Annales UMCS Informatica AI XIV, 1 (2014) 85–96
DOI: 10.2478/umcsinfo-2014-0008

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

A Fingerprint-Based Digital Images Watermarking for Identity Authentication

Wioletta Wójtowicz[1*]

[1] *Cracow University of Technology,*
al. Jana Pawła II 37, 31-864 Cracow, Poland

Abstract – In this paper the combination of fingerprint verification methods with watermarking technology to provide copyright protection and authentication of digital images is proposed. The goal of this study is to investigate how watermarking processing affects the quality of biometric watermarks. Performed experiments showed that extracted fingerprint images have roughly equal verification performance even if some watermarked images undergo additional degradation. Proposed methodology will be improved using more sophisticated fingerprint verification methods and subsequently incorporated into multimodal watermarking schemes.

1 Introduction

To ensure that multimedia data, that today can be easily accessed, copied and transmitted, are the forms of the sources for the claimed receivers (authentication), many security systems including cryptography, steganography and watermarking have been proposed, e.g. [**3**], [**4**] and [**13**]. Nowadays many of them are combined with biometrics, especially in the authentication and authorization systems (e.g., [**2**], [**6**], [**7**] and [**12**]). Traditionally the biometric systems operate by acquiring biometric data from an individual, extracting a feature set and comparing it against the template set in the database. Therefore, biometrics finds extensive applications for secure identification (the system recognizes an individual by searching the templates of all users in the database for a match) and personal verification (the system validates a person's identity by comparing the captured biometric data with the biometric templates stored

*wioletta.wojtowicz26@gmail.com

in the system database) purposes. Thus, biometrics-based authentication schemes, using unique, measurable physiological and behavioural characteristics of a person are a powerful alternative to the traditional authentication schemes.

In this paper a security model which enables authentication of digital images owners using watermarking coupled with biometric characteristics is proposed. Digital images watermarking, as a technique of secret communication, involves embedding some digital information (a watermark) into a cover image without changing the size, quality and readability of the image. Regardless of the applications, each watermarking system consists of two main components: encoder and decoder, that involve the processes of inserting the watermark into the cover image and extracting the watermark from the watermarked image, respectively. In the copyright protection applications the watermark should be invisible, secret and robust to resist attacks that attempt to remove or destroy it. It is important to note that even though the watermarking process is perceptually invisible, it alters the pixels of cover image as well as watermark values. For these reasons, in combining watermarking with biometric characteristics it is essential to check how the process of embedding some biometric data in the cover image affects the results of biometric recognition. There have been some papers on watermarking using biometric characteristics. Pankanti and Yeung [**15**] proposed a fragile watermarking method for fingerprint image verification. A logo watermark image is embedded in the spatial domain of a fingerprint image to enable localization of image regions that have been tampered. Jain and Uludag [**8**] proposed the method to hide biometric data (e.g., eigencoefficients of a face image) in cover images (e.g., fingerprints). However, both mentioned papers are focused on using watermarking to improve security of biometric templates. The aim of this paper is significantly different as the possibility of increasing the security of digital images by embedding fingerprint of the owner is elaborated. Thus, the watermarking techniques that guarantee watermark robustness and reliable fingerprint verification methods are the main focus. The first question is how images processing connected with watermarking affects the subsequent processing and utility of the extracted fingerprint images for verification purposes. On the other hand, it is also interesting how to make biometric feature extraction more robust so that it should not lead to significant differences in recognition accuracy for the extracted images.

This paper presents some preliminary results of study in which the known watermarking algorithm based on DWT and FMT ([**11**]) in conjunction with the fingerprint images as watermarks is used. Section 2 describes the proposed methodology in three main parts: fingerprint image processing and verification, watermarking scheme description and evaluation of verification accuracy. In Section 3. fingerprint database and experimental results are presented. Finally, Section 4 concludes the study and introduces future research directions.

2 Proposed Methodology

2.1 Fingerprint Images Processing and Minutiae Extraction

The fingerprint is the earliest and the best known form of biometrics. The proven uniqueness and stability of the fingerprint, as a pattern of flow-like ridges and valleys on the surface of a finger, make it widely used in recognition of a person's identity. Other strengths of this biometrics are low cost of acquisition and high user acceptance ([**7**], [**16**], [**18**]).

Current fingerprint recognition techniques can be mainly classified as minutiae-based, ridge feature-based and correlation-based ([**10**], [**14**]). Indeed, most automatic fingerprint identification methods belong to the first group and require extraction minutiae points (the ridge endings and bifurcations) from fingerprint images. These features are represented in terms of triplets $[x, y, \theta]$, where $[x, y]$ represents the spatial coordinates in a fixed image-centric coordinate system and θ represents orientation of the ridge at that minutia. As a result, each fingerprint is represented as the list of minutiae. Since the minutiae-based recognition methods require accurate detection of the minutiae, the fingerprint images should be first processed as explained in [**5**] and [**17**]. These pre-processing steps include: i) normalization and segmentation to find the fingerprint region in the image; ii) image enhancement in order to obtain a better image quality using ridge orientation, ridge frequency images and filtering with a complex filter; iii) binarization of filtered image and its skeletonisation. Then one pixel wide structure of ridges is obtained and minutiae are extracted by examining the local neighborhood of each ridge pixel using a 3×3 window (Crossing Number method, see [**17**]). Finally spurious minutiae detected in the highly corrupted fingerprint regions or introduced by preceding processing steps are removed from the extracted minutiae set according to the structural post-processing rules, [**10**]. Figure 1 presents some steps of fingerprint image processing, the image comes from the database examined in Section 3.

When minutiae are extracted from the fingerprint images, another important issue is minutiae matching. The objective of this procedure is to determine whether or not the two prints represent the same finger. The similarity between two representations is typically quantified in terms of matching score (values from 0 to 1), that is determined from the number of matched minutiae and normalized by the total number of minutiae in both fingerprint representations. Obviously, the higher the matching score, the more similar are the representations. In practice the matcher uses a threshold value to decide whether a given pair of prints belongs to the same finger (matching score higher or equal to the threshold value) or not (matching score lower than the threshold value).

2.2 Watermarking Scheme

Depending on the algorithm, the watermark embedding is performed either in the spatial domain, when some pixels values of cover image are changed directly or in the transform domain, when a watermark is embedded in the transformed cover image

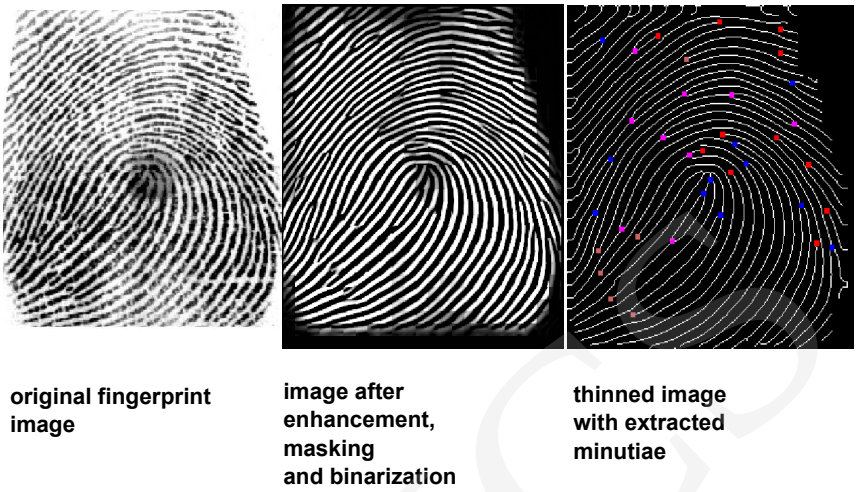

FIG. 1. Sample fingerprint images during the minutiae extraction process performed according to [**21**]

(e.g. DFT, DCT and DWT transforms). Even if the transform domain watermarking, compared with the spatial domain watermarking, is a more complex procedure, it generally increases watermark imperceptibility as well as robustness ([**1**], [**3**], [**9**]). For these reasons, watermarking algorithms, usually integrating a few image transforms simultaneously, are preferred in the copyright applications.
In [**11**] Manoochehr, Pourghassem and Shahgholian introduce a watermarking algorithm based on the combination of Discrete Wavelet Transform (DWT) and Fourier-Mellin Transform (FMT). The embedding procedure starts with computation of DWT of both the cover image and the watermark and selecting the horizontal or vertical subbands (the region of medium frequencies) for further processing. Then FMT is applied to both components and finally obtained magnitudes are combined. Using the inverse transformations IFMT and IDWT, the watermarked image is reconstructed. The proposed algorithm was tested on various watermarks and leads to low visibility of inserted images and robustness against many common attacks.

By virtue of these advantages we applied the algorithm from [**11**] to our scheme, replacing the logo watermark with the fingerprint image. The considered watermarking procedure, which was run for the same gray scale cover image "Lena" of the size 512×512 and different fingerprint images, is presented in Figure 2. Even if the embedding part of this procedure is quite straightforward, as having an original cover image and the watermark image of transformations could be performed easily, the decoding part needs some additional comments. One must note that in the presented watermarking scheme for the watermark extraction, the FMT magnitude of cover image I as well as the original watermark w are required. The first one is subtracted from the FMT magnitude of watermarked image Iw and the latter is needed to perform the final IDWT. Since at the decryption stage only the watermarked image is not sufficient to

extract the fingerprint image *w'*, the presented watermarking procedure could be placed between the semi-blind (semi-private) and non-blind (private) watermarking schemes. The semi-blind watermarking systems to extract watermark data from the watermarked image use additionally original watermark whereas the non-blind watermarking scheme needs the original cover image or the cover image and the watermark. Such schemes are often used for copyright protection (ownership), copy control and fingerprinting, where the goal is to answer the question whether the watermark data exists or to identify the original owner of images. Thus, introducing these issues into the biometrics-based watermarking scheme, the whole procedure could be summarized as follows. One part to prevent ownership of some image I, embed one's fingerprint watermark w in this image at the encoding stage. Then he or she sends this watermark w, watermarked image Iw and the FMT magnitude of I to the second part claiming ownership of I. The second part could then extract w' and additionally verify if w' is close enough to w, so the owner of the image could be verified.

2.3 Performance Evaluation

Generally the performance of watermarking algorithms is evaluated using some common measures such as peak signal-to-noise ratio (PSNR), mean square error (MSE), normalized cross correlation or histogram similarity (e.g.,[**1**]). However, taking into account the proposed watermarking scheme higher or lower values of these metrics do not ensure higher performance of biometric verification that is essential in this system. Therefore, more appropriate measure should be the recognition accuracy for data before and after extraction.

Two commonly used metrics in the authentication accuracy of biometric systems are False Acceptance Rate/False Matching Rate (FAR/FMR) and False Rejection Rate/False Non-Matching Rate (FRR/FNMR). Traditionally, FAR is defined as the ratio of the number of incorrectly accepted impostor tests to the total number of impostor tests. Simply, it is the percentage of times when a system produces a false acceptance, so an individual is incorrectly matched to another individual. Then FRR, as the ratio of the number of incorrectly rejected genuine tests to the total number of genuine tests, is the percentage of times the system produces false rejects, so when an individual is not matched to his/her own existing biometric template. These errors depending on different threshold values are illustrated using the ROC (Receiver Operating Characteristics) curves. These curves are used to compare different system performance, i.e. for FAR and FRR plotted ROC the closer is to the down left corner, the better system is.

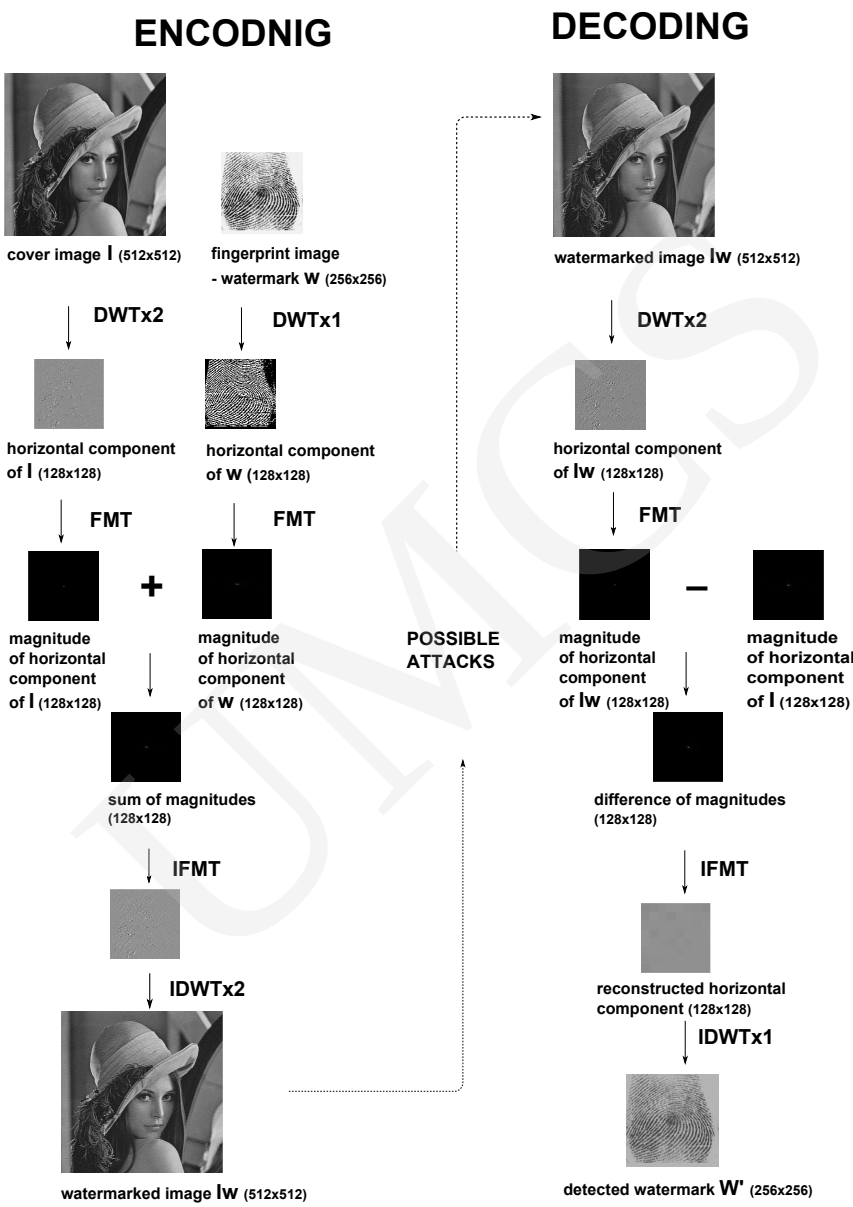

FIG. 2. Watermarking scheme, based on [**11**]

3 Experiments and Results

3.1 Database

In this experiment, a subset of 800 fingerprint images (100 subjects, 8 sample for each subject) was chosen from the SDUMLA-HMT multimodal database. This database was

set in 2010 by the Group of Machine Learning and Applications from Shandong University (SDUMLA) and now is freely available, [**20**]. The whole database includes real multimodal data (face images, finger vein images, gait videos, iris images and fingerprint images) from 106 individuals. The substantial part of the SDUMLA-HMT database is the multi-sensor fingerprint data set that includes fingerprint images captured from each of the 6 fingers with 5 different type of sensors (one swipe fingerprint scanner, one capacitive fingerprint and three optical fingerprint scanners). It must be noted that 8 impressions were captured for each of the 6 fingers using all five sensors. As a result, this multi-sensor fingerprint database contains $6 \cdot 5 \cdot 8 \cdot 106 = 25,440$ fingerprint images in total. Every fingerprint image is saved in 256 gray-level "bmp" format but the size varies according to the capturing sensors. Figure 3 shows the sample fingerprint images from the database, in each row there are three different impressions of the same finger.

FIG. 3. Sample images from SDUMLA-HMT database ([**20**]); in each row they are different impressions of the same finger

3.2 Experiments and Results

For the presented study 800 fingerprint images (100 subjects and 8 impressions per each subject) of the left hand thumb were selected from the SDUMLA-HMT database. First all images, originally of the size 294×304 using the URU4000 optical fingerprint scanner developed by Zhongkong Inc, were resized to 256×256 to enable incorporating

them into the watermarking scheme. According to the watermarking procedure described in Section 2.2 and presented in Figure 3 all fingerprint images were embedded as watermarks in the "Lena" cover image. Then minutiae extraction and matching were performed on the raw fingerprint images and the images after extraction to measure the influence of watermarking processing on verification accuracy.

All fingerprint images to extract minutiae sets are processed as explained in Section 2.1 and [**17**]. Figure 2 shows the sample outputs of this pre-processing procedure: original image, enhanced image and thinned binary image with minutiae. In this experiment for minutiae extraction and matching we used open source software ([**21**]), that was tested so far only on the well-known database FVC2002 DB1_A (Fingerprint Verification Competition 2002 database, [**19**]). However, even if it performs reasonably well on the FVC2002 database, there is no guarantee that it works in the same way for fingerprints from the SDUMLA-HMT data set. Furthermore, as the latter database is relatively new, it is even difficult to determine how high recognition accuracy should be expected. Therefore, in this preliminary study the high accuracy value is not a main focus. The goal is rather to elaborate how watermarking image processing affects this recognition.

First, the verification accuracy within the selected fingerprint data set (before watermarking) from the SDUMLA-HTM database was tested. According to the performance evaluation methodology (e.g., [**19**]) a symmetry of matching scores was assumed, i.e. matching score of i compared to j fingerprint for $i \neq j$ returns the same value as comparing j to i. Thus for 100 fingerprints with 8 impressions for each, the total numbers of genuine and impostor comparisons are equal to $8 \cdot \frac{7}{2} \cdot 100 = 2800$ and $100 \cdot \frac{99}{2} = 4950$, respectively. Then the same checks were performed within this data set after undergoing watermarking scheme (without attacks). The results in terms of the lowest EER value were equal to 13.6% (threshold equal to 0.45) and 16.5% (threshold equal to 0.44) for the data before and after watermarking, respectively. Even if the obtained recognition accuracy was quite poor, it was observed that the results decrease when the images undergo watermarking processing.

Another goal was to compare both databases, i.e. to check if sample fingerprint images after extraction from watermarking schemes, compared with the data before watermarking, still enable subjects verification. For each extracted sample fingerprint (800 images) similarity scores comparing it with the whole database of raw images were computed. The total number of genuine and impostor comparisons was $8 \cdot 8 \cdot 100 = 6400$ and $100 \cdot 99 = 9900$, respectively. Furthermore, as the electronic transmission of watermarked image over the communication channel could introduce degradations in the image data (see Figure 3), some attacks on the watermarked images were simulated. These effects were studied by using various processing attacks such as (i) resizing of watermarked image (to 0.5 scale and then back to the original size), (ii) median filtering using 4×4 element, (iii) adding salt and pepper noise, (iv) cropping: the square of size near to the quarter of the image is cropped from the upper right corner of image, (v)

TABLE 1. Equal Errors Rates (EER) and corresponding threshold values for the tested watermarking schemes

attacks	*treshold*	*ERE*
no attacks	0.44	0.1232
resizing	0.45	0.1208
median filtering	0.45	0.1214
salt and pepper	0.45	0.1220
cropping	0.45	0.1265
JPEG, Q=80	0.44	0.1263

JPEG compression: compressed images are written in the JPEG format using *imwrite* function, with the quality factor $Q = 80$.

For all experiments the recognition evaluation was performed comparing similarity scores with each hypothesized threshold value from 0.1 to 1 by 0.1, and characterized by the FARs and FRRs values. The obtained results were used to compute Equal Error Rates (EER), as the intersection of the FAR and FRR curves for the corresponding thresholds, see Table 1. Finally the authentication accuracy for different watermarking schemes was characterized using the ROC curves partially shown in Figure 4. These curves correspond to all performed comparisons for the raw and extracted data. The proximity of the ROC curves indicates that all watermarking schemes incorporating attacks do not show any significant degradation in the fingerprint verification accuracy compared with the schemes without attacks. However, it was observed that the attacks connected with resizing, filtering and adding a noise lead to less degradation than cropping and compression attacks. It should be also noted that for this first group of attacks recognition results were slightly better than for the watermarking scheme without attacks.

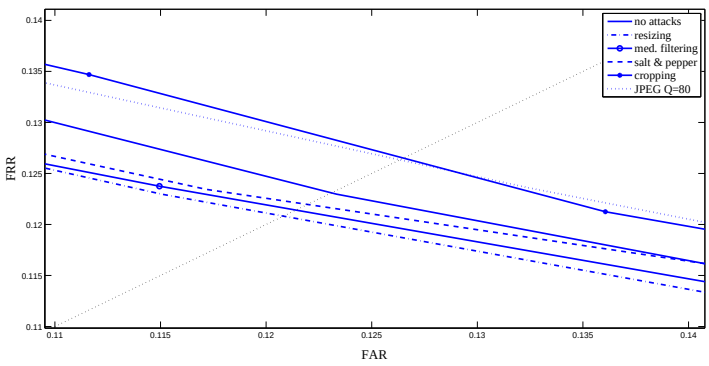

FIG. 4. ROC curves for the tested watermarking schemes

4 Conclusions and Future Directions

This paper presents some preliminary results of study concerned with incorporating fingerprint images in the digital images watermarking schemes for the user authentication purposes. Even if the algorithms used for verification accuracy of biometric data return not impressive results, the experiments elaborated the differences between raw and extracted fingerprint images as well as the influence of some common attacks on watermarking schemes in terms of biometric verification accuracy. Based on the obtained results we can conclude that the used watermarking method does not lead to a significant verification accuracy loss, however, it must be investigated closely using better minutiae extraction and matching tools. There is possibility that employing in the future more sophisticated algorithms connected with fingerprint matching (also ridge feature-based and correlation-based methods) will increase the recognition accuracy and the differences between the proposed watermarking schemes will become more significant. Furthermore, in the presented study the performance of authentication could be affected by matching fingerprint images to each other (to different impressions of the same finger and other fingers) rather than to the fingerprint templates. Since using templates instead, the raw fingerprint images make recognition procedure more robust to poor quality images and other artifacts influencing in the future the database of fingerprint templates will be constructed. Ultimately, the proposed methodology will be developed toward multimodal watermarking schemes, so that some other biometric features from the SDUMLA-HMT database could be included to improve the user authentication performance.

References

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

[2] Bringer J., Chabanne H., Kindarji B., Identification with encrypted biometric data, Security and Communication Networks 4 (2011): 548–562.

[3] Cox I.J., Miller M.L., Bloom J., Fridrich J., Kalker J., Digital watermarking and steganography, Morgan Kaufmann Publishers, Burlington (2008).

[4] Dittmann J., Wohlmacher P., Nahrstedt K., Using cryptographic and watermarking algorithms, IEEE MultiMedia 8 (2001): 54–65.

[5] Hong L., Wan Y., Jain A. K., Fingerprint image enhancement: Algorithm and performance evaluation, IEEE Transactions on Pattern Analysis and Machine Intelligence 20 (1998): 777–789.

[6] Jain A.K., Ross A., Prabhakar S., Biometrics: A Tool for Information Security, IEEE Transactions on Circuits and Systems for Video Technology 14 (2004): 4–20.

[7] Jain A.K., Ross A., Prabhakar S., An Introduction to Biometric Recognition, IEEE Transactions on Information Forensics and Security 1 (2006): 125–143.

[8] Jain A.K., Uludag U., Hiding biometric data, IEEE Transactions on Pattern Analysis and Machine Intelligence 25n(2003): 1494–1498.

[9] Katzenbeisser S., Petitcolas F.A., Information hiding techniques for steganography and digital watermarking, Artech House, Norwood (2000).

[10] Maltoni D., Maio D., Jain A.K., Prabhakar, S., Handbook of Fingerprint Recognition, Springer, London (2009).

[11] Manoochehri M., Pourghassem H., Shahgholian G., A Novel Synthetic Image Watermarking Algorithm Based on Discrete Wavelet Transform and Fourier-Mellin Transform, In: IEEE 3rd International Conference on Communication Software and Networks (ICCSN), IEEE Press, New York (2011): 265–269.

[12] Noore A., Singh R., Vasta M., Houck M.M., Enhancing security of fingerprints through contextual biometric watermarking, Forensic Science International, 169 (2007): 188–194.

[13] Ogiela M.R., Ogiela U., DNA-like linguistic secret sharing for strategic information systems, International journal of information managemant, 32 (2012): 175–181.

[14] Ouyang Z., Feng J., Su F. Cai A., Fingerprint Matching With Rotation-Descriptor Texture Features, In: 18th International Conference on Pattern Recognition (ICPR), IEEE Press, New York (2006): 417–420.

[15] Pankanti S., Yeung M.M., Verification Watermarks on Fingerprint Recognition and Retrieval, Proc. SPIE 3657 (1999): 66–78.

[16] Reid P., Biometrics for Network Security. Prentice Hall PTR, New Delhi (2003).

[17] Thai R., Fingerprint image enhancement and minutiae extraction, Programme report, University of Western Australia (2003).

[18] Tripathi K.P., A comparative study of biometric technologies with reference to human interface, International Journal of Computer Applications, 14 (2011): 10–15.

[19] Fingerprint Verification Competition 2002, available at http://bias.csr.unibo.it/fvc2002, accessed: 14.04.2014.

[20] Fingerprint SDUMLA-HMT database, available at http://mla.sdu.edu.cn/sdumla-hmt.html, accessed: 13.05.2014.

[21] Software for minutiae extraction and matching, available at http://mla.sdu.edu.cn/sdumla-hmt.html, accessed: 14.04.2014.