Biometric watermarking for security enhancement in digital images

Wioletta Wójtowicz
EAIiIB Department, Institute of Automatics and Biomedical Engineering,
AGH University of Science and Technology, al. Mickiewicza 30, 30-059 Kraków
e-mail: wwojtowi@agh.edu.pl

In this paper some preliminary investigation on combination of watermarking technique with biometric data to increase security of digital images in case of medical images is proposed. Performance of watermarking algorithm, based on discrete wavelet transform (DWT) decomposition, that incorporates biometric watermark is elaborated. The frequency domain were chosen as it is proven, that this domain provides better robustness against attacks and leads to less perceptibility of an embedded watermark. To assure confidentiality of patient data their hand geometry features are embedded instead of patient's name. Proposed system is evaluated by measuring the similarity between embedded and extracted biometric codes.

Key words: images security, watermarking technique, discrete wavelet transform (DWT), biometrics, principal component analysis (PCA)

Introduction

With increasing growth of the Internet, there is a need to restrict access to sensitive data e.g. medical images which are stored and transmitted between hospitals, health care centers, insurance companies etc., only to authorized users. As biometrics is getting more and more attention in recent years for security and other purposes, to increase the security of medical images we propose to combine biometric techniques with watermarking technology. 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 to protect content of images and to detect the adversary's modifications. As biometric data provide uniqueness and watermarking provide secrecy, some advantages of merging these techniques with regard to medical images are elaborated. The goal is to provide privacy and authentication for the patient, as the owner of medical image, by encapsulating in this image some biometrics code based on his/her hand geometry features.

This paper is organized as follows: Section 2 describes the basic issues connected with watermarking technique and biometric verification with emphasis on hand geometry features; in Section 3 proposed method is described; Section 4 gives experimental results; Conclusions are presented in Section 5.

Experimental methods

Watermarking in DWT domain

A watermarking systems consists of two components: a watermarking embedder and a watermark detector. Watermark embedding is performed either in spatial domain (e.g. Last Significant Bit algorithm) or transform domain (e.g. DFT, DCT and DWT). One of the most popular transforms operating in the frequency domain is Discrete Wavelet Transform (DWT), which provides excellent space for image watermarking, as it is a hierarchical transformation, which enables analysis of image in the spatial-frequency domain. DWT in any particular step separates the image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. Then the watermark is added to the coefficients of transformation, that are exposure and frequency functions, what makes it invisible and robust ([1]).

Watermarking in transform domain has become an important issue in regard to medical image security, confidentiality and integrity ([2],[3]). 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. A hard requirement connected with watermarking medical images is that the image during watermark insertion may not undergo any degradation that will affect the reading of it.

Biometric verification based on hand geometry

Biometric recognition refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics ([4],[5],[6]). To ensure that the rendered services are accessed only by legitimate users and no one else, biometric characteristics should be universal, discriminative and sufficiently invariant. Depending on the application context, biometric systems may operate either in the verification mode (the system validates a person's

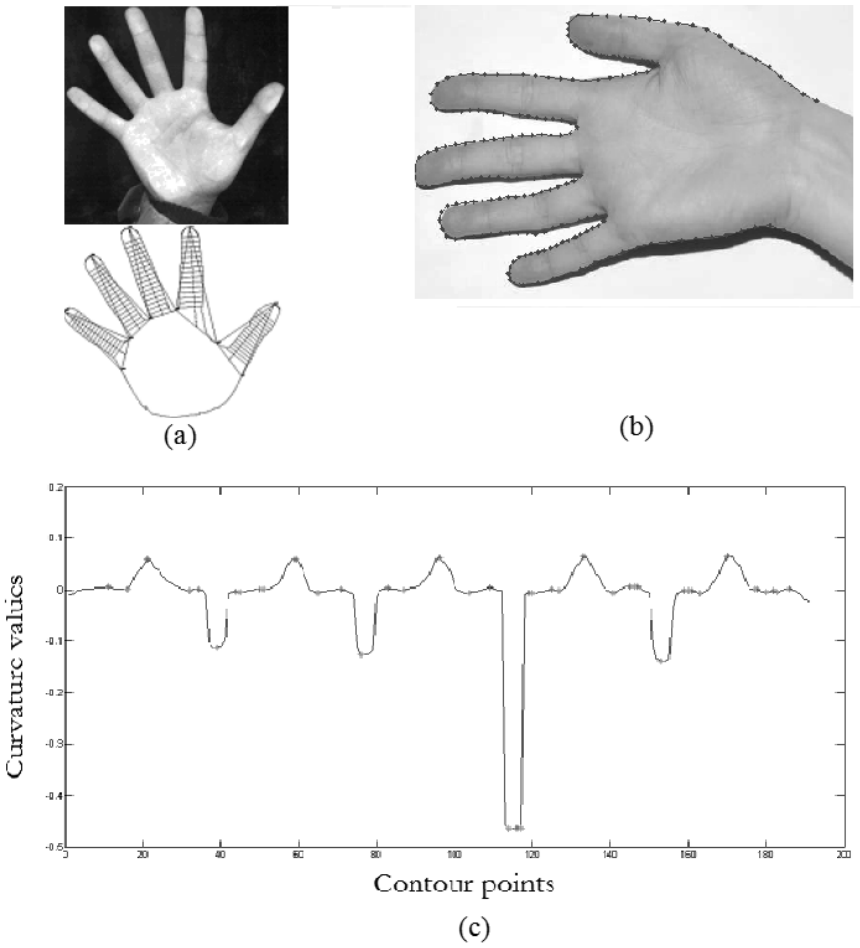

Figure 1. Hand geometry features; hand image and its contour with pointed landmarks, which are used to extract hand features, [4] (a); example of tested hand image with plotted hand contour (b); curvature (of length L=191) of hand presented in figure (b) with pointed extreme points (c)

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: fingerprints, facial images, voice characteristics, iris code, hand and finger geometry and signature. But even if different techniques have been developed there is no ideal biometric measurement, each has its strengths and limitations, according to user acceptance, cost, performance, etc.

In this study the possibility of using hand geometry features in watermarking medical images to authenticate patient's identity is elaborated. Although hand geometry is not very distinctive among human population, this biometrics is frequently used (rather in verification systems) for various reasons: almost all of working population have hands, hand geometry measurements can be easily collectible and ideally suited for integration with other biometrics, e.g. fingerprints, ([7],[8],[9]).

From anatomical point of view, human hand is usually characterized by its length, width, thickness, geometrical composition, shapes of the palm, and shape, geometry of the fingers. Traditionally, to extract these features from hand image during acquisition some special procedure is required to fix the placement of the hand, e.g. using pegs ([9]). However, it can cause deformation on hand geometry, which then reduces the accuracy in feature extraction and further analysis. For these reasons some alternative approaches were also developed to read and process data from hand image independently of the position of the user hand ([7], [8]). This is done by analyzing the curvature profile of the hand contour and segmenting the fingers according to the sequence of curvature extremes. Then nine landmarks (mainly 4 valley points and 5 tip points) are located in curvature profile. As a result features of the hand can be easily computed based only on location of extreme points, e.g. length of the fingers is a distance between section joining neighbor valley points and the tip point (see Figure 1 (a)).

Application scenarios

Hand image processing

During the acquisition of hand images the fingers must be clearly separated from each other in order to obtain a com-

plete hand shape. Then a binarization process takes place by the use of a thresholding method responsible for choosing which pixel belongs to the background and to the hand. As a result a one-pixel-wide hand contour of length L (with the wrist area cut off) is obtained (see Figure 1 (b)). For each contour point (x, y) curvature is calculated from the neighboring points. Before further processing curvature of length L is smoothed using Gaussian filter to reduce the number of curvature peaks. In the Figure 1 (c) there is presented soothed curvature profile with pointed extremes, the most significant peaks correspond either to the tip of the fingers (5 maximums) or to the base of each finger (4 minimums).

Feature selection and feature vector size

Since knowing the location of extremes points in the curvature enables to compute in turn many common hand geometry features ([7], [8]), in the current study construction of the feature vector is based only on hand curvature peaks. Advantage of this approach is that there is no need to embed a whole hand image as a watermark, because basic hand features can be easily computed just after extraction of hand curvature code from the cover image.

The watermark is obtained after certain modification of the curvature profile. Only points associated with extremes are left in the code (they are treated as "geometrical landmarks"), whereas the rest of the points are replaced by zeros. As the resulting vector is of length L and have a lot of non-informative elements (zero points) the reduction of its dimension using Principal Component Analysis (PCA) is also considered (see Figure 2 (b)).

Data hiding metod

In this section the proposed biometric watermarking algorithm will be described with regard to two considered schemes for full and reduced watermark codes presented on Figure 2, scheme (a) and (b), respectively.

In both scenarios the whole process starts with extraction of curvature profiles for 10 considered hand images. First to obtain curvatures, binarization and edge detection on each hand image were performed. Then 100 points from each hand contour were selected and after applaying interpolation procedue next 91 of evenly spaced points between these landmark points were obtained. Finally, sets of 191 hand contour points were used to compute curvatures, curvature extremes and features vectors of length L=191, as described in Section 3.2., (Figure 3 (b)).

Then features vectors are either directly used as watermarks in the first scenario (Figure 2 (a)) or additionally reduced to only 9-dimension vectors in the second scenario (Figure 2 (b)). Dimension reduction is performed after applying Principal Components Analysis (PCA) and reduced length of features vectors (L'=9) corresponds to the number of the most distinctive components obtained for the matrix of 10 full curvatures (Figure 3 (b), (c)).

Cover image in both cases is gray scale CT image of size 750×640 (see Figure 3 (a)). In these application scenarios the cover image is related to the watermark, since medical

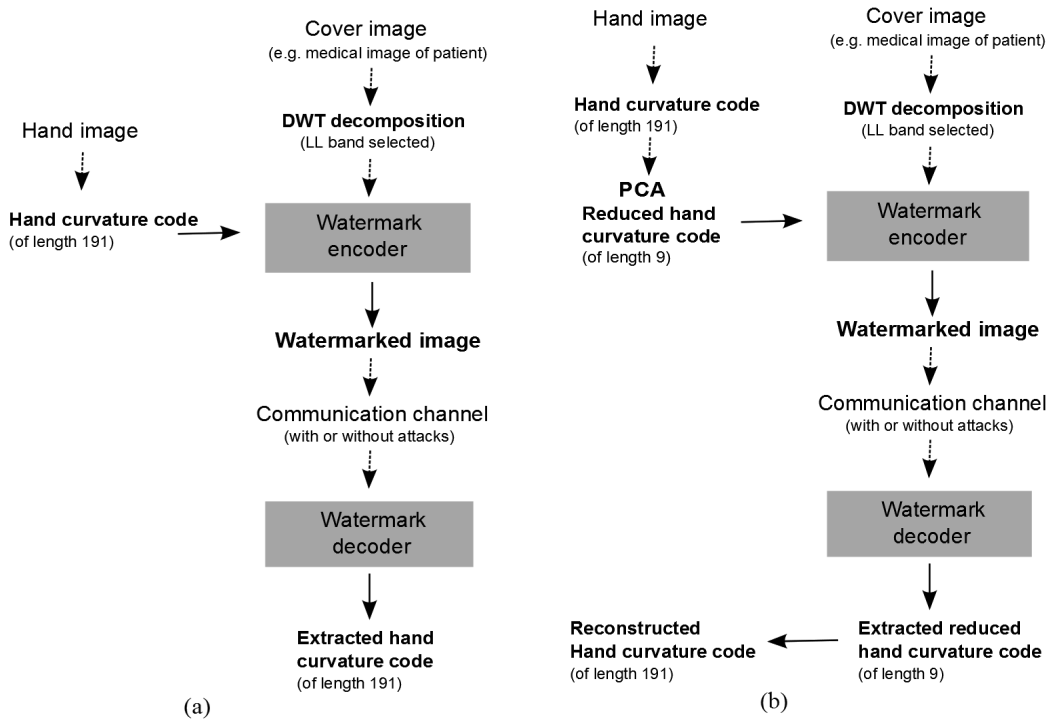

Figure 2. Watermarking schemes; for full curvature code (a); for curvature code reduced using PCA, then extracted code additionally required reconstruction and comparison with full normalized hand code (b).

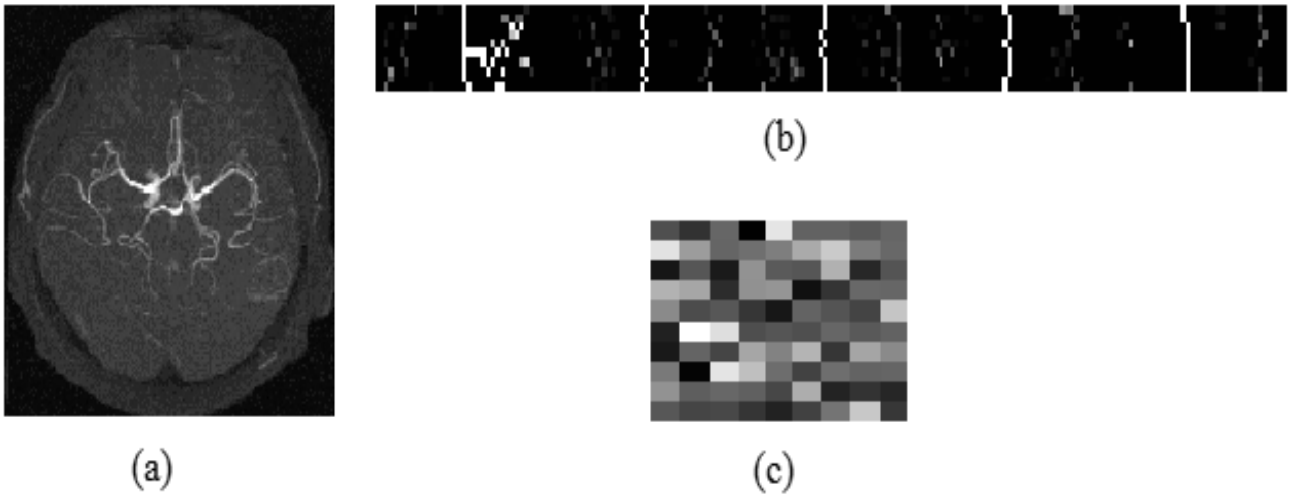

Figure 3. Cover medical image (a); curvature codes of 10 hands (of length 191), in each row there is code of other hand (b); reduced codes of 10 hands (of length 9) after applying PCA, in each row there is code of other hand (c)

image as well as biometric code could own to one person (patient). First for cover image one level DWT decomposition is computed and only LL region is selected to insert biometric watermark. As the size of this subimage (375× 320) is much bigger than the watermark length, the watermark is inserted just in the top left corner of LL band. The values of watermark are added to the image values and watermarked image is reconstructed using inverse of DWT (IDWT).

During the decoding process data encapsulated in the watermarked medical image are extracted and compared with their inserted version (Figure 4). 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 LL band) is selected to compare its pixels values with pixels of embedded watermark.

Experimental results

In the Figure 4 there are presented results for hand image from Figure 1 (b) (for the rest of tested hand images are rather comparable). Columns (a) - (c) are associated with

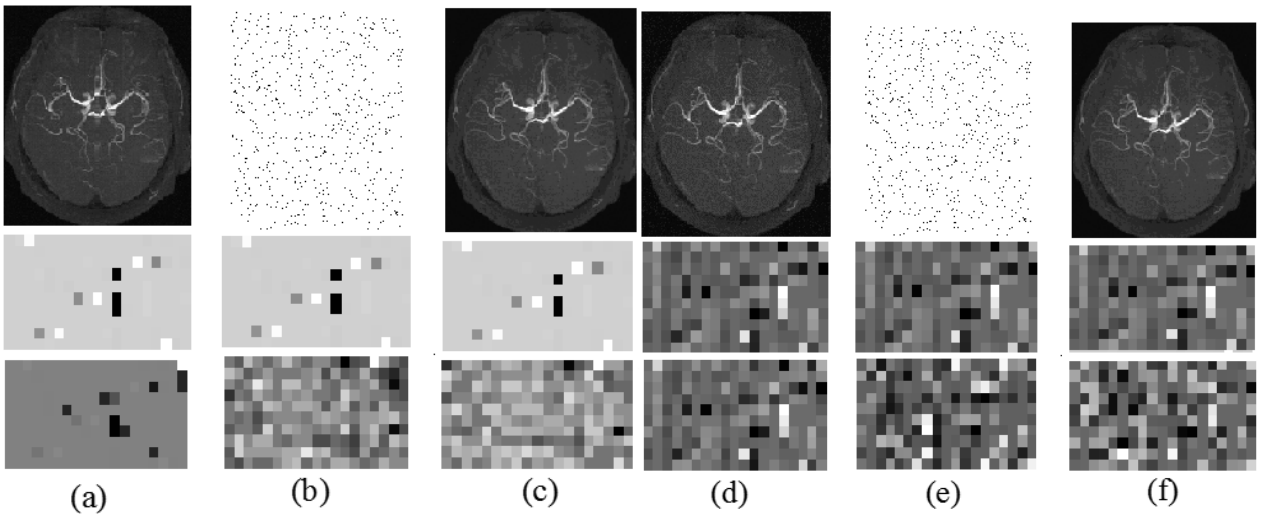

Figure 4. Experimental results for hand presented on Figure 1 for both considered watermarking schemes: (a) - (c) with full biometric codes insertion (scenario 1) and (d) - (f) with reduced biometric codes insertion (scenario 2); watermarked images without attacks, inserted and extracted watermarks (a), (d); watermarked images after "salt and pepper" attacks, inserted and extracted watermarks (b), (e); watermarked images with median filtering attacks, inserted and extracted watermarks (c), (f).

insertion full curvature code (see scheme in Figure 2 (a)) and columns (d) - (f) refer to algorithm with reduced curvature code (see scheme in Figure 2 (b)). In each column of images on the top there is watermarked image (optionally after attack performed), in the middle inserted watermarks resized to matrix form are presented (in (d) - (f) normalized version of watermark form (a) - (c)) and in the bottom there are extracted watermarks. For each of two considered scenarios there is also influence of two hypothetical attacks during the image transmission considered. Figures from (a) and (d) are associated with no attack cases, whereas these from (b), (d) are affected by "salt and pepper" attacks and from (c), (e) by median filtering attacks.

Regarding to the results where full code of hand was inserted, even in no attack case extracted watermark significantly differs from inserted one (very few pixels of inserted and extracted watermarks have the same values), (Figure 4 (a)). Additionally when watermarked image is subjected to different attacks, extracted watermarks were extremely different from inserted ones (pixel values in extracted watermark are strongly affected by attacks, Figure 4 (b), (c)), what during biometric verification means that inserted and extracted hand codes are not from the same person. In this background results presented in columns (d) - (f), seems to be preferable. For no attack case presented in column (d), extracted and inserted watermarks are identical (Figure 4 (b)). Additionally for attacked images presented in columns (e) and (f) biometric verification could be successfully preformed. As in second scenario an inserted code has length equal to 9 pixels, any modification on watermarked image affect the code less than in previous scenario and extracted watermarks are closer to the inserted ones.

Conclusions and future study

In this paper biometric watermarking algorithm based on biometric code for medical images security has been elaborated. The proposed scheme satisfies imperceptibility requirements and allow to authenticate medical images using hand curvature code of patient. 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. However, it was demonstrated that better verification could be obtained inserting as watermark reduced code of hand.

In a further work, hand images base will be expanded in order to construct hand curvature templates and perform biometric recognition with statistical evaluation of obtained results. It enables to enhance watermarking algorithm as well as perform biometric recognition with better accuracy.

References

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

[2] 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, pp. 93 – 98, 2010.

[3] Maeder A., Planitz B., *Medical image watermarking: a study on image degradation*. Australian Pattern Recognition Society (APRS) Workshop on Digital Image Computing (WDIC 2005), pp. 3 – 8, 2005.

[4] Bolle R.M., Connell J.H., Pankanti S., Ratha N.K., Senior A.W., *TAO biometria*, Wydawnictwa Naukowo-Techniczne , Warszawa, 2008.

[5] 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.

[6] Ślot K., *Wybrane zagadnienia biometrii*, Warszawa, Wydawnictwa Komunikacji i Łączności, 2008.

[7] Boreki G.., Zimmer A., *Hand Geometry Feature Extraction through Curvature Profile Analysis*, UNICENP, Computer Engineering Department, 2004.

[8] Wong L., Shi P., *Peg-free hand geometry recognition using hierarchical geometry and shape matching*, IAPR Workshop on Machine Vision Applications, Nara, Japan, pp.281–284, 2002.

[9] Wu J., Qiu Z., A *Hierarchical Palmprint Identification Method Using Hand Geometry and Grayscale Distribution Features*, Eighteenth IEEE International Conference on Pattern Recognition Vol. 00, Issue c, pp. 409-412, 2006.