Medical Image Authentication Using DPT Watermarking: A Preliminary Attempt

M.L. Dennis Wong, Antionette W.-T. Goh, and Hong Siang Chua

Information and Security Research Laboratory,
Swinburne University of Technology, Sarawak Campus, Malaysia
{dwong,agoh,hschua}@swinburne.edu.my
http://www.swinburne.edu.my

Abstract. Secure authentication of digital medical image content provides great value to the e-Health community and medical insurance industries. Fragile Watermarking has been proposed to provide the mechanism to authenticate digital medical image securely. Transform Domain based Watermarking are typically slower than spatial domain watermarking owing to the overhead in calculation of coefficients. In this paper, we propose a new Discrete Pascal Transform based watermarking technique. Preliminary experiment result shows authentication capability. Possible improvements on the proposed scheme are also presented before conclusions.

Keywords: Biomedical Image, Discrete Pascal Transform, Fragile Watermarking, Content Authentication.

1 Introduction

The progression of information technology in the past decade has resulted in proliferation in the field of health care information management. One fine example of this successful coupling of information technology and biomedicine is the move to store biomedical images in digital form. This move is well received by medical informatics practitioners as digital media can be easily archived, searched for and retrieved compared to its analog counterparts.

Despite the aforementioned feature of merits, there are arising concerns with regards to the security management of medical data which remain a critical bane to the practical implementation and deployment of Medical Information Systems (MIS). Among others, the major risk comes with the agility of medical media itself, as it is increasingly easier to manipulate digital images to one's content with digital image editing software readily installed in personal computers. Hence, any IT literate person with basic image editing knowledge could alter a biomedical image that leads to a different prognosis. With some level of persistence, the alteration may well be perceptually difficult to detect. In the scenario of medical insurance fraud, clusters of microcalcifications could be intentionally added to a healthy mammogram to indicate possible occurrence of breast cancer. Inversely, these regions could be removed intentionally from the mammogram,

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-02312-5_25

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 42–53, 2009.

resulting in an erroneous diagnosis that could lead to successful insurance policy approval or conversely claims.

Due to the strict nature of biomedical images, the research community readily adopted digital watermarking methods [1] as a viable solution to offer direly needed security to the digital biomedical images. Most watermarking schemes proposed for general image authentication are of the fragile type [2]. Fragile watermarking algorithms are usually strict tamper detection tools. They are built on the basis of inserting a watermark in such a way that any attempt to alter the host image will also result in destroying the watermark itself. As such, any manipulation of the image immediately causes the content itself to lose integrity. Another advantage of using fragile watermarking schemes is that one can locate the regions of distortions on the image that have been tampered with. Consequently, a medical expert can ascertain the level of trustworthiness of the image received to ensure accurate diagnosis.

Examples of biomedical image content authentication schemes work based on fragile watermarks can be found in [3,4] and [5].

In this paper, we report our preliminary attempt in designing a novel Transform Domain fragile watermarking method for biomedical image authentication, namely the Discrete Pascal Transform (DPT). Aburdene and Goodman first proposed the version of DPT studied herein based on a variation of the Pascal matrix [6]. To the best of our knowledge, this is the first biomedical image watermarking using DPT. The main motivation of choosing DPT as the transform domain is mainly owing two unique features of DPT. First, as it will be discussed later, the inverse transform of the DPT is equal to the forward transform itself. This specific property will eventually lead to a smaller footprint during VLSI implementation. Second, various multiplier-less implementation of DPT has been deviced [7,8]. This will lead to great speed in VLSI implementation.

Besides, DPT, when realized as a difference equation, leads to high pass filtering. Hence altering the DPT coefficients is the same as altering the high frequency components. The latter is a common idea available in other transform domain such as Discrete Cosine Transform and Discrete Wavelet Transform.

The outline of the paper is as follows. Section 2 discusses the role of watermarking with respect to the security of digital biomedical images. Section 3 describes the technicalities of the DPT in detail. An approach based on the DPT is demonstrated in Section 4 for digital biomedical image content authentication. Empirical results are presented in Section 5 with benchmarking results against potential attacks. Finally, some outstanding issues and future works are given before conclusions is drawn.

2 Biomedical Image Watermarking

2.1 Security of Medical Data

Coatrieux et al. [1] states the three mandatory components of security of medical data, namely, confidentiality, reliability and availability. They can be further explained as follows:

- **Confidentiality:** Only the entitled users have access to the medical information;
- **Availability:** This refers to the ability of a medical information system to be used by the entitled users in the stipulated conditions of access; and
- **Reliability:** This is tied to the aspects of integrity and authentication, where the integrity part checks that the information has not been altered by unauthorized persons and the authentication part checks that the information belongs to the entitled user and is issued from the right source.

2.2 Providing Security through Watermarking

In 1993, the Digital Imaging and Communications in Medicine (DICOM) standard [9] was developed to provide interoperability between all current and future medical systems from different manufacturers. This standard is now adopted by the medical community for the purpose of storing, transmitting and viewing medical images. It is also required by all Electronic Health Record (EHR) systems that include imaging information as an integral part of the patient record [9]. DICOM dependent medical specialties include radiology, cardiology, dentistry, surgery, neurology, breast imaging, and radiotherapy.

Conventionally, each DICOM medical image is associated with a patient's private data such as patient's name, age, results of examination/diagnosis, time taken, etc. All these private information are recorded into a meta data or header file, which is appended to the image. The DICOM standard stores the image data and the meta data separately. Clearly, this is dangerous as the link between the image and the textual information is practically non-existent. Using watermarking, it is possible to embed the meta data into the image data. This way, we introduce a situation where both pieces of information will depend on each other to provide the full information in a more secure manner. Not only does watermarking reduce the happenings of a mismatch between the image data and the patient's meta data, but it also prevents the loss of the header file when the image undergoes some intentional processing.

Watermarking has a very important role in medical image security in terms of confidentiality, integrity and authentication [1]. The three main objectives of applying watermarking in the medical domain according to [1] are:

- **data hiding** for the purpose of inserting meta data and other information so that the image is more useful or easier to use;
- **integrity control** which checks that the image has not been modified in an unauthorized manner; and
- **authenticity** which traces the origin of an image.

2.3 Watermarking Requirements for Biomedical Image Authentication

The criteria for generic watermarking authentication [10] can be applied to the medical domain. However, rigorous bindings in the medical domain due to strict

ethics and legislative rules [1] require other authentication features to substitute those in generic data authentication which are insufficient and sometimes too rigid for use in biomedical image authentication.

Based on literature review, requirements specific to watermarking-based biomedical image authentication include:

Imperceptibility/Reversible Watermarking. It is desirable that any watermarking should not affect the quality of the biomedical image. No distortion introduced by watermarking or degradation of image quality should be tolerated as this could result in a fallacious diagnosis. Thus, the watermarking should be reversible, in the sense that the original pixel values must be recovered exactly [11], and therefore recovering the original image (without the embedded watermark).

Integrity Control. Biomedical images usually undergo some preprocessing such as enhancement and contrast stretching [1] while being interpreted by a radiologist. As such, it is important to define whether the originally obtained image or the image processed by the radiologist should be used as a reference for integrity control.

Besides unintentional modification such as the image processing activities mentioned above, we must also address the malicious act of intentionally tampering images for illegal purposes. As such, we can easily see two levels of integrity control [3], that is:

- **strict** integrity control, where the modification of even one bit is not allowed; and
- **content-based** integrity control, where pixels are allowed to differ to the extent that the semantics of the image remain preserved.

Authentication. Transmission of biomedical images over the Internet for the purpose of telediagnosis and widespread exchange of medical data by the medical community has made authentication of biomedical images an essential issue. Coatrieux et al. [1] states that a critical requirement is to authenticate different parts of an Electronic Patient Record (EPR), in particular, the images.

3 Discrete Pascal Transform

The Discrete Pascal Transform (DPT) was introduced by Aburdene and Goodman [6]. It is a member of the discrete polynomial transform family and is based on a variation of the Pascal matrix.

The DPT coefficients, as with the case of other linear transformations, can be calculated using a transformation matrix, P. In the case of DPT, P takes the form of a lower-triangular matrix whose elements, P_{ij}, are equal to:

$$P_{ij} = \begin{cases} (-1)^j \binom{i}{j} & i \leq j \\ 0 & \text{otherwise} \end{cases}$$

where $\binom{i}{j} = \dfrac{i!}{j!(i-j)!}$ with i, j as non-negative integers.

The discrete Pascal transform of a one-dimensional vector, x, can then be defined as:

$$X = Px \tag{1}$$

where x, X are N x 1 vectors and P is the N x N Pascal transform matrix. An example of the the Pascal matrix of dimension $N = 4$ is given below:

$$P_{4\times4} = \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ 1 & -1 & \cdot & \cdot \\ 1 & -2 & 1 & \cdot \\ 1 & -3 & 3 & -1 \end{bmatrix}$$

where zero entries are replaced with $\cdot$ for clarity.

As such, we can see that the matrix P can be obtained from left compacting the row elements of a Pascal's triangle into a zero matrix and then alternating the signs of the columns.

The basic properties of the P matrices are:

- All elements in the first column are equal to 1,
- All matrices are lower triangular,
- The sum of the elements in each row (except of the first one) are equal to 0, and
- All matrices are equal to their inverse.

As the elements of the Pascal transform matrix that are above the diagonal are equal to zero, we can derive the forward DPT as:

$$X_k = \sum_{n=0}^{k} (-1)^n \binom{k}{n} x_n \tag{2}$$

where x_n is the data sequence, X_k are the transform coefficients and $k = 0, 1, ..., N-1$.

With the inverse of the Pascal matrix equal to the Pascal matrix itself, we can calculate the inverse DPT using the same equation as the forward transformation:

$$x = P^{-1}X = PX \tag{3}$$

In summation, it can be expressed as:

$$x_n = \sum_{n=0}^{k} (-1)^k \binom{n}{k} X_k \tag{4}$$

The matrix P can also be applied to a two-dimensional image, $\mathfrak{X}$, where the DPT coefficients can be obtained through:

$$X = P\mathfrak{X}P^T \tag{5}$$

where P^T is the transpose of matrix P
or equivalently:

$$X = (P(P\mathfrak{X})^T)^T \tag{6}$$

4 Proposed Method

4.1 Description of the Method

The proposed approach takes on the method of watermarking in a transform domain, namely the Discrete Pascal Transform (DPT) [6]. Recent research is mostly based on the frequency or transform domains as they offer better performance in terms of fidelity and detectability. The introduction of the DPT has brought about intensive study in applications such as signal processing and image processing, as well as communications and control systems [6].

In this work, we integrate a fragile watermarking approach that embeds the authentication information - in our case, we use a randomly generated secret - into the biomedical image itself. The authentication watermark is embedded in the transform coefficients of the entire image, thereby allowing strict integrity control on the overall image. In this way, regardless whether the region is of interest or non-interest, the quality of the image after watermarking will not be affected and the diagnostic value of the image is preserved. It is also possible to detect which portions of the image has been tampered with. This is known as the *localization* feature.

The proposed watermarking scheme attempts to address the three components of security of medical data and meets the requirements of watermarking-based biomedical image authentication mentioned in Section 2.

4.2 Algorithm

The embedding and authentication process of the proposed watermarking scheme is detailed here.

Selection of Embeddable Coefficients. We chose to implement the scheme on a 4 x 4 transform. Only six coefficients in a 4 x 4 transform block are used for embedding. The position of the six coefficients is shown in the matrix below:

$$\begin{bmatrix} 1 & n & n & n \\ n & 6 & 10 & 14 \\ n & 7 & 11 & 15 \\ n & 8 & 12 & 16 \end{bmatrix}$$

where n denotes the position of the chosen coefficients and the numbers indicate the remaining coefficients. It is noteworthy that the nature of the assignment of embedding in those particular coefficients (i.e. elements $2, 3, 4, 5, 9$, and 13) has been shown by a series of experiments to cause the least degradation to the image quality.

Generation of Quantization Codebook. Compared to cryptographic-based image authentication methods which authenticate binary representations of the

image, watermark-based approaches adopts a tamper detection mechanism based on the fragility of the imperceptible watermark. One approach is the quantization -based watermarking [12,13] which is by oblivious by nature. However, conventional quantization-based watermarking methods are sensitive toward modification and cannot differentiate between incidental manipulations and malicious tampering. As such, there is a need to decrease the fragility of the embedded watermark to ensure that incidental manipulations are not treated as malicious tampering causing the occurrence of false errors. To increase the robustness of the embedded watermark, the quantization intervals can be widened.

By nature, all medical images are usually grayscale images. Hence, we can restrict ourselves to integer values between 0 and 255 for computation purposes when determining the quantization levels. Given the nature of the DPT itself, one would find that it is necessary to form the quantization codebook with each quantization function having three quantization steps.

Watermark Embedding Procedure. Given a host image, I, of dimension $M_I \times N_I$, and a binary watermark image, W, of dimension $M_W \times N_W$, we can then choose the block size, $B = \dfrac{M_I N_I}{M_W N_W}$. For practicality, we have chosen a randomly generated binary message in place of a binary image.

Existing literature review [14,15] discusses the possibility of using the DICOM header or important portions of it as the watermark. In reality, the textual data stored in the DICOM header which consists of sensitive data such as patient information can be used as the watermark as long as it does not exceed the size of $M_W N_W$.

The host image, I, is first divided into adjacent non-overlapping blocks, B. As mentioned earlier, B would consist of a 4 x 4 block. For each block, we perform the two-dimensional DPT on the block to obtain the block of DPT coefficients (B_p).

We embed a watermark value by modulating a selected transform coefficient into the quantized interval determined from the corresponding watermark value:

$$B'_p = \mathrm{Q}_0(B_p) \quad \text{if } W(i,j) == 0$$

or

$$B'_p = \mathrm{Q}_1(B_p) \quad \text{if } W(i,j) == 1$$

After which, we apply the two-dimensional DPT again on the encoded block to obtain the spatial domain image. (Note that the forward and inverse DPT is the same operation).

In an attempt to maintain a high fidelity on the watermarked image, we have chosen Q_0 and Q_1 to embed the watermark value of 0 and 1 respectively.

Authentication Procedure. During the authentication process, the watermarked image is again divided into non-overlapping blocks and for each block, the DPT coefficients are calculated by applying the DPT on the specific block. A simple majority vote scheme is then used to allow more robust decoding of the

embedded check bits. If most of the coefficients are even, then the bit encoded is '0', otherwise the bit encoded is '1'.

The choice of a majority voting scheme would work well with end-users of a telediagnosis system who may have limited knowledge in the medical field, for example, administrative clerks. Hence, they may have trouble detecting modifications made to a digital x-ray if a reference image is unavailable. Thus, it is practical to use such a system which basically checks whether the image received is authentic or not and then, displays the results in a straightforward manner.

5 Experimental Results

The test set consisted of 512 x 512 grayscale single frame biomedical image samples provided by S. Barré [16]. The proposed scheme was implemented on Matlab R2006a with the aid of its Image Processing Toolbox (Version 5.2). For simplicity but without loss of generality, we demonstrate experimental results of the proposed watermarking scheme on three 512 x 512 grayscale images, namely OT-MONO2-8-hip, OT-MONO2-8-colon and OT-MONO2-8-a7. The watermark used was a randomly generated string of binary numbers of the matrix size 128 x 128.

Figs. 1 illustrates the original images and the corresponding watermarked images respectively. As it can be seen, the perceptual quality of the watermarked image is still preserved, hence, meeting the strict requirements of biomedical image watermarking.

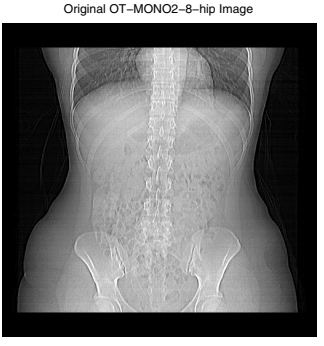
To examine the quality of the watermarked image, we used the peak signal-to-noise ratio (PSNR) signal quality evaluation parameter. Even though the PSNR is normally not associated with perceptual quality, it can provide a measure of image distorsion in terms of numerical values.

We can see that the watermarked versions of the three biomedical images look identical to the original images. The perceptual difference is minimal as indicated by its recorded PSNRs shown in the following table:

Table 1. PSNR Recorded for the Proposed Watermarking Scheme

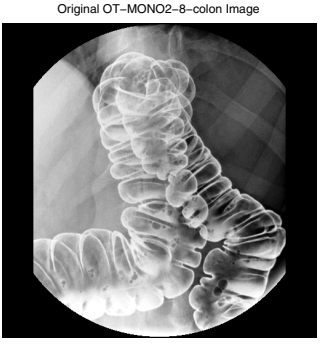
No.	Image Name	PSNR (dB)
1	OT-MONO2-8-hip	32
2	OT-MONO2-8-colon	33
3	OT-MONO2-8-a7	30

To test the authentication scheme, we modified the content of the OT-MONO2-8-hip image as shown in Fig. 2 (a) by adding a shaded region in the middle of the image. In a fragile watermarking scheme, any alteration to the watermarked image would result in an alteration in the watermark itself as well. The retrieved watermark from the modified watermark image is shown in Fig. 2(b).

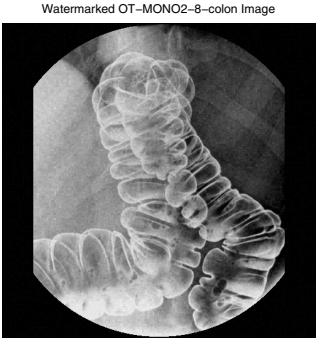


(a) OT-MONO2-8-hip

(b) Watermarked



(c) OT-MONO2-8-colon

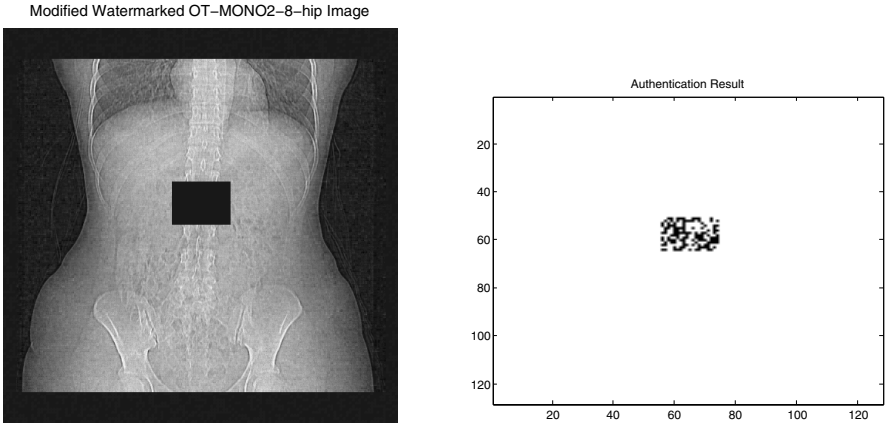


(d) Watermarked

(e) OT-MONO2-8-a7

(f) Watermarked

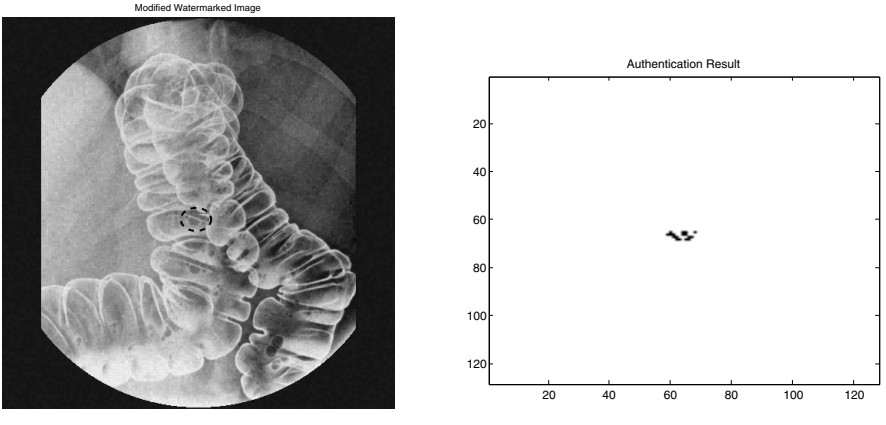
Fig. 1. Original Medical Images vs Their Respective Watermarked Counterparts



(a) Modified Image (Previously Watermarked)

(b) Retrieved Watermark

Fig. 2. An Illustration of the Authentication Ability



(a) Modified Image of Fig. 1d

(b) Retrieved Watermark

Fig. 3. A More Realistic Alteration Attempt

6 Conclusion and Future Works

While in general, we have shown that Watermarking in DPT domain is workable, there exists issues that require further investigation. First, the PSNR obtained from the existing scheme is not satisfactory for practical deployment. Depending on the image region, there exists visible artifacts in monotonous region. An

improved PSNR can be obtained by reducing the quantization steps but our experiments have shown that while achieving 10 dB increase in PSNR, the scheme will not withstand simple LSB erasure attack. An alternative might be selective watermarking where only certain segments of an image are watermarked. We await further results to confirm this intuition. Other perceptual metrics, e.g. Structural Similarity[17], should be taken in account as evaluation metrics.

Second, the security of the current scheme depends solely on the secrecy of the code book. In future version of the scheme, more effort should be put into code book design to prevent reverse engineering of the code book used. Selective watermarking will also increase the security of the current scheme.

From our experiments, it was shown that the current scheme withstands simple attacks such as the erasure of the LSB. As most medical images will be stored in their compressed form, it would be worthwhile to investigate methods of allowing the current scheme to withstand acceptable compression ratio.

In conclusion, an experimental scheme based on DPT for fragile watermarking was proposed and presented in this paper. The scheme is devised primarily with future real time VLSI implementation in mind. We envisage that, with careful revisions, the scheme is potentially useful for digital biomedical media authentication applications.

Acknowledgement

The authors would like to expressed their gratitudes to Swinburne University of Technology (Sarawak Campus) for the support of this work through the Swinburne Sarawak Seed Grant Scheme.

The authors would also like to thank Raphael C.-W. Phan, Loughborough University for his useful discussion in relation to this work.

References

1. Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R.: Relevance of watermarking in medical imaging. In: Proc. 3rd IEEE EMBS Int. Conf. Inform. Technology Applicat. in Biomedicine. 3rd Workshop Int. Telemedical Inform. Soc., Arlington, USA, pp. 250–255 (November 2000)
2. Walton, S.: Information authentification for a slippery new age. Dr. Dobbs Journal 20(4), 18–26 (1995)
3. Coatrieux, G., Maitre, H., Sankur, B.: Strict integrity control of biomedical images. In: Proc. SPIE: Security and Watermarking of Multimedia Contents III, vol. 4314 (2001)
4. Acharya, R., Niranjan, U.C., Lyengar, S.S., Kannathal, N., Lim, C.M.: Simultaneous storage of patient information with medical images in the frequency domain. Comput. Methods and Programs in Biomedicine 76, 13–19 (2004)
5. Ho, A.T.S., Zhu, X., Shen, J.: Authentication of biomedical images based on zero location watermarking. In: Proc. 8th Int. Conf. Control, Autom., Robot., and Vision (2004)

6. Aburdene, M.F., Goodman, T.J.: The discrete pascal transform. IEEE Signal Processing Letters 12(7), 493–495 (2005)
7. Skodras, A.N.: Fast discrete pascal transform. Electronics Letters 23, 17367–17368 (2006)
8. Zhong, Q.-C., Nandi, A.K., Aburdene, M.F.: Efficient implementation of discrete pascal transform using difference operators. Electronics Letters 43, 1367–1368 (2007)
9. DICOM Standard
10. Rey, C., Dugelay, J.-L.: A survey of watermarking algorithms for image authentication. EURASIP J. on Appl. Signal Processing 2002(6), 613–621 (2002) (special issue on image analysis for multimedia interactive services)
11. Macq, B., Dewey, F.: Trusted headers for medical images. In: Proc. DFG VIII-DII Watermarking Workshop (1999)
12. Chen, B., Wornell, G.W.: Quantization index modulation methods for digital watermarking and information embedding of multimedia. Journal of VLSI Signal Processing 27, 7–33 (2001)
13. Eggers, J.J., Bauml, R., Tzschoppe, R., Girod, B.: Scalar costa scheme for information embedding. IEEE Trans. Signal Processing 51(4), 1003–1019 (2003)
14. Coatrieux, G., Lecornu, L., Roux, C., Sankur, B.: A review of image watermarking applications in healthcare. In: Proc. 28th Annu. Int. Conf. of the IEEE EMBS, pp. 4691–4694 (2006)
15. Coatrieux, G., Quantin, C., Montagner, J., Fassa, M., Allaert, F.A., Roux, C.: Watermarking medical images with anonymous patient identification to verify authenticity. In: Proc. 21st Int. Congress of the European Federation for Medical Informatics MIE 2008, pp. 667–672 (2008)
16. Barré, S.: Medical imaging: Samples (2003)
17. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: From error visibility to structural similarity. IEEE Transactions On Image Processing 13(4), 600–612 (2004)