TECHNICAL TRANSACTIONS | CZASOPISMO TECHNICZNE
MECHANICS | MECHANIKA
1-M/2013

WIOLETTA WÓJTOWICZ*

BIOMETRIC WATERMARKING FOR MEDICAL IMAGES – EXAMPLE OF IRIS CODE

BIOMETRYCZNE ZNAKI WODNE W OBRAZACH MEDYCZNYCH NA PRZYKŁADZIE KODU TĘCZÓWKI

Abstract

This paper presents a preliminary investigation on medical image watermarking using biometric watermarks. The goal is to elaborate simple watermarking system based on discrete wavelet transform (DWT) decomposition and binary iris code insertion. The performance of proposed algorithm is evaluated by Hamming distance between embedded and extracted iris code.

Keywords: *watermarking technique*, *DWT decomposition*, *biometric recognition*, *Hamming distance*

Streszczenie

W artykule przedstawiono wstępne rezultaty badań związanych ze stosowaniem biometrycznych sygnatur jako znaków wodnych w obrazach medycznych. Przetestowano prosty algorytm oparty na przeprowadzeniu dyskretnej transformacie falkowej obrazu medycznego i umieszczenia w nim kodu tęczówki pacjenta. Wyniki związane ze skutecznością weryfikacji tożsamości pacjenta na podstawie zakodowanego i odkodowanego z obrazu kodu tęczówki oparto na analizie odległości Hamminga.

Słowa kluczowe: *technika znakowania wodnego*, *dyskretna transformacja falkowa*, *rozpoznawanie biometryczne odległość Hamminga*

* MSc. Wioletta Wójtowicz, Institute of Applied Informatics, Faculty of Mechanical Engineering, Cracow University of Technology.

1. Introduction

Today telemedicine applications play a vital role in the development of healthcare sector. The transmission, storage and sharing electronic medical data became a standard practice for many diagnosis and scientific purposes. Hospitals and health centers have huge databases including medical images and other patients' records. In the management of these databases privacy protection of medical images has always been an important issue. Security solutions should ensure that medical images cannot be accessed by unauthorized users, images are not modified during the transmission and storage and finally images are from correct sources to the claimed receivers. To achieve these objectives it is essential to provide copyright protection of medical images (e.g. [1, 2, 3, 10]). For that matter different techniques of digital watermarking have been employed. Digital watermarking is a technique of embedding a digital code into a cover image without changing the image size, quality and readability of the image. As a result usually watermark should be invisible, secret to unauthorized users, robust against attempt to tamper with it and provides data authentication ([4, 7, 12]).

In this paper, a combination of watermarking technique with biometric recognition system to increase security of medical images is proposed. As biometric data provide uniqueness and watermarking provide secrecy, some possible advantages of merging these techniques with regard to medical images will be demonstrated. The goal is to provide authentication for the patient as the owner of image by encapsulating some biometric characteristic in his medical image. Some simple watermarking algorithm based on discrete wavelet transform (DWT) decomposition, in which the watermark is embedded at different frequency bands, will be elaborated. This frequency domain were chosen as it provides better robustness against attacks and leads to less perceptibility of an embedded watermark. To assure confidentiality of patient data binary iris code is used as a watermark and system performance is evaluated by measuring the similarity between embedded and extracted iris code.

This paper is organized as follows: Section 2 describes the basic issues connected with watermarking technique and biometric recognition; in Section 3 proposed method will be described; Section 4 gives experimental results; Conclusions will be presented in section 5.

2. Review

2.1. Watermarking in DWT domain

A watermarking systems consists of two components: a watermarking embedder and a watermark detector ([2, 4, 7]). Watermark embedding is performed either in spatial domain (e.g. Last Significant Bit algorithm) or transform domain (e.g. DFT, DCT and DWT transforms). The transform domain is shown to be more robust than that is spatial domain. One of the most popular transforms operating in the frequency domain is Discrete Wavelet Transform (DWT), which provides excellent space for image watermarking ([2, 12]). DWT is a hierarchical transformation, which enables analysis of image in the spatial-frequency domain. DWT separates the image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. These bands could be next decomposed recursively in the same way. Finally, the representation of the image on

many resolution levels could be obtained. In practice to get the wavelet decomposition, the highpass filter (H) and lowpass filter (L) are applied to the rows and columns of the image in the spatial domain. Then the watermark could be added to the coefficients of transformation, that are exposure and frequency functions.

Watermarking has become an important issue in medical image security, confidentiality and integrity ([1, 3, 8, 9]). Medical image watermarks are usually used to authenticate (trace the origin of an image) and /or investigate the integrity (detect whether changes have been made) of medical images. One of the key problems with medical image watermarking, is that medical images have special requirements. A hard requirement is that the image may not undergo any degradation that will affect the reading of it (see Fig. 2).

2.2. Biometric recognition

Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics ([5, 6, 11]). To ensure that the rendered services are accessed only by legitimate users and no one else, personal recognition systems could be applied to either confirm or determine the identity of an individual requesting their services. Thus, biometric characteristic should be universal, discriminative and sufficient invariant. Biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Possible applications of such systems could be: commercial (e.g. computer network logging, credit card, medical records management, etc.), government (e.g. ID card, driver's license, passport control, etc.) and forensic (e.g. criminal investigation, terrorist identification, etc.). Depending on the application context, a biometric system may operate either in the verification mode (the system validates a person's identity by comparing the captured biometric data with her own biometric templates stored in the system database) or identification mode (the system recognizes an individual by searching the templates of all users in the database for a match). In various applications a number of biometric characteristics are in use. The most popular are: DNA code, shape of ear, facial images, hand and finger geometry, fingerprint, iris code, signature and voice characteristics. Each of this feature has its strengths and weaknesses, as there is no single biometric which effectively meet the requirements of all applications.

In this paper the iris code as biometric characteristic, which could be used as watermark, is elaborated. The iris is the annular region of the eye bounded by the pupil and the sclera on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition system is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. In addition, it is extremely difficult to surgically tamper the texture of the iris.

In proposed approach this biometric characteristic is used as a watermark to increase the security of medical image. Instead of inserting image of iris (Fig. 1b) just iris code (Fig. 1c) is embedded. Extraction of this code will be based on the Daugman algorithm ([5, 11]).

In proposed method first segmentation of eye image must be performed to detect an iris on this image. Thus, all three parameters (r, x_c, y_c) defining the pupillary circle must be estimated separately from those of the iris. A very effective differential operator for determining these parameters is, ([11]):

$$(r, x_c, y_c) = \arg\left(\max \left| \frac{\partial}{\partial r} \oint_{r, x_c, y_c} \frac{I(x, y)}{2\pi r} ds \right| \right) \tag{1}$$

where:

$I(x, y)$ – is an image containing an eye,
(x_c, y_c) – central coordinates,
r – radius.

The operator in (1) serves to find both the papillary boundary and the outer (limbus) boundary of the iris. Then the circuit shape of detected iris is normalized and mapped to polar representation. As a result every point of iris image from Cartesian coordinates (x, y) is transformed to polar coordinates (r, θ), where r is from [0, 1] and theta is an angle form $[0, 2\pi]$. For iris feature encoding Daugman's method uses Gabor filters which are convoluted with pieces of rectangular iris image. Then obtained complex coefficients are summed and only one resulted complex number is analyzed. The sign of real and imaginary part of this number is taken into account, and for positive values binary '1' is coded, otherwise '0' (Daugman proposed code of length equal to 2048 bits). In this method only phase information is used for recognizing irises because amplitude information is not very discriminating, and it depends upon extraneous factors such as imaging contrast, illumination, and camera gain ([5]).

For identification purposes some comparison between iris codes of different people or different codes of the same person could be performed. As a measure of similarity of iris codes Daugman proposed Hamming distance, which so far is still often used in biometric identification systems. This distance for two vectors A and B of length 2048 could be defined as:

$$H(A, B) = \frac{\sum xor(A, B)}{2048} \tag{2}$$

where xor is simple Boolean Exclusive-OR operator, that detects disagreement between any corresponding pair of bits in considered vectors. Thus, the value of H can be treated as a percent of different pixels in both vectors. If we measure distance of two different person this distance should be near to 0.5, as the probability of occurring '1' or '0' in iris code is equal to 0.5. But when the patterns form the same person are analyzed Hamming distance should be equal or near to 0.

3. Proposed biometric watermarking algorithm

In this section the proposed biometric watermarking algorithm will be described with regard to two main modules: watermark encoding and watermark decoding.

3.1. Watermark encoding

The whole process starts with conversion of iris image to gray scale (see Fig. 1b) and computation of iris code using Daugman algorithm. Then obtained binary vector of length 2048 is divided to 32 vectors of length equal to 64. These vectors are then joined line by line to form binary watermark of size 32×64 (see Fig. 1c).

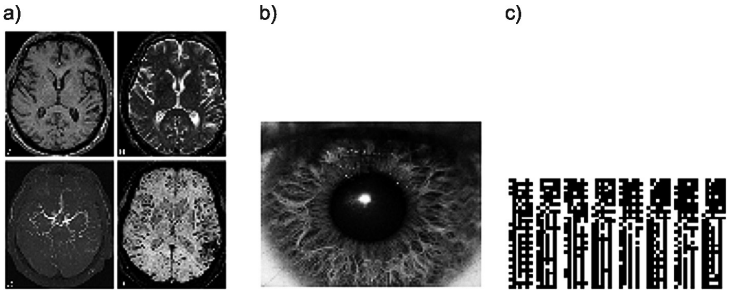

Fig. 1. Encoding: cover medical image ([15]) (a), iris image ([14]) (c), watermark – iris code (c)
Rys. 1. Kodowanie: oryginalny obraz ([15]) (a), obraz tęczówki (14) (c), znak wodny – kod tęczówki (c)

Cover image is gray scale CT image of size 1512×1304 (see Fig. 1a). First one level DWT decomposition of this medical image is computed. Then each of decomposition bands: LL, LH, HL, HH is selected to insert binary watermark. As the size of each band (756×652) is much bigger than the watermark size, it is important to note that watermark is inserted just in the top left corner of each band. The values of watermark are added to the band values and watermarked image is reconstructed using IDWT. According to watermarking of medical images requirements, for each band case watermark is imperceptible (see Fig. 2).

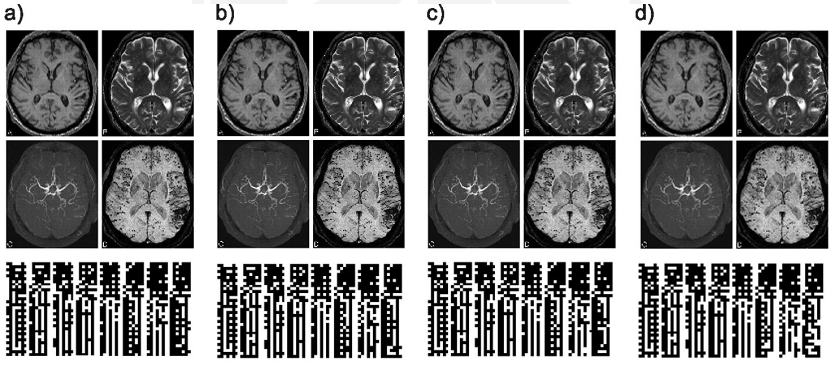

Fig. 2. Decoding: watermarked images and extracted watermarks for schemes when the watermark was inserted in LL (a), LH (b), HL (c), HH (d)
Rys. 2. Dekodowanie: obrazy ze znakami wodnym i wyeksrahowane z nich znaki wodne dla przypadków wstawiania znaku wodnego do komponentów: LL (a), LH (b), HL (c), HH (d)

3.2. Watermark decoding

During the decoding process the data encapsulated in the watermarked medical image are extracted for the authentication purposes. As in presented approach original cover image is available, first this original image is subtracted from watermarked image. Then obtained image is decomposed using DWT and region where the watermark was embedded (top left corner of each band) is selected. The chosen binary part of band should correspond to the code of inserted watermark. To measure the similarity between original iris code and the extracted one the Hamming distance could be employed (see (1), Table 1).

4. Experimental results

The performance of proposed algorithm is tested on each of DWT decomposition components. Obtained results are evaluated in terms of imperceptibility and robustness against three types of attacks: adding 'salt and pepper' noise, median filtering and rotation of watermarked image by 5º (and re-rotation before watermark extraction). The Hamming distance computed for all considered scenarios could be use to evaluate the robustness of watermarking algorithm (Table 1). Taking these values into account one can elaborate the authentication possibilities of watermarking scheme as well. As Hamming distance measures the similarity between inserted and extracted iris code of owner of medical image one can determine in which case the recognition (verification) will be possible. As most of the biometric features of the same individual taken at different times are almost never identical, the threshold t of acceptable difference between iris codes should be introduced. If one set $t = 0.2$, it means that if Hamming distance between two codes is less that t they come from the same person.

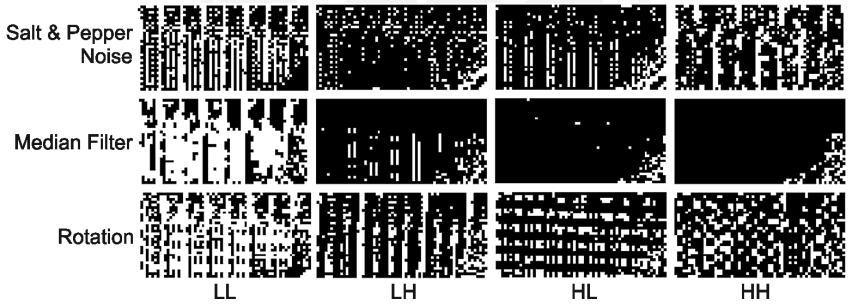

Fig. 3. Extracted watermarks for particular bands LL, LH, HL, HH and considered attacks
Rys. 3. Wyekstrahowane znaki wodne dla poszczególnych komponentów: LL, LH, HL, HH i rozpatrywanych typów ataków na obrazy

In the Figure 1 and Figure 2 all extracted watermarks are presented. In no attack case extracted iris codes are very similar to each other and to the inserted watermark as well, as the Hamming distance for all bands cases is almost equal to 0 (Table 1). But when watermarked image is subjected to different attacks this distance significantly increased, especially for

median filter attack, when for HL, LH, HH Hamming distance is not only much higher than threshold *t,* but it is almost equal to 0.5, what means that analyzed iris codes are from two different people. However obtained results demonstrate that the best verification could be obtained inserting watermark into LL component, which contains details of the original image.

Table 1

Experimental results – Hamming distance between inserted and extracted watermarks

DWT decomposition bands	No attack	Salt & pepper attack	Median filter attack	Rotation (5º → 5º)
LL	0.0059	0.0376	0.2725	0.2090
LH	0.0039	0.3496	0.4897	0.3018
HL	0.0044	0.3477	0.4458	0.2866
HH	0.0122	0.2617	0.4438	0.3286

5. Conclusions

In this paper biometric watermarking scheme for medical images has been elaborated. The proposed scheme satisfies the security and imperceptibility requirements and allow to authenticate medical images using iris code as biometric feature. The confidentiality of patient data is improved by hiding this biometric data as a watermark. The experimental results shows that some simple types of attack can make difficult or even impossible to find the data belongs to particular patient or not. Also it has been noticed that LL component of DWT of image is the most robust against performed attacks.

In a further work, the algorithm will be enhanced in order to obtain watermarked medical images with better robustness and to have recovered watermark with better accuracy.

References

[1] Abdelkader F.M., Elhindy H.M., El-sheimy N., Mostafa S.A., *Wavelet pac ket-based blin watermarking for medical image management*, Open Biomed Eng J, vol. 4, 2010, 93-98.

[2] Arnold M., Schmucker M., Wolthusen S.D., *Techniques and applications of digital watermarking and content protection*, Artech House, Boston, 2003.

[3] Coatrieux G., Maitre H., Sankur B., Rolland Y., Collorec R., *Relevance of watermarking in medical imaging*, 2000 IEEE EMBS Conference on Information Technology Applications in Biomedicine, Arlington, USA, 2000, 250-5.

[4] Cox I.J., Miller M.L., Bloom J.A., Fridrich J., Kalker T., *Digital watermarking and steganography*, San Francisco: Morgan Kaufmann Publishers, 2008.

[5] Daugman J., *How iris recognition works*, IEEE Trans. CSVT, vol. 14, no. 1, 2004, 21-30.

[6] Jain A.K., Ross A., Prabhakar S., *An Introduction to Biometric Recognition*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, 2004.

[7] Katzenbeisser S., Petitcolas F.A., *Information hiding techniques for steganography and digital watermarking*, Artech House, Norwood, MA, 2000.

[8] Maeder A., Planitz B., *Medical image watermarking: a study on image degradation*, Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC 2005), 2005, 3-8.
[9] Li M., Narayanan S., Poovendran R., *Engineering in Medicine and Biology Society*, 26th Annual International Conference of the IEEE,vol. 2, 2004, 3233-3236.
[10] Ogiela M.R., *Systemy utajania informacji – od algorytmów do kryptosystemów szyfrujących*, Wydawnictwa AGH, Kraków 2003.
[11] Ślot K., *Wybrane zagadnienia biometrii*, Wydawnictwa Komunikacji i Łączności, Warszawa 2008.
[12] Vatsa M., Singh R., Noore A., *Feature based RDWT watermarking for multimodal biometric system*, Image and Vision Computing, vol. 27, no. 3, 2009, 293-304.
[13] Zieliński T.P., *Cyfrowe przetwarzanie sygnałów*, Wydawnictwa Komunikacji i Łączności, Warszawa 2005.
[14] Bolwidt E., *In my eyes*, 2008 (http://www.nowpublic.com/health/my-eyes – accessed 1 March 2013).
[15] Mittala S., Wue Z., Neelavallib J., Haacke E.M., *Susceptibility-Weighted Imaging: Technical Aspects and Clinical Applications*, American Journal of neuroradiology, 2009, doi: 10.3174/ajnr. A1461 (http://www.ajnr.org/content/30/2/232/F6.expansion.html – accessed 1 March 2013).