Biometric Security Systems for Mobile Devices based on Fingerprint Recognition Algorithm

Michał Szczepanik, Ireneusz Jóźwiak
Institute of Informatics,
Wrocław University
of Technologies
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
Email: {michal.szczepanik, ireneusz.jozwiak}@pwr.wroc.pl

***Abstract*—In this paper, we propose a selective attention algorithm which increases the reliability of biometrics security system based on fingerprint recognition. We compare the existing fingerprint recognition algorithms and test our own algorithm on fingerprints database which changes in the structure as a result of physical damage. We propose new selective attention algorithms, which help to detect the most sensitive to damage areas, and add it as step of fingerprint analyses for the fingerprint recognition procedures. We also propose a new algorithm, which does not require complex hardware systems, so it can be applied in new smart mobile devices, which restrict unauthorized access to sensitive data or other user resources. The main goal of this work is to demonstrate the applicability of the developed algorithm in mobile devices.**

Keywords-biometric; fingerprint; minutia group; selective attention algorithms.

I. Introduction

Nowadays, mobile phones, tablet PCs and other mobile devices are an excellent source of data about users. They are used as a remote office, a tool for bank account management, email management, as well as entertainment like social media, real time social games, etc. The only applicable security method is a four-digit pin, which is usually easy to guess or break. Computational capabilities of current devices are not as limited as two years before [17]. Today, mobile phones have the computational capabilities similar to personal computers which could be bought one or two years ago; so, why should they not use better security systems, such as biometrics systems. The accuracy of a fingerprint verification system is critical in a wide variety of civilian, forensic and commercial applications such as access control systems, credit cards, phone usage, etc. The main problem, from an economic point of view, can be the size of the used system hardware and its cost, and therefore it cannot be too extensive and advanced. Fingerprints are the most widely used biometric feature for personal identification and verification in the field of biometric identification [11][19]. Most important for designing the system is the effectiveness of fingerprint recognition algorithms, which depends mainly on the quality of digital fingerprint images input and fingerprint's physical damage [9]. Current mobile devices typically use as collateral for a four digit pin code or face recognition system, which doesnt work when is too darker. Most fingerprint recognition algorithms are not immune to damage, so they are not use in mobile devices. The main problem, which we would like to solv,e is the stability of the recognition systems with respect to the capability to deal with fingers damage, will make the system more useful to the user.

In Section II, we explain the basic parameters and and measures for the safety and usability of biometric systems. In Section III, we briefly analyze existing algorithms and how they work. In Sections IV and V, we present preprocessing and method for comparing fingerprints by our algorithm. In the section The quality of the algorithms, we present first test of our algorithm on public fingerprints database. In the next section, we explain how we represent data for our algorithm. The most important section of this paper is The experiment, in which we present results of tests, which are done on real mobile devices.

II. Quality assessment of biometric algorithms

There are two most important performance metrics for biometric systems [17]: False Accept Rate (FAR), also called False Match Rate (FMR), is the probability that the system incorrectly matches the input pattern to a non-matching template from the database. It measures the percent of invalid inputs which are incorrectly accepted. False Reject Rate (FRR), also called False Non-Match Rate (FNMR), is the probability that the system fails to detect a match between the input pattern and a matching template from the database. It measures the percent of valid inputs which are incorrectly rejected. They can be presented mathematically as:

$$FAR(T) = \int_{Th}^{1} p_i(x)dx \quad (1)$$

$$FRR(T) = \int_{0}^{Th} p_i(x)dx \quad (2)$$

where Th is the value of a threshold used in the the algorithm. Both FAR and FRR are functions of a threshold T. When T decreases, the system has more tolerance to intraclass variations and noise; however, FAR increases. Similarly, if t is lower, the system is more secure and FRR decreases.

III. History and existing solutions

First mobile phone with fingerprint recognition system was developed by Siemens in 1998 [19]. Since that time, more than 100 phone models had such a protection [15]. Unfortunately, the biggest problem of those systems was usability. Every day, people are exposed to cuts, wounds and burns; therefore, it is important that the algorithms are resistant to this type of damage. The current fingerprint recognition systems for mobile devices usually use one of the algorithms: Minutiae Adjacency Graph (MAG), Elastic minutiae matching (EMM), Delaunay Triangulation (DT), Pattern-Based Templates (PBT) [10]. The most popular algorithms are based on local and global structures represented by graphs like in MAG [16]. In this type of algorithms, local structures to find corresponding points to align feature vector are used first, then global structures are matched [4][5]. This type of algorithm was used by He and Ou [6], Ross et al. [16]. They also use thin-plate spline (TPS) model to build an average deformation model from multiple impressions of the same finger. Owing to iteratively aligning minutiae between input and template impressions, a risk of forcing an alignment between impressions originating from two different fingers arises and leads to a higher false accept rate. Typically, a minutia matching has two steps:

- Registration aligns fingerprints, which could be matched, as well as possible.
- Evaluation calculates matching scores using a tolerance box between every possibly matched point (minutiae) pairs.

The EMM algorithm typically uses only global matching where each point (minutia) which has a type, like end point or bifurcation, needs to be matched to a related point in the second fingerprint image. Based on elastic deformations which are used to tolerate minutiae pairs that are further apart because of plastic disrotations, and therefore to decrease the False Rejection Rate, so in most popular algorithms authors increase the size of bounding boxes [13] to reduce this problem, but as side effect they got higher False Acceptation Rate (FAR). In this type of algorithms, for elastic match, TSP [1] also can be used, which provides better performance than only one parameter of deformation.

The DT algorithm [2][14] is the most popular version of MAG, so it was tested as separate algorithm. Its structure based on triangulation connects neighboring minutiae to create triangles, such that no point (minutia) in P is inside the circumcircle of any triangle in DT(P). DT algorithm analyzes the structure of points identically as minutiae adjacency graph algorithm, so it also is not resistant to typical injury of physical fingerprint (see Figure 1).

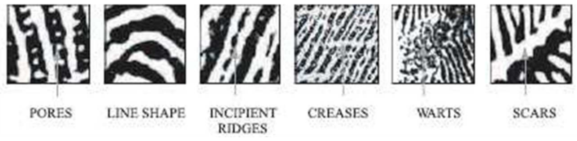

Figure 1. Typical damages on fingerprint

The Pattern based algorithms [3] compare the basic fingerprint patterns (like arch, whorl, and loop between a previously stored template and a candidate fingerprint. This algorithm requires that the images be aligned in the same orientation and in the same scale. To do this, the algorithm finds a central point in the fingerprint image and centers on it, and after that, scales to the same size of the fingerprints ridge. In a pattern-based algorithm, the template contains the type, size and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match. Due to the storage of the original picture for the algorithm there is a high risk that this image can be read from the memory card reader or fingerprints database.

IV. Fingerprint recognition algorithm based on minutia' groups

The proposed solutions, in contrast to other algorithms, are more resistant to damage.

A. Fingerprint recognition algorithm based on minutes groups

For older low-resolution readers it is required to detect the areas of correct scanning of the fingerprint. First step of image analysis is the search for the imprint area including the exclusion of areas containing significant damage [18]. Fingerprint image is represented by a gray scale image that defines the area of forced application fingerprint for the reader (see Figure 2).

$$I_{fp}(i,j) =< 1,255 > \tag{3}$$

The operation that converts a grayscale image into a binary image is known as binarization. We carried out the binarization process using adaptive thresholding. Each pixel is assigned a new value (1 or 0) according to intensity mean in a local area and the parameter t_g which excludes poorly read fingerprint areas from the analysis (see Figure 3).

$$B_{fp}(i,j) = \begin{cases} 1 for I_f p(i,j) \geqslant t_g \\ 0 for I_f p(i,j) < t_g \end{cases} \tag{4}$$

The last step is creating the fingerprint mask based on the binarized image. The Mask for the area of a square (X, Y), which size is 2.5 wide edges, is determined by two

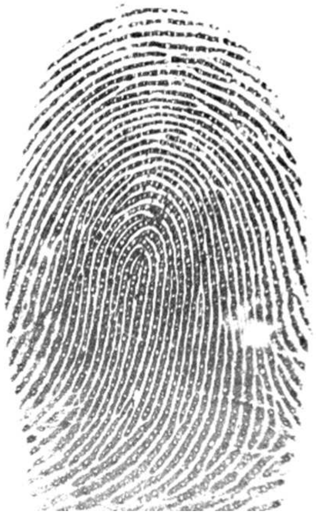

Figure 2. Original image (Source: own work)

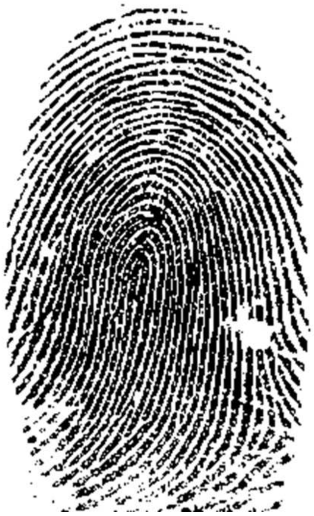

Figure 3. Image after binarization (Source: own work)

parameters p_{lo}, which is a limitation that excludes areas with an insufficient number of pixels describing the image, and p_{hi} excludes blurred areas, such as moist (see Figure 4).

$$F_fp(X,Y) = \begin{cases} I_fp(X,Y) for F_{img} \geqslant p_{lo} \wedge F_{img} \leqslant p_{hi} \\ 0 \; otherwise \end{cases} \tag{5}$$

Where F_{img} is

$$F_{img} = \sum_{i \in X} \sum_{j \in Y} Bfp(i,j) \tag{6}$$

Created mask is used for finding the most damaged area in the fingerprint image.

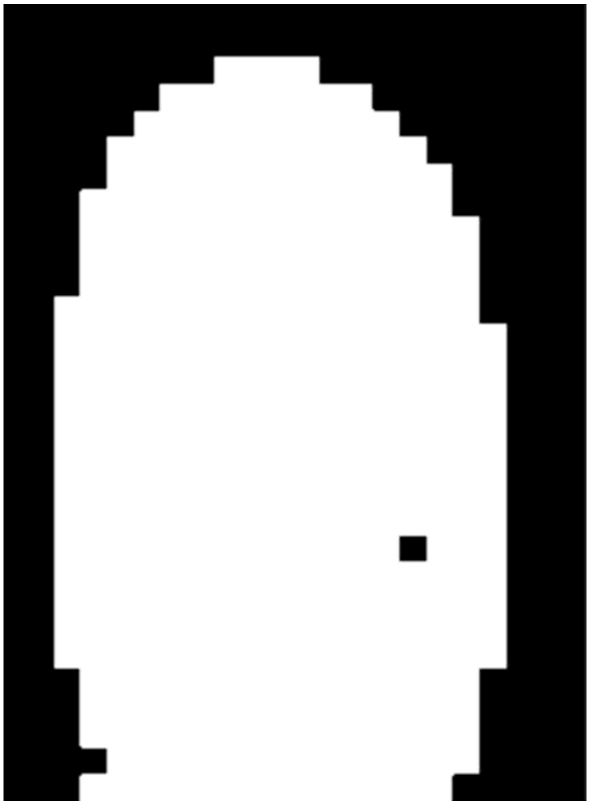

Figure 4. Mask for fingerprint with detecting damage (Source: own work)

B. Detecting features and leveling of the damage in segmentations

Standard leveling of damage is carried out by calculating the variance of points and the analysis of brightness. Based on these two parameters, the frequency of furrows is calculated, which is used for each fingerprint image. After applying Gabor filter [12] to highlight the pits and valleys, it uses segmentation in accordance with its size, 2.5 width of segment furrow, the image is redrawn. After that process fingerprints are continuous and lint. In contrast to the literature, the algorithm does not require additional transformations to find the minutiae, such as converting the width of 1px furrows. It does not require information about the orientation of minutiae; it only requires the data about its position. Therefore, the resulting image is used to find the edge - the minutiae are located at the intersection of the edge of the furrows. The problem of fingerprint recognition is a complex process, even in laboratory conditions; therefore, if used as a system to control access to the mobile devices, it should be insensitive to certain natural changes or damages in physical structure of fingerprints, which can include: incomplete fingerprint, fingerprint parts which can be injured or burned, blurred, partly unreadable or rotation. In order to detect the most sensitive to damage areas, we use neural network with selective attention technique [7]. This type of

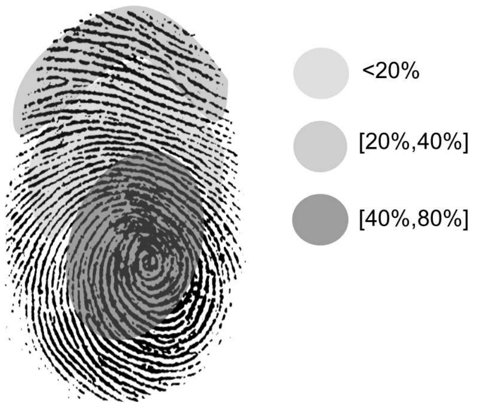

Figure 5. Mask of fingerprint's areas vulnerable to damage. (Source: own work)

neural network is more like an analysis done by a human [8]. This allows us to create a mask of areas vulnerable to damage (see Figure 5).

We created 15 different masks, broken down by the type of fingerprints core also known as fingerprint patterns (arch, whorl and loop) and the type of finger (thumb, index finger, middle finger, ring finger, small finger). Basing on this mask we created a filter, which we use to compare fingerprints where specific minutiae are weighted in the decision process and their score is based on the location on the fingerprints.

V. Comparison of fingerprints

Minutiae image is divided into segments, each segment is corresponding minutiaes group is described by parameters (x, y, nom), where x and y are the coordinates, and nom determines the number of minutiae in the group. Additionally, one implementation uses an additional parameter specifying the probabilities of damage in a given segment, which is estimated by a neural network, based on the distribution of areas rejected by the mask described by the formula. Current algorithm implementation searches small groups of minutiae that that contain up to 5 minutiae (see Figure 6). Then, based on the neighboring groups (max 4) creates a new large group (see Figure 7). For each, the orientation parameters and the number of characteristic points are recalculated. The last step is to create a matrix of Euclidean distances between the largest groups.

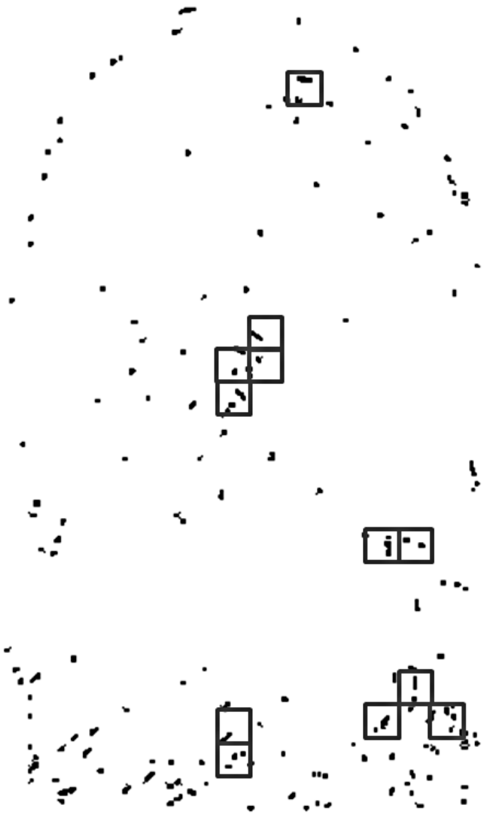

Figure 6. Fingerprint devided into segments. (Source: own work)

Table I
The result of experiment using FVC2004 database

	FAR	FRR
MAG	0.82%	0.65%
EMM	1.23%	1.15%
PBTA	0.15%	1.73%
MGM64	6.60%	0.54%
MGM32	3.23%	0.32%
MGM32_SA	0.38%	0.09%

When comparing the use of two parameters: dx - the distance defining the difference between groups in the pattern and tested fingerprint, px - the threshold of damage occurrence probability (determined by whether the group is under consideration in the analysis), we decide which groups should be compered and we set the priority for them. After that we do the comparison of the groups, which are divided according to the priority, that is defined by the number of minutiae in the group and selective attention (SA) algorithms, which are based on probabilities of damage in a group segment. This provides quick verification of whether the analyzed fingerprint is consistent with the pattern.

VI. The quality of the algorithms

First test was done using FVC2004 [12] fingerprint databases. For each of four databases, a total of 120 fingers and 12 impressions per finger (1440 impressions) were gathered. Unfortunately, most of the publicly available databases of fingerprints do not include the problem of physical damage, so additionally small damage such as cuts and burns has been generated on each sample. In most cases artificially applied damages cover 5-20% of the fingerprint. For 10% of the samples they cover approximately 50% of the area to simulate severe damage.

Most algorithms cannot process fingerprints with severe

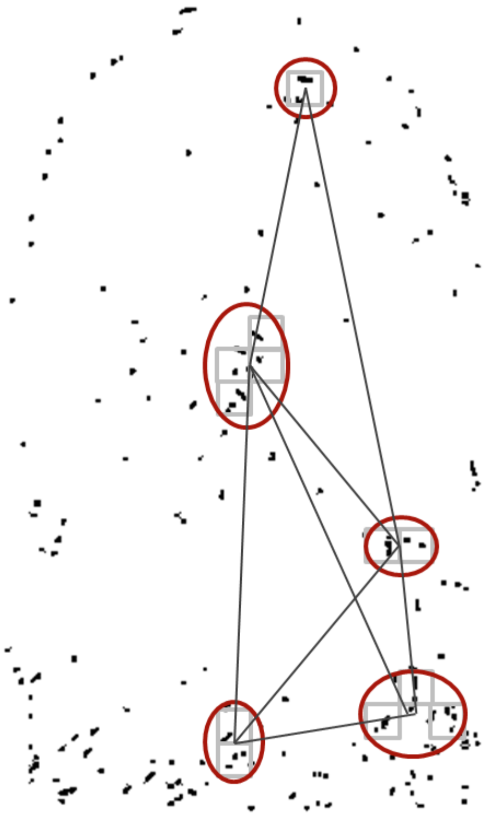

Figure 7. Detecting relations between minutiaes groups. (Source: own work)

physical damage correctly. Also, the proposed one has proven to have a very dangerous level of False Acceptation Rate. After applying the selective attention algorithm, fingerprint recognition algorithm improved its performance and reliability. The proposed algorithm has been developed in such a way, that it uses the property of a damage map, so its results have improved the most.

VII. CLASSIFICATION AND DATA MANAGMENT USED IN THE ALGORITHM

The developed algorithm is based on minutiae groups, where each group is basically represented by the coordinates - x, y and the number of minutiae - nom contained in the group. Group covers an area equal to 2.5 the width of the furrow and its coordinates are in the middle of the square which is boundaring this area. Number of minutiae in the group describes its priority. Additionally, a stored parameter defines the probability of damage - p_d in the area represented by the group. In conclusion the group is defined as follows:

$$M_{group} : \{x, y, nom, p_d\} \tag{7}$$

Based on these data, a matrix of Euclidean distances between the groups is created. Data on the characteristic point is limited to its weight (nom) and the probability of damage p_d. Finally we obtain:

$$M_{group}(I) : \{nom_I, (p_d)_I)\} \tag{8}$$

$$M_{group}(I, J) : dist(M_{group}(I), M_{group}(J)) \tag{9}$$

where $dist(M_{group}(I), M_{group}(J))$ is Euclidean distances between the group I and J. Data stored for analysis to prevent reproduction of the original fingerprint image. Additional storage parameters to estimate the damage allow us to better match fingerprints in the event of damage.

Table II
THE RESULT OF EXPERIMENT ON SAMSUNG GALAXY SII

	FAR	FRR	Average time to decision in ms
MAG	0.80%	0.63%	138
EMM	1.15%	1.20%	127
PBTA	0.25%	1.70%	130
MGM64	6.75%	0.55%	127
MGM32	3.43%	0.42%	128
MGM32_SA	0.43%	0.18%	132

Table III
THE RESULT OF EXPERIMENT ON HTC WIDEFIRE S

	FAR	FRR	Average time to decision in ms
MAG	0.80%	0.63%	225
EMM	1.15%	1.20%	220
PBTA	0.25%	1.70%	232
MGM64	6.75%	0.55%	215
MGM32	3.43%	0.42%	228
MGM32_SA	0.43%	0.18%	225

VIII. THE EXPERIMENT

The tests were conducted on two devices: Samsung Galaxy SII (see Table II) and HTC Widefire S (see Table III). For test authors used real fingerprints. Due to the nature of work, we use real fingerprints. Each user was exposed to frequent damage of fingerprints, like cuts and burns presented on Figure 1. All algorithms were compared using 112 different fingerprints and each had 10 samples.

In the test, we use not optimal algorithm, because first implementation was done in Android SDK, not in NDK, which allow developer to use more code optimizations, but need much more time to implement it for specific devices. The implementation in Android NDK is planned in future work. This implementation should also allow us to create a dynamic mask of the damaged sectors and the most vulnerable to damage area of the fingerprint for a specific user and not only use a general mask, which is hardcoded in our current implementation to reduce memory usage. Our algorithm can be used on mobile devices because its decision time is very similar to other algorithms; however, other parameters are much better.

ISBN: 978-1-61208-226-4

IX. Conclusion

In this paper, we proposed a new step for fingerprint-matching approach, which is based on selective attention. Inserted mask can be hardcoded in the algorithm or generated in real time by neural network, but it required devices with better performance. With a hardcoded mask we can provide significant improvement in algorithms we with a low performance cost. The proposed solution can be used by everyone who is exposed to damage of fingerprints. The system can also be applied to protect access to important data or premises, which are very important for mobile device users.

Acknowledgment

Experiment is co-financed by the European Union under the European Social Fund.

References

[1] A.M. Bazen and S.H Gerez, "Fingerprint Matching by Thin-plate Spline Modelling of Elastic Deformations.", in Pattern recognition, vol. 36 (8), 2003, pp. 1859-1867

[2] G. Bebis , T. Deaconu, and M. Georgiopoulos, "Fingerprint Identification Using Delaunay Triangulation", in Proc. IEEE International Conference on Intelligence, Information, and Systems, 1999, pp. 452-459

[3] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Classification by Directional Image Partitioning", in IEEE Transactions on Pattern Analysis Machine Intelligence, vol.21, no.5, 1999 pp. 402-421

[4] S. Chikkerur, V. Govindaraju, and E. N. Cartwright, "K-plet and coupled bfs: A graph based fingerprint representation and matching algorithm.", in LNCS vol. 3832, 2006, pp. 309315

[5] C. Grzeszyk, "Forensic fingerprint examination marks." (in Polish), Wydawnictwo Centrum Szkolenia Policji, Legionowo 1992

[6] Y. He, Z. Ou, "Fingerprint matching algorithm based on local minutiae adjacency graph", in Journal of Harbin Institute of Technology 10/05, 2005, pp. 95-103

[7] M. Huk, "Sigma-if neural network as the use of selective attention technique in classification and knowledge discovery problems solving", in Annales Universitatis Mariae Curie-Skodowska. AI Informatica. vol. 5, 2006, pp. 121-131

[8] M. Huk, "Learning Distributed Selective Attention Strategies with the Sigma-if Neural Network", in Advances in computer science and IT / ed. by D. M. Akbar Hussain. Vukovar : In-Teh, 2009. pp. 209-232

[9] A. Hicklin, C. Watson, and B. Ulery, "How many people have fingerprints that are hard to match", NIST Interagency Report 7271 ,2005

[10] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation" in IEEE Transactions on Pattern Analysis and Machine Intelligence 20, 1998, pp 777-789.

[11] A. K. Jain, A. Ross, and K. Nandakumar, "Introducing to biometrics", Spinger 2011

[12] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition, 2nd Edition", Springer 2009

[13] S. Pankanti, S. Prabhakar, and A.K. Jain, "On the individuality of fingerprints", in Proceedings of Computer Vision and Pattern Recognition (CVPR), 2001, pp. 805-812

[14] G. Parziale and A. Niel "A fingerprint matching using minutiae triangulation.", In: Proc. of International Conference on Biometric Authentication (ICBA) , Springer, vol. 3072, 2004, pp. 241-248

[15] N. K. Ratha and V. Govindaraju, "Advances in Biometrics: Sensors, Algorithms and Systems", Springer 2007

[16] A. Ross, S.C. Dass, and A.K. Jain, "A deformable model for fingerprint matching", in Pattern Recognition 38(1), 2005, pp. 95103

[17] A. Ross, K. Nandakumar, and A.K. Jain, "Handbook of Multibiometrics (International Series on Biometrics)", Springer 2011

[18] M. Szczepanik and R. Szewczyk, "Fingerprint identification algorithm (in Polish)". KNS, vol. 1, 2008, pp. 131 -136

[19] J.L. Wayman, A.K. Jain , D. Maltoni, and D. Maio, "Biometric Systems. Technology, Design and Performance Evaluation, 1st Edition.", Springer 2005