Medical image integrity control combining digital signature and lossless watermarking

Wei Pan, Gouenou Coatrieux, Nora Cuppens-Boulahia, Frédéric Cuppens, Christian Roux

Medical Image Integrity Control Combining Digital Signature and Lossless Watermarking

W. Pan[1,3], G. Coatrieux[1,3], N. Cuppens-Boulahia[2,3], F. Cuppens[2,3]and Ch. Roux[1,3]

[1] Institut Telecom; Telecom Bretagne; Unite INSERM 650 LaTIM, Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3 France
e-mail: {wei.pan, gouenou.coatrieux, christian.roux}@telecom-bretagne.eu
[2] Institut Telecom; Telecom Bretagne; LUSSI Department, 2 rue de la Châtaigneraie, CS 17607, 35576 Cesson Sévigné Cedex France
e-mail: {nora.cuppens, frederic.cuppens}@telecom-bretagne.eu
[3] Université Européenne de Bretagne, France

Abstract. Enforcing protection of medical content becomes a major issue of computer security. Since medical contents are more and more widely distributed, it is necessary to develop security mechanism to guarantee their confidentiality, integrity and traceability in an autonomous way. In this context, watermarking has been recently proposed as a complementary mechanism for medical data protection. In this paper, we focus on the verification of medical image integrity through the combination of digital signatures with such a technology, and especially with Reversible Watermarking (RW). RW schemes have been proposed for images of sensitive content for which any modification may affect their interpretation. Whence, we compare several recent RW schemes and discuss their potential use in the framework of an integrity control process in application to different sets of medical images issued from three distinct modalities: Magnetic Resonance Images, Positron Emission Tomography and Ultrasound Imaging. Experimental results with respect to two aspects including data hiding capacity and image quality preservation, show different limitations which depend on the watermark approach but also on image modality specificities.

1 Introduction

With the advances of Internet technology, especially in healthcare, images can be cross-exchange in right time allowing new medical practice through for example telediagnosis, teleconsultation services. At the same time, ensuring the security of exchanged medical data becomes a major issue. Three mandatory characteristics need then to be addressed: confidentiality, availability and reliability based on the outcomes of information integrity and authenticity.

Current healthcare information systems are no longer based on a centralized architecture introducing the need for means to control distribution of medical contents in distributed infrastructures. Enforcing content protection using classical access control mechanisms is no longer sufficient. It is thus necessary to

develop security mechanisms that guarantee protection of medical contents in an autonomous way, especially their integrity and traceability.

In such a framework, watermarking has been shown as a complementary mechanism to enhance medical image security [1] [2]. In general speaking, Watermarking allows inserting a message, also called a watermark, in a host document by modifying the host content in an imperceptible way. For one image, the message is attached at the signal level slightly modifying its gray values. Whence, the hosted message and the host image are intimately associated independently of the image file format. By its ability to introduce a protection level the nearest as possible of the data, watermarking can rise up medical image reliability by asserting its integrity and its authenticity (i.e. an evidence that the information belongs to the correct patient and is issued from the right source). To do so, the embedded message may for instance correspond to a digital signature of the image pixels [3] [4].

For medical images, it is widely expected that the watermark should not hinder the qualitative perception of the image. This constraint implies that the interpretation of the image by a specialist shall remain unchanged after message insertion. However, the majority of watermarking methods irreversibly alters the image. Distortions may be low-level when the watermark insertion is weighted by use of a visual perception model [5], but to our knowledge none of these models has been validated in the case of medical imaging. Consequently, these distortions may mask some subtle image details.

Reversible or lossless watermarking has been proposed to overcome this issue. It allows the user to reconstruct the original image after having extracted the watermark (i.e. by removing image distortion). However, once the watermark has been removed, the image is no more protected, just like for data encryption. So even if removing the watermark is possible, most applications have a high interest to keep it as long as possible in the image in order first to continuously protect the information and second to not limit image interpretation to compliant systems (i.e. with watermarking abilities). Whence, in our view, even for reversible watermarking, the imperceptibility property has to be guaranteed in the medical domain. The reversible property has an interest for watermark content update.

Several reversible watermarking methods have been proposed since 1999. We have selected 13 the most representative methods [8-20] to give a classification in section 3. They introduce more or less visible distortions with varying insertion capacities. Capacity is the amount of information that can be embedded into one image and which is expressed in bit of message per pixel of image (*bpp*). In this paper, we have tested some of these methods among different medical image issued from different modalities (MRI (magnetic resonance imaging), PET (positron emission tomography) and US (ultrasound imaging) for the purpose of verifying the integrity of medical images by embedding a digital signature. Before comparing these methods with respect to the criterions given above in section 4, we present in section 2 an integrity control verification process based on

lossless watermarking and cryptographic hash. Conclusions are made in section 5.

2 Verifying Integrity of medical image with lossless watermarking

Integrity control of images can be addressed at two levels, that is: strict integrity control whereby one has to guarantee that the whole image is preserved as entire bit planes, or; content-based control in which pixels are allowed to vary while the visual content meaning remains preserved. In this work our interest is given to strict integrity which can be achieved by making use of cryptographic hash function.

Cryptographic hash functions are commonly used for digital signatures as they extract a resume or digest from the message data to be protected. Between the two function classes, the first one, called Message Code Authentication (MCA), uses a secret key and permits signature identification. The second one, known as Manipulation Detection Code (MDC), is calculated without a secret key. Since MCA function usually makes use of a MDC function concatenated with a secret key or asymmetrically encrypted, interest is given here to MDC hash function. These functions are said one way hash functions (i.e. non reversible), and from a message of arbitrary length they provide a fixed length digest or resume. For example, one of the best known methods is the SHA-256 (Secure Hash Algorithm) that yields to a signature of 256 bits [6]. Its collision probability, that is the probability to find another message with the same hash, is upper bounded by $1/2^{256}$. SHA also has good dispersion property in that a slight difference in a message will lead to a very different signature.

Such a cryptographic hash can be encrypted in asymmetric way allowing non repudiation property. The RSA (Rivest Shamir Adleman) algorithm [7] is the most widely-used asymmetric system. The system uses two different keys for encryption and decryption. One of these two keys, the public key, is meant to be known to everyone, and the other, the private key, is known to only one individual. In order to write to a recipient, all that needs to happen is to encrypt the message with the public key of the recipient. Upon reception, only the recipient will be able to decrypt the message with his private key. Data confidentiality is ensured in that case. The RSA algorithm allows also encryption with ones own private key (signature). In this case, everyone can read the message thanks to the public key. Since the sender is potentially the only person who could have encrypted it with his private key: the sender has signed the message. In DICOM (Digital Imaging and COmmunications in Medicine), the standard of reference for medical image storage and sharing (medical.nema.org), there exists a digital signature profile based on the RSA. This profile is combined with the RIPEMD-160, MD5, or SHA-1 hashing functions to generate a MAC (Message Authentication Code), which is encrypted using a private RSA key. This digital signature is actually stored in the header of a DICOM image file.

Reversibly watermarking a cryptographic hash within a medical image leads to the integrity control process illustrated in Fig. 1. A hash of the image I to be protected is calculated making use of a cryptographic hash function H ($H(I)$) and is then embedded in I leading to the watermarked image I_w. At the verification stage, the watermark reader extracts the hash $H(I)$ and removes the watermark from I_w obtaining the restored image I_r. $H(I)$ is compared to $H(I_r)$. If $H(I)$ and $H(I_r)$ are equal then I_r is said to be identical to I; if not, the system states that the image has been modified. The hash can be calculated on the image pixel gray values or on the full representation of the document. In the latter case the integrity will also depend on the image file format.

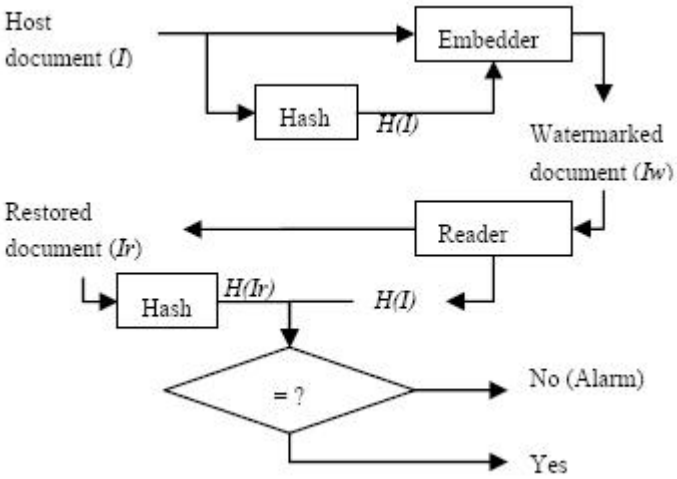

Fig. 1. Verifying image integrity thought reversible watermarking and cryptographic hash function.

With such a system, any modifications will give an alarm. However, the reversibility property allows the hash update like in the case of an authorized image modification, like a lossy image compression.

Several lossless watermarking schemes have been proposed in the literature. Each of them allows the reversible embedding of a message within an image while inducing at the same time more or less visible distortions. In the next section, we compare these different methods for different medical image modality.

3 Lossless watermarking methods

Two classes of reversible watermarking methods may be distinguished: additive methods and substitutive methods.

3.1 Additive schemes

In the case of an additive insertion, the message m to be embedded is first transformed into a watermark signal w, next added to the host signal s leading to the watermarked signal sw: $s_w = s + w$.

Additive insertion has been primarily applied in the spatial domain in which the image pixel gray level values are limited to a fixed dynamic (2^p possible gray levels for an image of p bits depth). Consequently, watermark addition may lead to over/underflows, it means that modified pixel values may fall out of the allowed gray value range [0...2^p-1]. Obviously, such a problem occurs also when embedding is conducted in a transformed domain like in the wavelet or DCT domain.

Different strategies have been proposed to overcome over/underflow problem. One approach introduced in [8] consists in using modulo arithmetic. Insertion equation $I_w = (I + w) \bmod 2^p$ can however lead to a salt and pepper noise due to jumps between congruent values of the dynamic. An improved version of this method has been proposed in [13] where visual distortions are minimized by making use of arithmetic modulo on shorter cycles, obtained by splitting the signal dynamic in ranges of small size.

Another approach makes use of a signal classification before message embedding. In [9], the proposed scheme is based on image signal estimation, an image of reference invariant to the insertion process. More clearly the image and its watermarked version will have the same image of reference. In a first time, the reference image is used to decide whether or not a pixel block can be modified. The image of reference serves a classification procedure for identifying blocks that if modified lead to an over/underflow. Then insertion is conducted on the authorized parts of image by modulating the difference between the original image and its estimated version. As the image of reference is the same for the watermarked image, the decoder can easily retrieve watermarked parts of the image.

A third approach regroups methods that modulate the image histogram in a spatial or transformed domain. The method suggested by Ni *et al.* in [10] shifts a range of the image histogram. This range is identified by the couple (zp, pp), where zp and pp correspond respectively to the gray levels with the smallest ("zero-point") and the highest ("peak-point") number of pixels. This range is shifted by adding or subtracting one gray level from the peak point toward the zero point in order to leave one gray level (a "gap") near the peak point empty. Pixels that belong to the peak point class are moved to the gap or left unchanged for message embedding. Two gray values are used to code the message. Consequently, the alteration is not more important that one gray level for the modified pixels. However, the embedded data cannot be recovered unless the position of initial peak point is known by the decoder. This modulation has been applied in the wavelet domain by Xuan *et al.* [11] where the identification of the couple (zp, pp) is simplified as integer wavelet coefficients have a "laplacian" distribution centered around '0'.

Leest *et al.* [12] have proposed a similar approach. This latter is based on creating "gaps" at the minimum and maximum luminance values in local histograms of 2×2 pixels blocks. However with this approach, positions of pixels which have the value 0 and 2^p-1 have to be embedded in the image to solve the over/underflow problem. As a consequence, embedding capacity decreases when the numbers of such a pixel increase.

3.2 Substitutive schemes

Substitutive insertion technique differs from the additive in the sense that rather than disrupting the signal by adding a watermark, it comes directly to replace the signal by another one stemmed from a predetermined dictionary signal. For example: the basic LSB scheme removes the pixels' least significant bits by bits of the message to be embedded. To make this scheme reversible, original binary values should be preserved and communicated to the decoder. Fridrich *et al.* [13] have shown that there exists a bit-plane B in the original image I, so that B can be losslessly compressed and disrupted randomly, without visible distortion in I. If such a bit-plane exists, it can be replaced by its compressed version and a binary message m. The insertion capacity of such a method is $|B|$-$|compress(B)|$ bits, where $|.|$ denotes the cardinal. Since several solutions have been proposed, some do not required embedding of data overhead. We class them into two categories: Lossless Compression Embedding (LCE) techniques and Expansion Embedding (EE) techniques.

Xuan *et al.* have proposed an insertion technique on coefficients of the integer wavelet transform [14]. They losslessly compress one or more middle bit-planes of integer wavelet coefficients to save space for data embedding. Celik *et al.* [15] proposed a generalized LSB substitutive technique, which firstly converts the binary message ($w \in \{0, 1\}$) to M-ary watermark ($w \in \{0, 1, , M-1\}$) by arithmetic coding. For example, a watermark w can be converted from $(1000101011)_2$ to $(4210)_5$, where $M = 5$. Then the lowest M-levels of the pixels of the original image are replaced by the M-ary watermarks: $p_w = M\lfloor p/M \rfloor + w$, where p and p_w represent the original pixel and its watermarked version respectively and, $\lfloor . \rfloor$ the "floor" operator meaning "the greatest integer less than or equal to". The original values are losslessly compressed using the CALIC algorithm [21].

Differently to the above-mentioned LCE techniques, Tian's algorithm [16] may be the first one to use the Expansion Embedding technique for reversible watermarking. EE shifts to the left the binary representation of an integer value h to watermark (h can be a gray value or a transformed coefficient), thus creating a new virtual LSB that can be used for insertion: $h_w = 2h + b$, where h_w is a watermarked value and b is one bit of the message. To control the insertion distortion, the EE is combined with LSB substitution: $h_w = 2\lfloor h/2 \rfloor + b$. LSB substitution is applied to h values which cannot be expanded because of the limited dynamic of the signal or because of the limited distortion to be applied. As LSB substitution is used, original LSBs have to be watermarked along with the message. To distinguish at the reader stage which h values have been expanded, a binary location map L is required. In Tian's scheme L is

losslessly compressed and added to the embedded message with the original LSBs. Alattar extended this scheme by applying the EE to a generalized integer transform [17]: several bits are embedded into vectors of adjacent pixels.

In the same way, Lee *et al.* [18] divide a pixel image into 16×16 pixel blocks, and a watermark is embedded into the high-frequency wavelet coefficients of each block by LSB-substitution or EE technique. Their location map is of small dimension $((M \times N)/(16 \times 16))$ and does not require to be compressed. Always in the same view, Xuan *et al.* in their scheme [19] introduce a threshold T. If the absolute value of an integer wavelet coefficient is lower than T, then EE is applied for data embedding. With this approach, it may be difficult for the reader to distinguish between watermarked and non-watermarked coefficients. To solve this problem, the coefficients which have the absolute values higher or equal to T should be shifted to the left or right according to their signs by $T-1$ or T. So all watermarked coefficients that carry the message are in the interval $]-2T+1, 2T[$. With this approach there is no need for a location map. This is almost the same for the method proposed by Thodi *et al.* [20], which combines Tian's method and this shifting pretreatment in order to gain better performances.

All of these methods are known to be fragile, i.e. the watermarks will not survive any image alteration. This is why these methods are at first proposed for data integrity control. For this study, we have implemented some of the most recent or original methods, and indicated by their authors as efficient on usual test images such as "Lena", "Baboon" .... Three of these schemes are additive: Ni *et al.* [10], Leest *et al.* [12], Coatrieux *et al.* [9] and two substitutive: Xuan *et al.* [19], Thodi *et al.* [20].

4 Losslessly watermarking medical images

The five algorithms were implemented with MATLAB and the message bits were generated by the function of the MATLAB rand(). Experiments were conducted on three modalities: three 12 bits encoded MRI volumes of 79, 80 and 99 axial slices of 256×256 pixels respectively, three 16 bits encoded PET volumes of 234, 213 and 212 axial slices of 144×144 pixels respectively, and, three sequences of 8 bits encoded ultrasound images (14 of 480×592 pixels, 9 and 30 of 480×472 pixels respectively). Fig. 2 gives some samples of our data set.

To objectively quantify algorithms' performances, two indicators have been considered: the capacity rate C expressed in *bpp* and, in order to quantify the distortion between an image I and its watermarked version I_w, the peak signal to noise ratio (PSNR):

$$PSNR = 10log_{10}(\frac{NM(2^p-1)^2}{\sum_{i,j=1,1}^{N,M}(I(i,j)-I_w(i,j))^2}) \quad (1)$$

where p corresponds to the image depth, N and M correspond to the image dimensions.

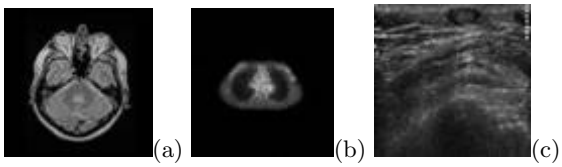

Fig. 2. Image samples extracted from our test set (a) MRI of the head-axial slice of 256×256 pixels, 12 bits encoded. (b) PET image of 144×144 pixels, 16 bits encoded, (c) ultrasound image of 480×592 pixels encoded on 8 bits.

Results are given in Tables 1 and 2. They provide the mean value and the standard deviation of the capacity and of distortion for each method and image modality. If we consider additive schemes in Table 1, [10] and [12] allow a watermark capacity close to 0.2 *bpp* with PSNR about 73-75 *dB* for MRI, 97-99 *dB* for PET. This means that nearly 13000 bits can be embedded in MRI slice and 4000 bits within PET slice. It is almost the same for ultrasound images ($>$ 10000 bits). [9] provides higher capacity for ultrasound images but may failed to watermark MRI slice as the capacity is rather small.

	MRI		PET		US	
	C(*bpp*)	PSNR(*dB*)	C(*bpp*)	PSNR(*dB*)	C(*bpp*)	PSNR(*dB*)
[10]	0.26(0.011)	73.00(0.46)	0.20(0.013)	97.98(0.92)	0.05(0.053)	52.63(4.19)
[12]	0.20(0.007)	75.72(0.067)	0.22(0.033)	99.57(0.29)	0.04(0.013)	53.19(0.52)
[9]	0.0031(0.002)	78.43(0.84)	0.020(0.016)	100.79(1.16)	0.101(0.032)	48.51(0.20)

Table 1. Capacity and distortion measurements for additive methods: Ni *et al.* [10], Leest *et al.* [12] and Coatrieux *et al.* [9]. Standard deviation is given in parenthesis.

Results of substitutive methods [19] [20] are less effective than for additive methods [10] [12] when considering MRI and PET modalities. On the contrary, for ultrasound images, these methods are more efficient than additive methods. However, for the minimal distortion (see Table 2), the smallest attended capacity is greater than 1000 bits which is enough in our framework. For ultrasound images in Table 2, [19] and [20] propose a compromise of 0.14 *bpp*/48.77 *dB* and 0.22 *bpp*/48.44 *dB* respectively. Even if some methods keep limited as they require embedding a lot of information for reconstructing the original image along with the message, it is possible to embed one digital signature. However it must be noticed that for images, [19] was not able to insert a message as the amount of information for reconstruction was more important than the offered capacity. For PET images, in Table 2, only 7% of 659 images can be watermarked with a compromise C/PSNR = 0.15 *bpp*/93.73 *dB*. Considering the integrity

	Thodi *et al.* [20]		Xuan *et al.* [19]	
	C(*bpp*)	PSNR(*dB*)	C(*bpp*)	PSNR(*dB*)
MRI	0.021(0.004)	72.40(0.17)	0.098(0.012)	68.84(0.068)
	0.199(0.015)	44.62(3.44)	0.02(30%)	65.47(30%)
PET	0.13(0.026)	97.27(0.30)	0.15(7%)	93.73(7%)
	0.212(0.03)	67.87(2.77)	0.31(2%)	90.51(2%)
US	0.22(0.090)	48.44(0.77)	0.14(0.012)	48.77(0.65)
	0.49 (0.02)	40.58(2.88)	0.55(0.02)	43.22(0.60)

Table 2. Capacity and distortion measurements for MRI image axial slices, PET axial slices and ultrasound images. Standard deviation is given in parenthesis.

control process shown in section 2 - Fig. 1, most methods allow the embedding of one hash produced by the SHA-256 hash function. With such a hash length of 256 bits, if we consider the constraint of preserving the image quality at best, [12] seems to be the most adapted. When the question is to protect the whole image volume, [9] will be more appropriate. Beyond integrity control, if the objective is the insertion of a big amount of information: [10] offers a compromise of 0.26 *bpp*/73 *dB* for MRI, [12] proposes 0.22 *bpp*/99.57 *dB* for PET and at least, for ultrasound images, [19] proposes a compromise of approximately 0.55 *bpp*/43.3 *dB*. Regardless the medical image modality, [20] proposes a satisfactory compromise of 0.021 *bpp*/72.40 *dB*, 0.13 *bpp*/97.27 *dB* and 0.22 *bpp*/48.44 *dB* for MRI, PET and ultrasound images respectively.

5 Conclusion

The main advantage of watermarking technology is to provide an autonomous and continuous protection of contents. In medical imaging, watermarking allows different applications. Also the performances of the proposed solutions vary according to the method proposed. Reversible watermarking is of main concern for medical images. However, in order to beneficiate of the watermarkings advantages, it is mandatory to propose reversible methods which minimize distortion and maximize capacity.

In this article, five reversible watermarking methods have been implemented and compared under different imaging modalities for the purpose of verifying the integrity of medical images though cryptographic hash embedding. Some limitations have been identified. They are mainly related to specific imaging modalities for which each method gives variable results in terms of capacity and distortion. From these experiments, it appears that the methods [12] are

more suitable for PET, MRI and ultrasound images since they allow signature insertion with the smallest distortion.

Based on the presented work, the optimization is to modify the studied methods taking into account the specificities of the signal to be watermarked. Beyond verifying the integrity of medical images, there is a need for inserting a significant amount of data in order to cover a wide field of applications ranging from data protection (integrity, authenticity, traceability) to the addition of metadata.

References

1. G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec: Relevance of Watermarking in Medical Imaging. in Proc. of IEEE EMBS Int. Conf ITAB, Arlington, USA, 2000, pp.250-255.
2. X. Q. Zhou, H. K. Huang, and S. L. Lou: Authenticity and integrity of digital mammography images. IEEE Trans. on Medical Imaging,vol. 20, no. 8, pp. 784791, 2001.
3. H. M. Chao, C. M. Hsu, S. G. Miaou: A Data-Hidding Technique With Authentication, Integration, and Confidentiality for Electronic Patient Records. IEEE Trans. on Information Technology in Biomedicine, Vol. 6, No. 1, pp. 46-53, 2002.
4. G. Coatrieux, L. Lecornu, B. Sankur, and Ch. Roux: A Review of Image Watermarking Applications in Healthcare, in Proc. of the IEEE EMBC Conf., New York, USA, 2006, pp. 46914694.
5. A. Piva, M. Barni, F. Bartolini, V. Capellini: Exploiting the cross-correlation of RGB channels for robust watermarking of color images. in Proc. of IEEE Int. Conf. on ICIP, vol. I, 1999, pp. 306-310.
6. Henri Gilbert, Helena Handschuh: Security Analysis of SHA-256 and Sisters. Selected Areas in Cryptography 2003: 175-193
7. R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120126. 1978.
8. C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel: Lossless recovery of an original image containing embedded data. US Patent application, Docket No.:77102/E-D, 1999.
9. G. Coatrieux, M. Lamard, W. Daccache, J. Puentes, and C. Roux: A low distortion and reversible watermark application to angiographic images of the retina. in Proc. of the IEEE EMBC Conf., Shanghai, China, 2005, pp. 22242227.
10. Z. Ni, Y. Shi, N. Ansari, and S.Wei: Reversible data hiding. in Proc. IEEE Int. Symp. Circuits and Systems, May 2003, vol. 2, pp. 912915.
11. G.R. Xuan, Q.M. Yao, C. Yang, J. Gao: Lossless Data Hiding Using Histogram Shifting Method Based on Integer Wavelets. IWDW 2006, LNCS-4283 (2006) 323-332.
12. A. Leest, M. Veen, and F. Bruekers: Reversible watermarking for images. in Proc. of Int Conf. SPIE, Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, Jan. 2004.
13. J. Fridrich, J. Goljan, and R. Du: Invertible authentication. in Proc. of Int. Conf. SPIE, Security and Watermarking of Multimedia Content, San Jose, CA, Jan. 2001, pp. 197-208.

14. G. Xuan, J. Chen, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su: Lossless data hiding based on integer wavelet transform. in Proc. MMSP, St. Thomas, Virgin Islands,2002, pp. 312315.
15. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber: Reversible data hiding. in Proc. IEEE ICIP, 2002, vol. 2, pp.157160.
16. J. Tian: Reversible data embedding using a difference expansion. IEEE Trans. on Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890896, Aug. 2003.
17. A. M. Alattar: Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. on Image Processing, vol. 13, no. 8, pp. 11471156, Aug. 2004.
18. S. Lee, C. D. Yoo, T. Kalker: Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform Information Forensics and Security. IEEE Trans. Info. Forensics and security, vol. 2, no. 3, pp. 321 330, Sept. 2007.
19. G.R. Xuan, Y.Q. Shi, C.Y. Yang, Y.Z. Zheng, D.K. Zou, P.Q. Chai: Lossless Data Hiding Using Integer Wavelet Transform and Threshold Embedding Technique.in proc. of Int. Conf. Multimedia and Expo, 2005, pp. 1520 1523.
20. D. M. Thodi and J. J. Rodriquez: Expansion Embedding Techniques for Reversible Watermarking. in IEEE Trans. Image Processing, vol.16, no.3, pp. 721-730, March 2007.
21. X. Wu: Lossless compression of continuous-tone images via context selection, quantization, and modeling. IEEE Trans. on Image Proc., vol. 6, no. 5, pp. 656664, May 1997.