Lossless Watermarking for Verifying the Integrity of Medical Images with Tamper Localization

Xiaotao Guo and Tian-ge Zhuang

Given the ease of alteration of digital data, integrity verification and tamper detection for medical images are becoming ever more important. In this paper, instead of using the conventional irreversible block-based watermarking approach to achieve tamper localization, we propose to incorporate such functionality into the region-based lossless watermarking scheme. This is achieved by partitioning an image into certain non-overlapping regions and appending the associated local authentication information directly into the watermark payload. A region of authentication, which can be flexibly specified by the user, is partitioned into small regions in a multilevel hierarchical manner. Such hierarchical structure allows the user to easily adjust the localization accuracy, and makes the tamper detection efficient. Experimental results demonstrate the effectiveness of tamper localization.

KEY WORDS: Watermarking, security, integrity, image authentication, tamper localization, telemedicine, PACS, ROI

INTRODUCTION

In a modern integrated health care environment, digital information systems such as hospital information systems (HIS), picture archiving and communication systems (PACS), and electronic patient record (EPR) systems, are playing an ever more important role. As is well known, the digital representation of medical data has lots of advantages over its analogy counterpart in data compression, storage, and transmission. On the other hand, with current techniques, it is fairly easy for malicious adversary to intercept or tamper sensitive medical data when the public network (e.g., the Internet) is being used for telemedicine. The patient and the imaging data, transmitted between imaging centers and other interested individuals using compact disc digital media, are also ex-

tremely vulnerable to alteration.¹ Authenticating the integrity of medical images becomes a critical issue. Meanwhile, mandates for ensuring health data security have been issued by the federal government such as Health Insurance Portability and Accountability Act (HIPAA).² Guidelines, such as digital imaging and communication in medicine (DICOM) standards that deal with security issues, continue to be published by organizing bodies in health care. This paper focuses on verifying the integrity of medical images with tamper localization functionality.

Traditionally, source authentication and integrity verification of digital data have been performed by digital signature or message authentication code (MAC). Image authentication in the traditional manner often requires the storage and transmission of the associated authentication information in the image header, such as DICOM header. However, such information is susceptible to loss during format conversions, e.g., converting a DICOM image to Joint Photographic Experts Group (JPEG) format etc. It is therefore desirable to include the authentication information within the image data itself. This goal can be achieved using digital watermarking techniques, which embed additional

From the Department of Biomedical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China.

Correspondence to: Xiaotao Guo, Department of Biomedical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China; tel: +86-21-52540226; fax: +86-21-52540226; e-mail: gxt@sjtu.org

Copyright © 2008 by Society for Imaging Informatics in Medicine

Online publication 13 May 2008

doi: 10.1007/s10278-008-9120-5

information imperceptibly within the host image. In addition to format independence, digital watermarks have the advantage of tamper localization, which refers to the ability to pinpoint the image region that has been tampered.

The earlier watermarking methods used for integrity verification were inserting the authentication information into the least significant bit (LSB) plane. For instance, Zhou et al. presented a watermarking method for verifying authenticity and integrity of digital mammography images.³ With this method, to embed the digital envelope into the image, the LSB of one random pixel of the mammogram was replaced by one bit of the digital envelope bit stream. The digital signature was computed for the entire mammogram image and was unable to provide tamper localization functionality. To enable such functionality, Wong et al. presented a typical block-based authentication watermarking scheme,⁴ where an image was divided into certain non-overlapping blocks. Integrity verification was performed on per block basis. Celic et al. introduced a hierarchical structure based on Wong's algorithm,⁵ where the image was divided into blocks in a multilevel hierarchy manner. Note that in the above-mentioned watermarking approaches, instead of the whole image data, only partial image data (not including LSB plane) was used for calculating the image block signature. A modification of image data in the LSB plane can not be detected. The drawback of the above bit-replacement data embedding approaches is that the original image is distorted in a non-invertible manner. It is impossible for a watermark decoder to recover the original image. Thus, they are referred to as *irreversible* watermarking.

The irreversible distortion is generally not acceptable for medical images, even if it is imperceptible. Medical tradition has been very strict with the quality of biomedical images. Alteration of the bit field representing the image is, generally, not allowed.⁶ Lossless (also referred to as *reversible*) watermarking, which can recover the exact original image, has drawn lots of interest recently.⁷⁻¹³ Goljan et al. introduced distortion-free data embedding for images.⁷ De Vleeschouwer et al. used a circular interpretation of bijective transformations of the histogram to embed data.⁸ Tian proposed a high-capacity reversible data embedding method using difference expansion of pairs of pixel values.⁹ Alattar generalized Tian's method to arbitrary vectors

instead of pairs.¹⁰ Celic et al. presented a reversible data embedding algorithm by compressing quantization residues.¹¹ Zhou et al. presented two lossless data embedding methods to embed digital signature into medical images.¹² The first one was based on compressing the LSBs of randomly selected image pixels; the second one was based on the regular/singular (RS) embedding approach. Thodi et al. proposed a prediction-error expansion-based reversible data embedding technique.¹³

The aforementioned lossless watermarking approaches solve the problems existed in the irreversible block-based authentication watermarking. However, almost all of them lost the tamper localization capability. We will discuss the underlying factors later. To remedy this deficiency, Celic et al. proposed a new framework by combining one irreversible block-based authentication watermarking system with another reversible watermarking system.¹⁴ The original information, which was lost due to the first irreversible watermarking system, was collected and embedded into the rest of the image using the second reversible watermarking system, thus offering tamper localization and reversibility simultaneously. The overall embedding distortion level, which comes from both watermarking systems, however, was often very high. Applying this framework to medical images brings great inconvenience in practical medical applications. Since the authentication information was distributed in each partitioned block, it was not easy to restrict the embedding-induced distortion outside the region of interest (ROI). The watermark decoder had to restore the original image all the time, to ensure that the diagnostic accuracy inside the ROI was not jeopardized by such distortion. This significantly restricted its wide usage in medical applications.

This paper exploits the features provided by the region-based lossless watermarking scheme¹⁵ to enable tamper localization functionality in a natural way. Instead of using another conventional irreversible block-based authentication watermarking approach to achieve tamper localization, we propose to incorporate such functionality into the lossless watermarking scheme itself. This is achieved by partitioning an image into certain non-overlapping regions and appending the associated local authentication information *directly* into the watermark payload. While enabling reversibility and tamper localization, the watermarked image can be used for diagnostic purpose as well as many

other medical applications, since the embedding-induced distortion can be restricted outside the ROI. Experimental results demonstrate the effectiveness of tamper localization.

MATERIALS AND METHODS

The main idea of the proposed scheme is to embed the local authentication information (used for tamper localization) directly into the watermark payload, using only one lossless watermarking system. The required lossless watermarking system need to have two properties: high embedding capacity and retrievability. The embedding capacity, which refers to the maximal amount of information that can be embedded in the image, determines the localization accuracy. A lossless watermarking with low capacity cannot provide enough localization accuracy. The property of retrievability refers to the ability to successfully retrieve the embedded local authentication information from the tampered image. We assume that the modification is mild, restricted in some small areas. This assumption is reasonable for most of the medical applications.

The region-based lossless watermarking scheme proposed by Guo et al.¹⁵ bears the aforementioned properties. One feature is that it achieves high embedding capacity with a low level of embedding-induced distortion. Another attractive feature is that it has the capability of not introducing any embedding-induced distortion in the ROI of the medical images. Thus, the watermarked image can be used for diagnostic purpose as well as many other medical applications, provided the embedding region does not intersect with the ROI. The add-on value is that the watermark information can always be successfully extracted, as long as the modification of image data is outside the embedding region. Since the embedding region is relatively small and could be restricted outside the ROI, the probability of failing to extract the watermark information is relatively low. This lossless watermarking scheme is a good candidate for embedding the local authentication information directly into the watermark payload to enable tamper localization.

Hierarchical Partition of Image Data

This section introduces the hierarchical structure for partitioning the image data in a region. It

will be used for computing local authentication information.

Suppose the image data we want to authenticate is X . It can be defined as the entire image, an image block, or a specified region of the image. In a hierarchical partition of image data, X is partitioned into certain non-overlapping blocks or regions successively in a hierarchical manner as depicted in Figure 1.

In Figure 1(a), an image block X is partitioned into 2×2 non-overlapping blocks successively. Let us denote a block in this hierarchy by X_{ij}^l , where the indices ij represent the spatial position of the block and l the level of the hierarchy to which the block belongs. The total number of levels in the hierarchy is denoted by L . Top level of the hierarchy consists of only one block $X_{00}^1 = X$. Bottom level L of the hierarchy consists of $2^{L-1} \times 2^{L-1}$ blocks. A block X_{ij}^l at level l is composed of 2×2 blocks at level $l+1$, that is:

for $l = L - 1$ to 1

$$\begin{bmatrix} X_{2i,2j}^{l+1} & X_{2i,2j+1}^{l+1} \\ X_{2i+1,2j}^{l+1} & X_{2i+1,2j+1}^{l+1} \end{bmatrix} = X_{ij}^l.$$

Fig 1. Hierarchical partition of image data in a region. (a) A rectangular region. (b) A polygonal region.

For a given block, a set of subblocks at the lower level is located inside this block. All of the subblocks are referred to as the *descendants* of the given block.

In Figure 1(b), a polygonal region R is firstly partitioned into some non-overlapping triangular regions. Then each triangular region is decomposed further into three triangular regions successively. Let us denote a region in the hierarchy by X_i^l , where the index i represents the scan order of the region, e.g., the raster scan order. This hierarchy can be expressed as:

$$\text{for } l = L - 1 \text{ to } 2 \\ [X_{3i}^{l+1} \quad X_{3i+1}^{l+1} \quad X_{3i+2}^{l+1}] = X_i^l.$$

Top level of the hierarchy consists of only one region $X_0^1 = R$. For a pentagonal region, level 2 of the hierarchy consists of three triangular regions $\{X_0^2, X_1^2, X_2^2\}$. In general, a polygonal region with n vertexes can be decomposed into $n-2$ triangular regions. It is worthy to mention that there exist a variety of ways to partition a polygonal region. For example, a polygonal region with n vertexes can be decomposed into n triangular regions, with its center as a common vertex.

Region of Authentication

A region of authentication (ROA) is a region used for integrity authentication. It can be defined as the entire image or a portion of the image. It can be specified by the user as an image block or a polygonal region. To let the decoder reconstruct the ROA for tamper localization, the ROA description information R_A must be transmitted to the decoder as a part of the watermark payload. To efficiently represent the ROA, a data structure with variable length, which forms the bit stream of R_A , is introduced in this study. One bit is used for specifying whether the ROA is the entire image or a portion of the image. If the ROA is a portion of the image, one bit is used for specifying whether the ROA is a rectangular region, or a polygonal region. Then the vertex number n_v of the rectangle or the polygon, and all the vertex coordinates (x_i, y_i) , $i \in \{1, 2, \dots, n_v\}$, are appended into the bit stream R_A . For an image with size of 1024×1024 , 20 bits are needed to represent each vertex coordinates. After extraction of the ROA description informa-

tion R_A , the ROA can be completely reconstructed in the image.

For simplicity, an image block is used in the following to describe the working procedure. For a polygonal region, the procedure is the same except for the difference in hierarchy formation.

The basic procedure follows the data embedding procedure, as well as the data extracting and verifying procedure in the region-based lossless watermarking scheme.¹⁵ The main modification includes: 1) in the data embedding procedure, add a local authentication information embedding procedure; 2) in the data extracting and verifying procedure, add a tamper detection procedure.

Local Authentication Information Embedding Procedure

The local authentication information embedding procedure consists of three main steps: i) formation of the block hierarchy, ii) computation of the block signature, and iii) authentication information insertion.

The formation of block hierarchy is described as in Figure 1(a). Upon the formation of a proper hierarchy, for each block X_{ij}^l , compute the associated block signatures S_{ij}^l . This step consists of the calculation of the hash value H_{ij}^l of the block X_{ij}^l , and the associated block signature S_{ij}^l :

$$\text{for } l = 1 \text{ to } L$$

$$H_{ij}^l = H(X_{ij}^l) \quad (1)$$

$$S_{ij}^l = S(H_{ij}^l, K), \quad (2)$$

where $H(\bullet)$ denotes a hashing function, $S(\bullet)$ denotes a signature function, and K denotes the authentication key. Note that if the entire image is defined as the ROA, then there is no need to compute the signature of the top level block, since the digital signature DS for the entire image is already included in the watermark payload P .

Let us denote S as the local authentication information bit stream. It consists of the ROA description information R_A and all the block signatures. The embedded ROA description information will be used for reconstructing the ROA in the verifying procedure. Starting from the highest level in a predefined order, e.g., raster scan order,

the block signature S_{ij}^l is appended into S sequentially, that is:

$$S = R_A \oplus S_{00}^1 \oplus S_{00}^2 \oplus S_{01}^2 \oplus S_{10}^2 \oplus S_{11}^2 \cdots \oplus S_{ij}^l, \quad (3)$$

where $\oplus$ denotes a concatenating operator.

The watermark payload P , which consists of the additional data D , the image digital signature DS , and the local authentication information S , is subject to the constraint:

$$P = D \oplus DS \oplus S \leq C \quad (4)$$

where C denotes the embedding capacity. The partition of an image stops when the condition (Eq. 4) does not hold. The final hierarchy level is L .

For a given embedding capacity C and a given additional data D , the maximal bit length of S is determined by the condition (Eq. 4). The maximal hierarchy level could be deduced based on the number of block signatures included in S . For later convenience, the value of L is included in the watermark payload to let watermark decoder know the actual hierarchy level being used.

Tamper Detection Procedure

The tamper detection procedure consists of three basic steps analogous to the local authentication information embedding procedure: (i) extraction of the block signature, (ii) formation of the block hierarchy, and (iii) verification of the block signature.

The watermark payload P' is extracted using the data extracting and verifying procedure in the region-based lossless watermarking scheme.¹⁵ From the watermark payload, extract the image digital signature DS' and the local authentication information S' . Decrypt DS' to obtain the hash value H' using the corresponding public key. Compute the hash value for the whole image data of the recovered image I' . Compare it with the hash value H' . If they do match exactly, the integrity of the image is assured, no further verification is needed. Otherwise, tamper detection procedure is started.

First, extract the ROA description information R'_A from the bit stream S' . Based on R'_A , whether the ROA is the entire image or a portion of the image can be determined. If the ROA is a portion of the image, then extract the vertex coordinates from R'_A to reconstruct the ROA in the recovered image.

Assuming the reconstructed ROA is a rectangular region, a block hierarchy is formed accordingly as in the data embedding procedure. Upon formation of a proper hierarchy, for each block, starting from the highest level, compute the associated block signature. Compare it with the corresponding extracted signature from S' . If both signatures do match exactly, the block is deemed authentic. Thus, its descendants need not be verified further. Otherwise, if the signatures do not match with each other, the block is deemed not authentic. Then partition this tampered block into the next level and verify its integrity in the same way. The verification process stops when the last extracted block signature is verified. Since an authentic block does not need to be processed further, and often only a small number of tampered blocks need to be partitioned into the last level, the tamper detection procedure is efficient.

RESULTS

For comparison, the same medical image as in our previous work¹⁵ is used to demonstrate the functionality of tamper localization. In particular, the original image is a typical 640×480 , 8-bpp ultrasound image. In our experiments, the total hierarchy level L is set at 4. A 128-bit MD5 hashing algorithm and a 64-bit HMAC algorithm are used as the hashing function and the signature function in Eqs. 1 and 2, respectively.^{16,17}

Figure 2 shows the original medical image. Figure 3 shows the watermarked image. Three polygons with the sides in white in the watermarked image indicate the embedding regions. The watermark information is embedded inside these polygonal regions. Thus, the embedding-induced distortion is also restricted inside these regions. The embedding capacity is 11,183 bits. Figure 4 shows the tampered image. The tampered image is obtained from the watermarked image by some manipulation. We intentionally changed the pixel values near the center of the ROI at two black spots (for illustrative purpose). We also modified the pixel values at the upper right corner such that the original date "2000/09/29" becomes "2000/09/20." Comparing Figure 4 with Figure 3, obvious a total of three different places have been tampered.

Figure 5 shows the tamper detection output with the entire image being considered as the ROA. In

Fig 2. Original 640×480, 8-bpp ultrasound image.

such scenario, the watermark decoder can successfully extract the embedded information, including the hash value for the original host image, “6cac2ace305cea4937a4922647137091”, the additional patient information, and the attached local authentication information. After restoration, the recomputed hash value for the recovered image becomes “8fe45d3f834478da838abd413c431e63”, indicating that the watermarked image has been tampered with. Tamper detection procedure then follows. The shading is used to reflect the level of confidence in the integrity of a particular block or a region, where light shading corresponds to high confidence value and dark shading corresponds to low confidence value. In Figure 5, three tampered places are successfully located, as indicated by the three darkest blocks. The smallest block dimension has a dimension of 80×60, indicating the localization accuracy.

Fig 3. Watermarked image (three polygons with the sides in white indicate the embedding regions).

Fig 4. Tampered image: some pixels are modified at two black spots near the center; the date “2000/09/29” at the right-upper corner is modified to “2000/09/20.”

Figures 6 and 7 both show the tamper detection outputs when a portion of the image is chosen as the ROA. The watermarked images are modified in the same way as in Figure 4, i.e., three different places have been tampered with. In Figure 6, the rectangular image block is specified as the ROA. The modified black spots are successfully located, as indicated by the two darkest blocks. The smallest block’s dimension now becomes 32×40. In Figure 7, the pentagonal region is specified as the ROA. One black spot is also successfully located, as indicated by the darkest triangle. These two results also demonstrate that the user has the freedom to choose the shape of the authentication region. A rectangular ROA is not the only choice. In some scenarios, a polygonal ROA may be a better choice, especially when an interactive operation is involved.

Fig 5. Tamper detection output. The entire image is considered as the ROA.

Fig 6. Tamper detection output. The rectangular image block is specified as the ROA.

We also examined the tamper localization for other typical medical images. In general, for medical images of small size, it is relatively easy to achieve good localization accuracy. For some computed radiography (CR) images, the image size is relatively large. For example, a typical chest CR image can have a dimension of 3480×4240 . Nevertheless, it also has very large embedding capacity. If the total hierarchy level L is set appropriately, sufficient localization accuracy can still be achieved.

DISCUSSION

The high-capacity property provided by the region-based lossless watermarking scheme is exploited to achieve sufficient localization accuracy.

Fig 7. Tamper detection output. The pentagonal region is specified as the ROA.

cy. To further improve localization accuracy, a particular region can be specified for integrity authentication. If the size of the authentication region is much smaller than that of the original image, with the same amount of authentication information, the localization accuracy can be improved considerably. This can be demonstrated by comparing the final tamper location accuracy in Figures 5 and 6. In our scheme, the user can choose a rectangular region or a polygonal region as the ROA at will. The conventional irreversible block-based authentication watermarking, however, is restricted to rectangular regions only.

An attractive feature of the region-based lossless watermarking scheme is that the embedding-induced distortion can be easily restricted outside the ROI. The watermarked image can be used for diagnostic purpose and other medical applications, provided the embedding region does not intersect with the ROI. On the contrary, as mentioned in the “Introduction,” the framework proposed by Celic et al.¹⁴ does not bear this feature. The embedding-induced distortion comes from two sources: one is from the irreversible authentication watermarking system; the other is from the lossless watermarking system. Therefore, the watermark extraction and the original image restoration procedure must be performed, to ensure the diagnostic accuracy in the ROI is not compromised by the embedding-induced distortion.

The accuracy of the tamper localization is determined by the size of the smallest cell block in the hierarchy. For a given authentication region, the higher the hierarchy level, the smaller the cell block can be divided. However, more hierarchy levels imply more local authentication information needs to be embedded. The amount of authentication information used for the tamper detection is subject to the constraint of condition (4). Therefore, those lossless watermarking approaches with low capacity^{7,8,12} are unable to provide sufficient localization accuracy. The property of retrievability is the key to the success of tamper localization. Unfortunately, most of the high-capacity lossless watermarking approaches are vulnerable to the slightest alteration of image data. In the algorithm of Tian and Alattar,^{9,10} the location map is compressed using the JBIG2 method; modification of image data may lead to decoding error or syntax error in the JBIG2 stream. In the algorithm of Celic et al.,¹¹ the quantization residues are compressed

using the lossless image compression algorithm CALIC, with quantized values as side information. An alteration of image data may also lead to syntax error of CALIC. In the prediction-error based algorithm of Thodi et al.,¹³ a slight modification of image data may lead to drastic change of the context used for prediction, which leads to failure of watermark extraction and restoration. The discussion above indicates that many current lossless watermarking methods⁷⁻¹³ are not good candidates for embedding local authentication information directly into the watermark payload.

Chiang et al.¹⁸ recently proposed a tampering detection and restoring system by using reversible data embedding scheme. In their scheme, the original image was divided into several non-overlapping blocks. The average pixel value of each block was calculated as the recovery feature. These features were embedded in the image for tamper detection. However, a malicious adversary could easily modify the pixel values in a block without changing its average value. Therefore, it could not be regarded as the strict integrity verification. On the contrary, our method is based on the hashing function, where any modification in the input image data (including LSB plane) can be detected sensitively.

There also exist some limitations in our method. If the tampering occurs in the embedding region, it is possible that the watermark decoder could not retrieve the authentication information successfully. As a consequence, the tamper may not be located. Nevertheless, since the embedding region is restricted in the small regions outside the ROI, the probability of failing to extract the watermark information is relatively small, compared with other lossless watermarking schemes. For some important scenarios such as when the embedding region is outside the ROI and the tampering area is restricted inside the ROI, our method can always successfully locate the alteration. We are interested in limited tampering in this study, which is reasonable for many practical medical applications. If the entire image is significantly tampered, there is no need for tamper localization.

CONCLUSION

This paper has addressed the security issue for medical images. The region-based lossless water-

marking scheme is enhanced to achieve integrity verification with tamper localization capability. We proposed to embed local authentication information into the watermark payload directly, which makes the algorithm simple and sensitive enough to intentional tampering. We introduced a hierarchical structure for partitioning an authentication region, which makes it easy for adjusting the localization accuracy and efficient for tamper detection. The authentication region offers flexibility of user specification to obtain sufficient tamper localization accuracy. Experimental results indicate the effectiveness of tamper localization. Finally, provided the embedding region is restricted outside the ROI, the watermarked image can be safely used for a variety of medical applications without compromising any diagnostic accuracy.

REFERENCES

1. McEvoy FJ, Svalastoga E: Security of patient and study data associated with DICOM images when transferred using compact disc media. *J Digit Imaging* 2007 Aug 21. DOI [10.1007/s10278-007-9068-x](https://doi.org/10.1007/s10278-007-9068-x)
2. Cao F, Huang HK, Zhou XQ: Medical image security in a HIPAA mandated PACS environment. *Comput Med Imaging Graph* 27:185-196, 2003
3. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. *IEEE Trans Med Imag* 20:784-791, 2001
4. Wong PW, Memon N: Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Trans Image Process* 10:1593-1601, 2001
5. Celik MU, Sharma G, Saber E, Tekalp AM: Hierarchical watermarking for secure image authentication with localization. *IEEE Trans Image Process* 11:585-595, 2002
6. Coatrieux G, Maitre H, et al: Relevance of watermarking in medical imaging. *Proc IEEE EMBS Information Technology Applications in Biomedicine*:250-255, 2000
7. Goljan M, Fridrich J, Du R: Distortion-free data embedding for images. *Proceedings of the 4th Information Hiding Workshop*, vol. 2137:27-41, 2001
8. De Vleeschouwer C, Delaigle JF, Macq B: Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Trans Multimedia* 5:97-105, 2003
9. Tian J: Reversible data embedding using a difference expansion. *IEEE Trans Circuits Syst Video Technol* 13:890-896, 2003
10. Alattar AM: Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Trans Image Process* 13:1147-1156, 2004
11. Celik MU, Sharma G, Tekalp AM, Saber E: Lossless generalized-LSB data embedding. *IEEE Trans Image Process* 14:253-266, 2005

12. Zhou Z, Huang HK, Liu BJ: Digital signature embedding (DSE) for medical image integrity in a data grid off-site backup archive. *Proc SPIE* 5748:306–317, 2005
13. Thodi DM, Rodríguez JJ: Expansion embedding techniques for reversible watermarking. *IEEE Trans Image Process* 16:721–30, 2007
14. Celik MU, Sharma G, Tekalp AM: Lossless watermarking for image authentication: a new framework and an implementation. *IEEE Trans Image Process* 15:1042–1049, 2006
15. Guo X, Zhuang TG: A Region-Based lossless watermarking scheme for enhancing security of medical data. *J Digit Imaging* 2007 Jul 10. DOI [10.1007/s10278-007-9043-6](https://doi.org/10.1007/s10278-007-9043-6)
16. Rivest RL: The MD5 Message-Digest Algorithm. RFC 1321, 1992
17. Krawczyk H, Bellare M, Canetti R: HMAC: Keyed Hashing for Message Authentication. RFC 2104, 1997
18. Chiang KH, Chang KC, Chang RF, Yen HY: Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *J Digit Imaging* 2007 Mar 1. DOI [10.1007/s10278-007-9012-0](https://doi.org/10.1007/s10278-007-9012-0)