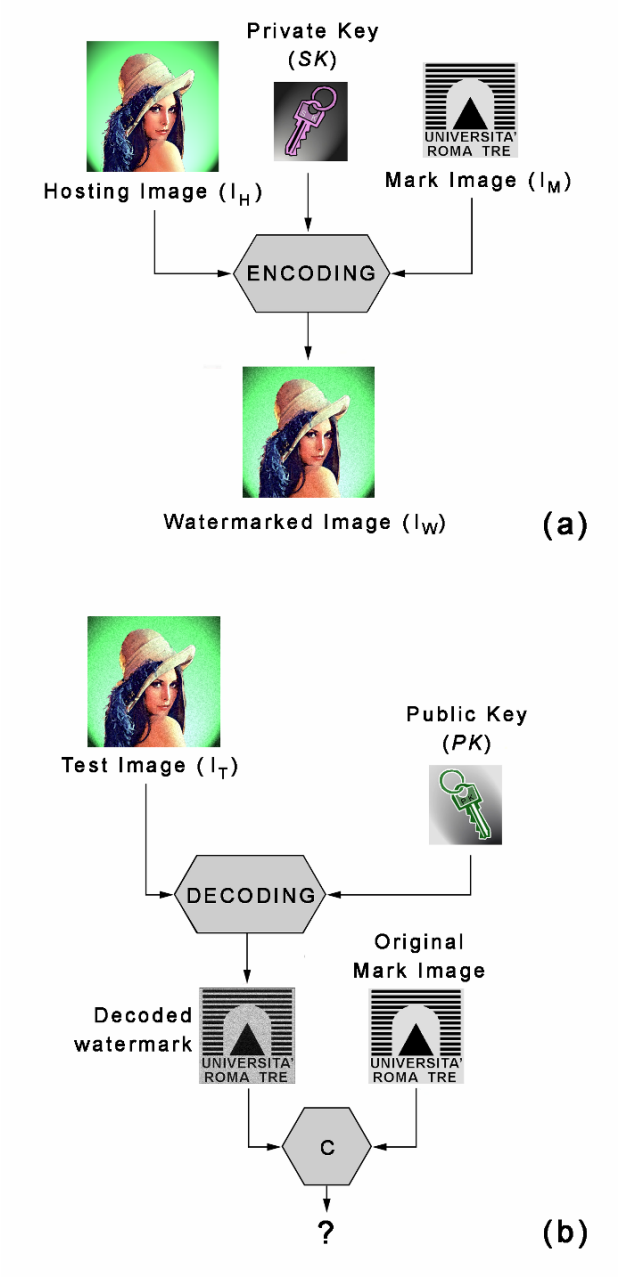

Fig. 1 Encoding, decoding, and comparing embedded watermarks in a digital image. In the encoding process (a), a content creator/owner inserts a watermark into an original digital image. In the decoding process (b), a content owner checks a test image to recover a watermark, and then compares the recovered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

The remainder of this paper is organized as follows. The CGH construction, insertion and extraction are described in Sec. 2. Information on the cryptographic solution adopted in this paper is addressed in Sec. 3. Experimental results are presented in Sec. 4. Eventually Sec. 5 contains conclusions.

II. Fragile Watermarking Based on Computer Generated Hologram Coding Techniques.

Watermark is a digital, stubborn, signature used for identifying possible malicious data manipulations or for certifying Intellectual Property Right (IPR). Two different classification schemas exist for watermarks, one based on mark "visibility", and another based on mark "robustness". In the first case we have Visible Watermarks and Invisible Watermarks. In the second case we have Robust Watermarks and Fragile Watermarks.

Each watermarking schema has a different set of property to be addressed to. For example invisible ones have the necessity to be not detectable at human sight, robust ones have the requirement to be not simply removable even if the hosting image is manipulated, filtered, cropped and so on.

In the application of digital image authentication, the desirable features of fragile marking systems are:

- the impossibility to reintroduce a mark into a photo after its extraction;
- the destruction of the mark in case of manipulation;
- the mark invisibility.

The proposed technique, of watermarking based on Computer Generated Hologram (CGH), has the important advantage that a content-fragile schema can be defined: every manipulation changing the visual content of the cover can be detected. Another important characteristic of hologram watermarks is that, even if the embedded data are content-related to the cover, they are noise-like and therefore difficult to be detected and removed.

A. Overview on Computer Generated Hologram construction.

Optical holography is a technique by which both the amplitude and phase of optical field diffracted from an object of interest are recorded as a hologram in the form of interference fringes. When the optical field diffused from the object is recorded as hologram, the hologram becomes very similar to a random pattern, because the interference fringes of randomly phase-modulated waves are recorded in the hologram with high density. Nevertheless, the original image of the object can be recovered from the hologram. A Computer Generated Hologram (CGH) image is a hologram computed by numerically simulating the physical phenomena of light diffraction and interference. Also the CGH is similar to a random pattern. Therefore, if we use a CGH of a mark image as input data of the watermarking algorithm, it can be considered as pseudo-noise mask.

The production of hologram using a computer has been discussed in detail in Ref. [14], here only the necessaries are presented, to understand the following discussion.

In this paper, the mask image is hidden in a form of a Fourier-transformed digital hologram of diffused type. Unfortunately, this type of hologram produces, in reconstruction, twin effect (these copies, superimposing themselves, provoke loss of information). To avoid this problem, off-axis hologram is simulated, by means of the

following procedure. First of all, the image of the mark ($\mathbf{I}_M$) is resized to an eighth of the dimensions of the hosting image, or, if necessary, to a sixteenth. Subsequently, it is duplicated and positioned inside a structure with the same dimensions as the hosting image which must be watermarked. In this way we obtained the modified mark image ($\mathbf{I}_{MM}$), as like that as shown in Figure 2 (here we used, as mark, the "ROMA TRE" university logo), used to construct the CGH.

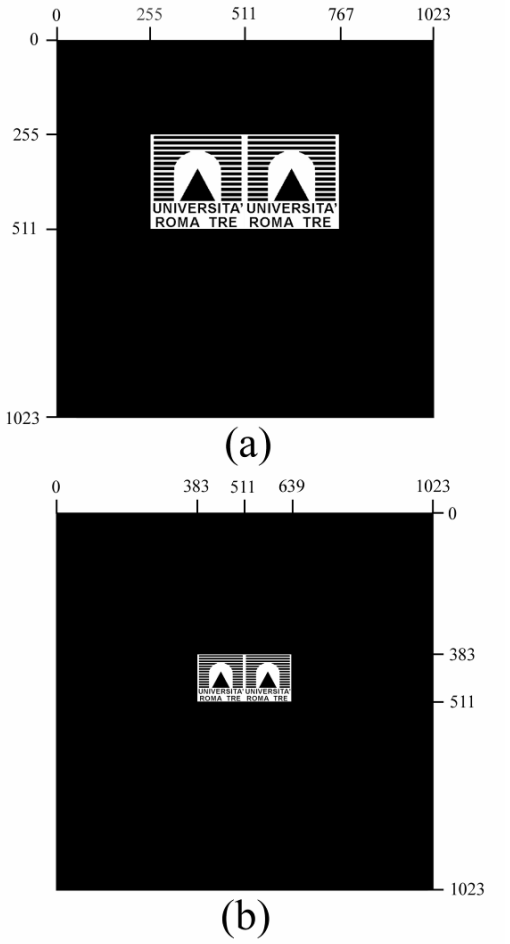

Fig. 2 Resizing and zero padding of the "SPIE" logo. (a) "SPIE" logo, at 256 x 256 pixels, padded in a 1024 x 1024 zero matrix (mark at an eight of the image size). (b) "SPIE" logo, at 128 x 128 pixels, padded in a 1024 x 1024 zero matrix (mark at a sixteenth of the image size).

To make Fourier-transformed digital hologram, the $\mathbf{I}_{MM}$ image is modulated by a random phase mask $\exp[i\phi(\xi, \eta)]$.

The two-dimensional phase $\phi(\xi, \eta)$ is given by random numbers. The $\mathbf{I}_{MM}$ image modulated by the random phase is subsequently numerically Fourier transformed.

$$T(x,y) = FFT\left\{I_{MM}(\xi,\eta)\exp\left[i\phi(\xi,\eta)\right]\right\} . \quad (1)$$

Now, each element (x, y) of the matrix **T** is divided in four sub-elements. The first sub-element represents the real and positive part of $T(x, y)$ (0° angle in the corresponding phasor notation); the second one represents the imaginary and positive part of $T(x, y)$ (90° angle in the corresponding phasor notation); the third the real and negative part of $T(x, y)$ (180° angle in the corresponding phasor notation); eventually the last one represents the imaginary and negative part of $T(x, y)$ (270° angle in the corresponding phasor notation).

After this procedure, the resulting matrix has a dimension four times greater than the original one, due to the fact that each original pixel is now represented by four values. To obtain the CGH with the same dimension of the original image, we have substituted each set of four values, with the related average, made by linear interpolation. In this way we obtain the matrix **SH** which represents our Computer Generated Hologram (also called Synthetic Hologram).

B. Watermarking technique – CGH insertion procedure

The matrix **SH** of the mark image is embedded into a hosting matrix image $\mathbf{I}_H$, resulting in the fragile watermarking by means of CGH.

Before embedding the **SH**, the hosting image $\mathbf{I}_H$ is filtered, using the FFT domain, by a Hamming circular filter. In this way all high frequency information is eliminated from the 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 ($\mathbf{I}_F$) and the spectra of the **SH** have to be spatially separated. By means of the high frequency filtering the hosting image spectra is concentrated only in the low and medium frequencies, whereas the **SH** spectrum is only in high frequency. The Hamming Filter used is:

$$\text{if} \quad (x-x_c)^2 + (y-y_c)^2 \le R$$
$$\Downarrow$$
$$0.08 + 0.46 \cdot \left\{1 - \cos\left[\frac{\pi\sqrt{(x-x_c)^2+(y-y_c)^2}}{R} - \pi\right]\right\} \quad (2)$$
$$\text{Otherwise} \quad \Rightarrow \quad 0$$

Where R is the Filter radius and (x_c, y_c) is the filter center position. In this case (x_c, y_c) correspond to the center of the $\mathbf{I}_H$ spectra, and R is chosen so that the frequency information of the image is not overlapped with **SH** information. Using a mark of an eight of the hosting image, it is necessary a relative small radius, otherwise, using a mark of a sixteenth of the image, it is possible using a relative large radius. Obviously, the usage of a relative small R, it is possible with low detailed images. Figure 3 shows a parrot filtered with the radiuses used in the above-mentioned cases. In particular in Figure 3(a) is shown the original image, while Figure 3(b) and 3(c) show the filtered images. Eventually in Figure 3(d) is shown a detail of original and filtered images. The Figure 3 shows that the usage of this kind of filter does not decrease the detail level.

Fig. 3 The "parrot" images. (a) Original Image; (b) Filtered Image used for inserting a mark of an eight of the image dimensions – using an host image of 1024 x 1024 with an R = 512; (c) Filtered Image used for inserting a mark of a sixteenth of the image dimensions – using an host image of 1024 x 1024 with an R = 1024; (d) Details of the original image and the filtered ones highlighting that the used filter does not damage the image quality.

Before introducing **SH** inside the filtered image, it is modified to take into account the human eye contrast response. The previous transformation made possible by applying a brightness-dependent attenuation, in which is applied a greater attenuation value to the lighter image pixels than to the darker ones:

$$SH_{MD}(x,y) = \alpha\left[SH(x,y)\cdot 2I_F(x,y) + SH(x,y)\right]. \quad (3)$$

In equation (3) we have considered both **SH** and $\mathbf{I}_F$ normalized between zero to one in the Image Space. In this way the weight of the **SH** is three time greater on high intensity level pixels. This value is evaluated in empirical way. In other words, during our experiments we have used different weight values of darkened and lightened pixels. The choice of the value 3 is due to optimize the ratio between content information inside the marked image and invisibility.

From now on, $\mathbf{SH}_{MD}$ indicates the synthetic hologram utilized in the SHW schema, see figure 5(a). This value is subtracted to the filtered image $\mathbf{I}_F$, obtaining the watermarked image $\mathbf{I}_W$.

The parameter α controls the fragility of the content insert in the host image. For medical or military images the best value of α is 0.004. For image of news reporting it is possible to use α = 0.01 or more; in this way the content is more resistant to accidental distortion related to the use of images.

The resulting image has a difference in comparison with the initial one. To obtain the marked image with the same dynamic of the hosting image, the marked image is obtained by the following equations:

$$\mathbf{I}_W = \left\{ \frac{\left(\mathbf{I}_F - \mathbf{SH}_{MD}\right) - \min\left[\mathbf{I}_F - \mathbf{SH}_{MD}\right]}{\max\left[\mathbf{I}_F - \mathbf{SH}_{MD}\right] - \min\left[\mathbf{I}_F - \mathbf{SH}_{MD}\right]} \cdot \left(\max\left[\mathbf{I}_H\right] - \min\left[\mathbf{I}_H\right]\right) \right\} + \min\left[\mathbf{I}_H\right]. \quad (4)$$

The equation (4) shows that the watermarked image ($\mathbf{I}_F$ - $\mathbf{SH}_{MD}$) is firstly normalized between the values 0 and 1, and then its dynamic range is equalized to the $\mathbf{I}_F$ one. Finally the obtained values are shifted to the minimum value of the original image. In this way the marked image $\mathbf{I}_W$ is statistically similar to the original one, with an increasing in mark invisibility.

The pipeline used to obtain the watermarking image by means of this procedure is synthesized in Figure 4. This figure shows as the Fragile Image Watermarking by Computer Generated Holograms method can be applied either to Gray Scale hosting images, or to RGB Color ones, working on each color channel.

C. Watermarking technique – Mark Detection Procedure

To recover the mark from the watermarked images the procedure is very easy. On the watermarked image $\mathbf{I}_W$ the FFT

is performed, obtaining four copies of the mark image positioned on the four corners of the frame, see figure 5(b).

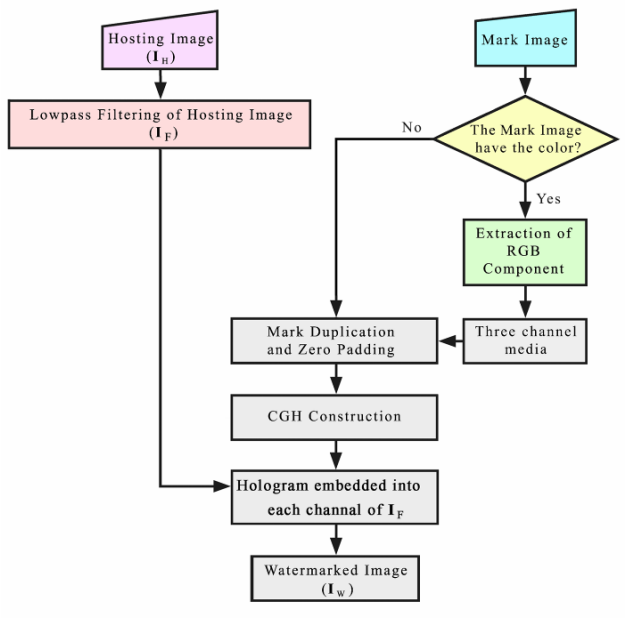

Fig. 4 Pipeline for the production of the CGH- Watermarking.

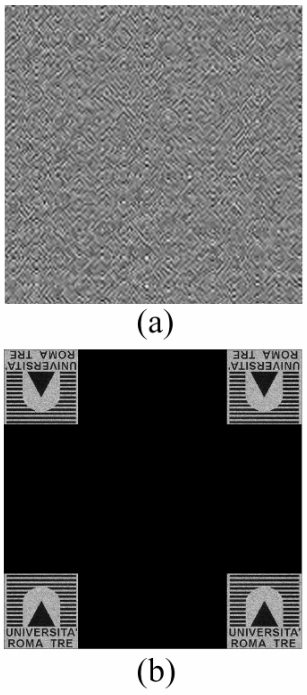

Fig. 5 (a) Production phase: synthetic hologram of the mark; (b) Detection phase: mark's copies on the four corners of the frame.

These four copies are due to the Twin Image Effect, which reproduces, in reconstruction phase, two copies, symmetric with respect to the image's center, of the figures present in the zero-padding of the original mark. Unfortunately, due to the necessity to use a random phase to spread, into all the numerical FFT range, the information related to the mark, the reconstructed image is affected by a speckle pattern. To mitigate this problem, the four extracted copies of the mark are averaged.

The so obtained extracted mark is compared with the original one, by a Threshold Correlation.

If the recovered mark is extracted from a cropped image (with dimension different from the original image), the averaged mark's size is not equal to the originally inserted one. For this reason, to correctly apply the Threshold Correlation, the recovered mark is resized to the original one before the comparison.

III. Cryptographical Enhancement

At this point, for creating a Fragile Watermarking schema useful for image authentication, the mark has been encoded with an appropriate cryptographic signature. Because, a digital signature is used, it is not only possible to verify that the image has not been tampered with, but also identify the origination of the image. The used cryptographic signature is derived from the AES and from RSA cryptosystem [15].

Two different vectors (one for rows and one for columns) are generated using a pseudo-random number generator, they are called Rand_{ROW} and Rand_{COL}, with dimensions equal to the number of rows and columns of the mark image respectively. After, a shift rotation operation to each pixel of each row is carried out, using has offset the related Rand_{ROW} element value (i.e. to shift the i-th row pixels, the i-th Rand_{ROW} element is used). The same approach is repeated also for each pixels of each column, using the other random vector, Rand_{COL}.

In the following figure, Figure 6, the complete path applied to a 6 x 6 matrix is shown.

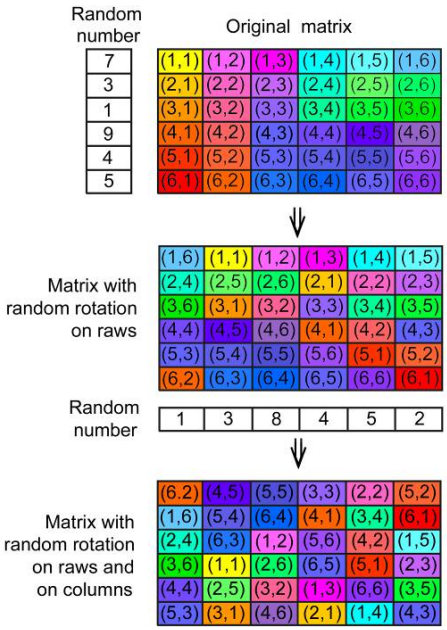

Fig. 6 Scheme used to encode the $\mathbf{SH}_{MD}$ of the mark.

To realize a cryptographic signature, it has been applied, to the Rand_{ROW} and Rand_{COL} vectors, an asymmetric cryptographic algorithm (RSA algorithm). In asymmetric cryptography, the key for the encoding is not the same as the key for the decoding. Each user has two keys: a Public Key (PK), which is known to all, and a Private Key (SK), which is kept secret (private).

A. Overview of the RSA Algorithm

The concept of an asymmetric cryptography (also called Public-Key Cryptography) was developed by Diffe and Hellman [16] and the first practical algorithm was published by River, Shamir and Adleman (RSA) [17]. The RSA algorithm is widely used in Public-Key Cryptography. It is based on the following property of numbers: it is easy to multiply two integers while it is very difficult to factor a number that is a product of two large primes. Even with the recent advances in computational number theory and in computer technology it is, in general, impossible to factor a 1024-bit integer, which is the minimal size recommended by the current standards, within any reasonable amount of time. Like any other public key algorithm, RSA begins with the key generation procedure.

It is supposed to generate the needed asymmetric keys, to be used for signing a message.

Two random large prime numbers, p and q ,are chosen. It is computed $n = p \cdot q$. The factors p and q will remain secret. The product $n = p \bullet q$ is made public.

It is reckoned $\phi(n) = (p - 1) \cdot (q - 1)$.

It is chosen a small odd number, e, that is relatively prime to $\phi(n)$.

The number e (with $e < n$) has no common factors with $\phi(n)$ [e, $\phi(n)$ are "relatively prime"].

It is drawn d such that $e \cdot d$ -1 is exactly divisible by $\phi(n)$. In other words: $d = e - 1 \cdot \text{mod}[\phi(n)]$.

The public key is PK ≡ (n, e), while SK ≡ (n, d) is the private key.

RSA can also be used to sign a message. Suppose Alice wishes to send a signed message to Bob. She produces a hash value of the message, encodes it with her secret key, and attaches it as a "signature" to the message. This signature can only be decoded with her public key. When Bob receives the signed message, he decodes the signature with Alice's public key, and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of the message was in possession of Alice's secret key, and that the message has not been tampered with.

To sign a message **M** (must be smaller than n), Alice compute the signature $\mathbf{S} = \mathbf{M}^d \cdot (\text{mod } n)$. Anyone that knows the corresponding public key can verify the signature by checking whether $\mathbf{M} = \mathbf{S}^e \cdot (\text{mod } n)$.

Figure 7 shows the use of a digital signature realized by means of the RSA algorithm.

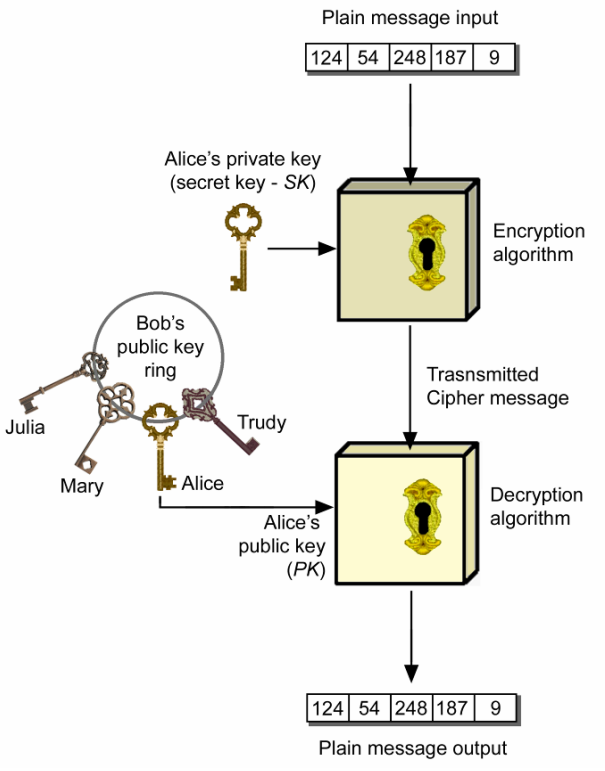

Fig. 7 Sender (Alice) digitally signs the document, establishing she is the document owner/creator. Recipient can prove to someone that Alice, and no one else (including recipient), signed the document.

B. Implementation of Public-Key Cryptography in CGH watermarking

As it has been said, using a pseudo-random number generator two different vectors are generated (one for rows and one for columns), called $Rand_{ROW}$ and $Rand_{COL}$, with dimensions equal to the number of rows and columns of the mark image respectively. The mark's encoding is carried out with these vectors. The encoded mark is inserted, in the hosting image, using an appropriate weight value. In this way, the CGH watermarking is performed. Subsequently, sender (Alice) encodes $Rand_{ROW}$ and $Rand_{COL}$ vectors with the secret key of the RSA algorithm, obtaining two new vectors E_Rand_{ROW} and E_Rand_{COL}. In this way, Alice digitally signs the document, establishing she is the document owner/creator. When recipient (Bob) gets the signed document extracts the mark, embedded in the watermarking image, by means of an appropriate FFT technique. This mark must be decoded by means of $Rand_{ROW}$ and RandCOL vectors. The $Rand_{ROW}$ and $Rand_{COL}$ vectors can be obtained from E_Rand_{ROW} and E_Rand_{COL} using the public key of Alice. Bob obtains $Rand_{ROW}$ and $Rand_{COL}$ vectors signed by Alice by applying Alices's public key to E_Rand_{ROW} and E_Rand_{COL}.

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

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

$$\left.\begin{aligned}\mathbf{Rand}_{\mathrm{ROW}} &= \left(\mathbf{E\_Rand}_{\mathrm{ROW}}\right)^{e} \bmod (n)\\ \mathbf{Rand}_{\mathrm{COL}} &= \left(\mathbf{E\_Rand}_{\mathrm{COL}}\right)^{e} \bmod (n)\end{aligned}\right\} Bob \qquad (5)$$

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

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

The Figure 8 shows the complete scheme of the CGH watermarking.

IV. Experimental Results

During tests, hosting images have been used (both color ones and gray level ones) with dimensions of 1024 x 1024 pixels. Each one has been filtered to allow the correct mark insertion. The used mark was B/W "SPIE" logo with dimensions of 256 x 256 pixels (see Figure 2). It has to be underlined that there is no limitation in image and mark size; in fact the mark is resized to an 1/4 of the width and an 1/4 of the height of the hosting image. In this schema, it is not used the mark as it is, but the hosting image is marked by means of the encoded version of it. To compare the recovered watermark to the originally inserted one, and then verify the presence of a forgery and/or a tampering, the correlation coefficient is used as statistic test.

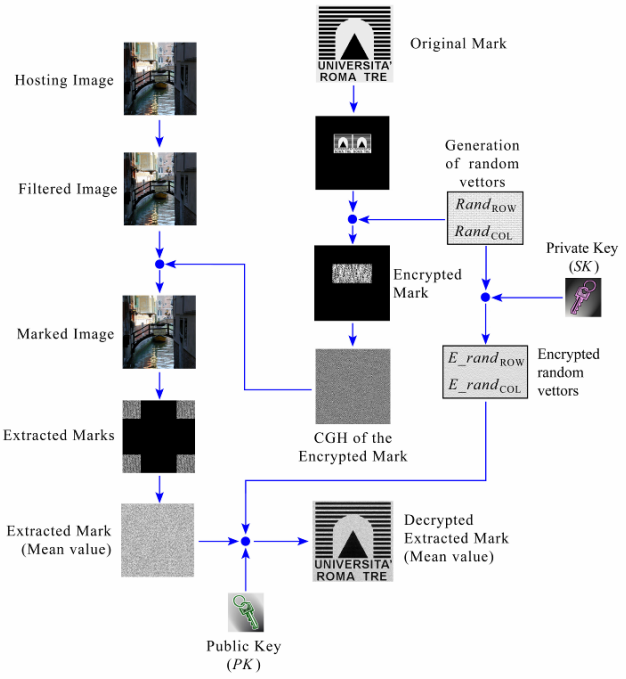

Fig. 8 Complete scheme of the CGH watermarking.

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

Figure 9(a) shows an hosting image and figure 9(b) shows an image. In this image an invisible watermark is added using a weight of $\alpha = 0.008$. It clearly demonstrates that the watermark is invisible.

If one uses the correct keys, then applies the watermark extraction procedure to figure 9(b), one obtains as output image, figure 9(c), indicating the presence of a proper watermark.

An important advantage, of the proposed method, is that it is robust to possible losses of bits during the transmission of the digital signature (transmission of E_Rand_{ROW} and of E_Rand_{COL} vectors). In fact, the method is able to recover, correctly, the hidden mark, even with a loss of data more than 1/100 bits.

Figure 10(a) shows an image marked with "Roma TRE" logo (using an α=0.004). Figure 10(b) shows the mark extracted in the presence of a loss of data equal to 6 bits over 512.

V. Conclusions

In the proposed CGH watermarking, there is the problem of the impossibility to apply a cryptographic approach with a pure substitution method. In fact, in this CGH watermarking, the reconstructed mark image is similar, but not equal to the embedded one.

Fig. 9 (a) hosting image; (b) watermarked image (α = 0.008); (c) extracted mark.

For this reason, it is impossible, to use a substitution table, such as direct AES or RSA methods, to replace the CGH amplitude values with the correspondent encoded one (e.g. if the i-th pixel of value 125 is replaced with 56, it is necessary to extract, in reconstruction phase, exactly the value 56, but this solution brings to extract, for instance, the value 78, so the decoding is not possible).

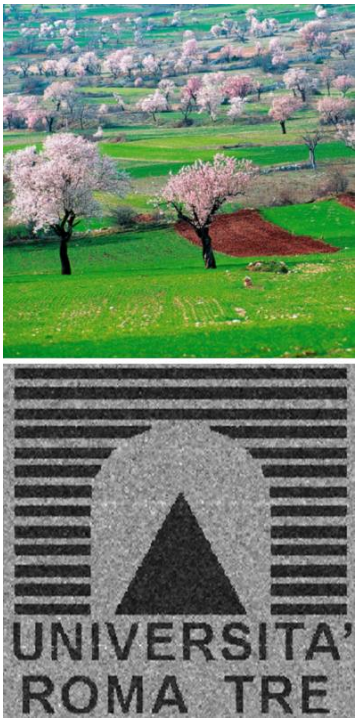

Fig. 10 (a) Marked image using a weight factor of 0.004.
(b) Mark extracted with loss of data of 6 bits over 512

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

Besides, further studies have to begin to make the system, even, suitable for the authentication of images exchanged over the Internet. In comparison with other fragile watermarking methods [4, 20-22], the proposed one introduces the concept of public key cryptography, necessary to assure 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 data loss transmissions.

REFERENCES

[1] Y. Aoki, Watermarking Technique Using Computer-Generated Holograms, Electronics and Communications in Japan, Part 3, 84(1) (2001) 21-31.
[2] L. Croce Ferri, Visualization of 3D information with digital holography using laser printers, Computers & Graphics 25(2) (2001) 309-321.
[3] 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.
[4] 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.
[5] N. Takai and Y. Mifune, Digital watermarking by a holographic technique, Appl. Opt. 41(5) (2002) 865-873.
[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. 7(7) (2005) 333-342.
[8] M.M. Yeung, F.C. Mintzer, Invisible watermarking for image verification, J. Electronic Imaging 7(3) (1998) 578-591.
[9] P.W. Wong, N. Memon, Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, IEEE Trans. Image Processing 10(10) (2001) 1593-1601.
[10] N. Memon, P.W. Wong, Protecting digital media content: Watermarks for copyrighting and authentication, Commun. ACM 41 (1998) 35-43.
[11] L.M. Marnel, C.G. Boncelet Jr., C.T. Retter, Spread spectrum image steganography, IEEE Trans. on Image Processing (1999) 1075-1083.
[12] 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.
[13] C. Rey, J.L. Dugelay, A Survey of Watermarking Algorithms for Image Authentication, EURASIP Journal on Applied Signal Processing 6 (2002) 613–621.
[14] W. R. Lee, Computer Generated Holograms: techniques and applications, Progress in Optics 16 (1974) 121-231.
[15] NIST FIPS 197 – Advanced Encryption Standard, 26 Nov 2001.
[16] W. Diffe, M. Hellman, New directions in cryptography, IEEE Trans. Information 22(6) (1976) 644-654.
[17] 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.

Giuseppe Schirripa Spagnolo was born in Locri (RC- Italy), in 1955. He received the degree cum laude in Physics, in 1978 from the Università della Calabria. From 1979 to 1984 he was Head of the R&D Section of S.E.A. (Strumentazione Elettronica Avanzata) in Rome. In 1985 he joined the Engineering Faculty of the University of L'Aquila (Italy) as an Assistant Professor. In 1998 he joined the Electronic Engineering Department of the University of "Roma Tre" as an Associate Professor. His research interests include electronic instrumentation and sensors, optical metrology and digital image processing. In these fields he has published more than 150 papers. He is a member of SPIE and IEEE and Italian association of Non-Destructive Testing (AIPnD - Associazione Italiana Prove non Distruttive Monitoraggio Diagnostica). He was the recipient (with D. Ambrosini) of the 2001 SPIE Kingslake Medal. Actual researches are based on developed of instrumentation and technique to use in the field of Security.

Michele De Santis received his degree in electronic engineering in 2005 from "Roma Tre" university, Rome Italy. He is currently working toward the PhD degree in electronic engineering at "Roma Tre" university. His research interests include digital watermarking and multimedia authentication.