Volume 51, Number 4, 2010

ACTA TECHNICA NAPOCENSIS

Electronics and Telecommunications

A MULTIMODAL AUTHENTICATION SYSTEM

Marius DAVID, Monica BORDA

Faculty of Electronics, Telecommunications and Information Technology, Cluj - Napoca
Technical University of Cluj-Napoca, 26-28 Barițiu Street, 400027,
Email: davidmarius@email.ro

Abstract: In this paper, we propose a secure fingerprint matching technique, which was combined with conventional authentication methods to achieve more secure communications. We describe in detail all the steps needed for preprocessing and fingerprint image classification. Also an algorithm based on the local structure of the minutiae is presented to match the fingerprints.

Keywords: *Fingerprint, identification, authentication, normalization, filtering, binarization, skeletonization, fingerprint matching unimodal biometric system, multimodal biometric system*

I. INTRODUCTION

Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition. Along with the rapid growing of this emerging technology, the system performance, such as accuracy and speed, is continuously improved. At the same time, the security of the biometric system itself is becoming more and more important.

Automatic fingerprint recognition has become a widely used technology in biometrics applications. Despite a history of a thousand years during witch fingerprints have been used as individual's proof of identity an decades of research on automated systems, reliable fully automatic fingerprint recognition is still an challenging research problem.

Since a fingerprint data is in the order of several kilobytes, it provides the security of having a long password without the overhead of remembering that information. However, unlike a password system, in which an exact match is expected for authentication of an individual, a fingerprint recognition system can only provide the individual's identity information with a certain confidence level. Thus, some kind of distortion tolerant mechanism is required witch can reduce the security strength of the system.. Before we create multimodal access control system we must answer the question "how secure is the fingerprint based system compared to the password or PIN based systems ?"

II. THE PROCESS OF MATCHING

A fingerprint is believed to be unique to each person. Even the fingerprints of identical twins are different. The pattern is quite stable trough out our lifetime, in case of a cut; the same pattern will grow back. The features of a fingerprint depend on the nerve growth in the skin's surface. This growth is determined by genetic factors and environmental factors such as nutrients, oxygen levels and blood flow which are unique for every individual. [1]

Fingerprints are one of the most full-grown biometric technologies and are used as proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigation.

The performance of matching techniques relies partly on the quality of the input fingerprint. In practice, due to skin conditions, sensor noise, incorrect finger pressure and bad quality fingers like from elderly people and manual workers, a significant percentage of fingerprint images are of poor quality. This makes it quite difficult to compare fingerprints.

Fingerprints are unique; there are no two individuals that have exactly the same pattern. In principle, every finger is suitable to give prints for authentication purposes. However, there are differences between the ten fingers. There is no clear evidence as to which specific finger should be used for identification. The thumb provides a bigger surface area but there is not much association of the thumb with criminality. Forefingers have been typically used in civilian applications. In most cases one can assume that the index finger obtains the best performance. Since the majority of the people are right handed, the best choice would be to take the right hand index finger. [2, 3]

The matching of fingerprints has been studied a lot, resulting in multiple approaches. One of these approaches is minutiae matching. It is the most well known and often used method that makes use of small details in the fingerprint, called minutiae, as ridge endings and split points. Each minutia has its own information, like the angle and position.

Extracting this information is one of the steps of the minutiae matching approach, matching these extracted minutiae is another problem. This matching of minutiae can be seen as a point matching problem. A suitable algorithm to solve this problem is the Hough transform-based algorithm.

It calculates the optimal transformation for matching minutiae. If there exists a matching fingerprint in the database, the template with the most matching minutiae is probably the same as the input.

Between the extraction of minutiae points and the matching, there is often a post-processing step to filter out false minutiae, caused by scars, sweat, and dirt or even by the preprocessing step. In the end, using the minutiae can lead to a

Manuscript received September 12, 2010; revised December 21, 2010

unique match of fingerprints.

The procedure described above can be extended with one important time saving step, namely classification. Classification is used in cases where the database containing fingerprints is so large that matching a fingerprint with all the images is too time-consuming. Fingerprints can be categorized by their patterns. The classification is based on the following patterns: loops, whorls and arches. In this way an input fingerprint does not have to be matched with all the fingerprints in the database, but only a part of it.

The steps to take for the whole process of matching an input fingerprint with one of the templates from the database, is depicted in figure 1. The assumption is made that the templates in the database have already gone through this process and so only the input fingerprint has to be prepared for matching.

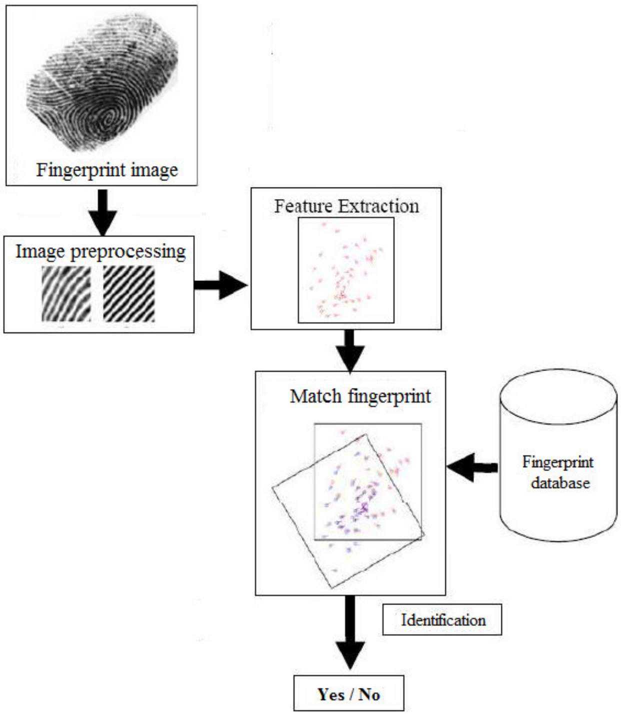


Figure 1. The process of matching an input fingerprint with a template from the database

The first phase of the fingerprint verification process is the fingerprint enrollment phase. Is very important to know the size and quality of the image that the fingerprint sensor in use takes, so we can have an idea on how we are going to preprocess it. From this image, minutiae are extracted and stored in a data base. This process repeats, resulting in the generation of a 'live template'.

The measurement of our success is going to include some steps to achieve our goal:

- An image is going to be taken of the same fingerprint to cover various aspects of the image. (Position, dryness, humidity, dust, brightness, darkness, etc.)
- There is going to be a limited number of person's fingerprints in a database to be recognized; if a person enters its finger and its fingerprint is not in the database, it has to be rejected.
- A threshold is going to be set for the acceptance or rejection of a specific fingerprint.

II.1. PREPROCESSING

After a fingerprint image is captured it contains a lot of redundant information. Problems with scars, too dry or too moist fingers, or incorrect pressure must also be overcome to get an acceptable image. Therefore, preprocessing, consisting of enhancement and segmentation is applied to the image [4].

It is widely acknowledged that at least two to five percent of target population has fingerprints of poor quality. These fingerprints that cannot be reliably processed using automatic image processing methods.

In the literature there are several methods to improve the quality of an image and make it ready for matching details.

The steps that are present in almost every process are:

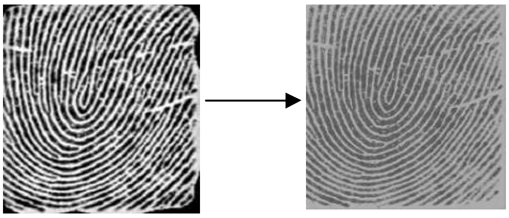
- normalization,
- filtering,
- binarization,
- skeletonization

A. Normalization

Normalization is a good first step for improving image quality. To normalize an image is to spread the gray scale in a way that it is spread evenly and fill all available values instead of just a part of the available gray scale, see figure 2. The normal way to plot the distribution of pixels with a certain amount of gray (the intensity) is via a histogram. To be able to normalize an image, the area which is to normalize within, has to be known. Thus it is necessary to find the highest and the lowest pixel value of the current image. Every pixel is then evenly spread out along this scale. Equation (1) represents the normalization process.

$$I_{norm}(x,y) = \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}} \times M \tag{1}$$

In equation (1) I is the intensity (gray level) of the image. $\mathbf{I}_{\min}$ is the lowest pixel value found in the image, $\boldsymbol{I_{MAX}}$ is the highest one found. M represents the new maximum value of the scale, mostly $M = 255$, resulting in 256 different gray levels, including black (0) and white (255). $\boldsymbol{I_{norm}}(x, y)$ is the normalized value of the pixel with coordinates x and y in the original image $I(x,y)$. When images have been normalized it is much easier to compare and determine quality since the spread now has the same scale. Without the normalization it would not be possible to use a global method for comparing quality.



Raw image from sensor *Normalized image*

Figure 2. The normalization step

B. Filtering

It is important to filter out image noise coming from finger consistency and sensor noise. For that purpose the orientation of the ridges can be determined so that it is able to filter the image exactly in the direction of the ridges. In figure 3 an orientation field overlaid on a fingerprint is shown.

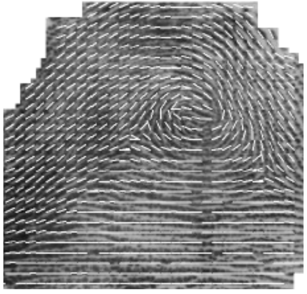
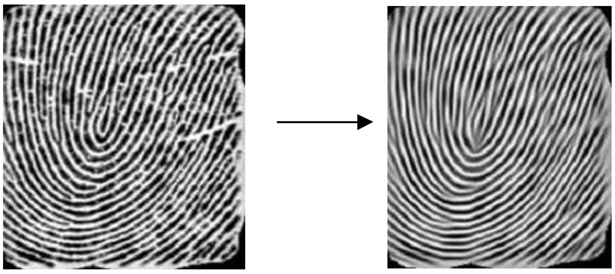


Figure 3. An orientation field overlaid on a fingerprint

By this filter method the ridge noise is greatly reduced without affecting the ridge structure itself, see figure 4. One approach to ridge orientation estimation relies on the local image gradient. A gray scale gradient is a vector whose orientation indicates the direction of the steepest change in the gray values and whose magnitude depend upon the amount of change of the gray values in the direction of the gradient. The local orientation in a block can be determined from the pixel gradient orientations of the block. [5,6]



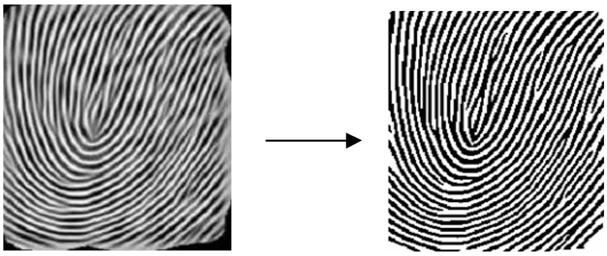
Normalized image *directionally filtered image*

Figure 4. The filtering step (orientation field filters)

C. Binarization

Binarization can be seen as the separation of the object and background. It turns a gray scale picture into a binary picture. A binary picture has only two different values. The values 0 and 1 are represented by the colors black and white, respectively. Refer to figure 5 for a binarized image. To perform binarization on an image, a threshold value in the gray scale image is picked. Everything darker (lower in value) than this threshold value is converted to black and everything lighter (higher in value) is converted to white. The difficulty with binarization lies in finding the right threshold value to be able to remove unimportant information and enhance the important one. It is impossible to find a working global threshold value that can be used on every image. The variations can be too large in these types of fingerprint images that the background in one image can be darker than the print in another image. Therefore, algorithms to find the optimal value must be applied separate on each image to get a functional binarization. There are a number of algorithms to perform this; the simplest one uses the mean value or the median of the pixel values in the image. This algorithm is based on global thresholds.

What often are used nowadays are local thresholds. The image is separated into smaller parts and threshold values are then calculated for each of these parts. This enables adjustments that are not possible with global calculations.



Directionally filtered image *Binarized image*

Figure 5: The binarization step

D. Skeleton modeling

One way to make a skeleton is with thinning algorithms. The technique takes a binary image of a fingerprint and makes the ridges that appear in the print just one pixel wide without changing the overall pattern and leaving gaps in the ridges creating a sort of "skeleton" of the image. See figure 6 for an example of skeletonization. The form ✚ is used as structural element, consisting of five blocks that each present a pixel. The pixel in the center of that element is called the origin. When the structural element overlays the object pixels in its entirety, only the pixels of the origin remain. The others pixels are deleted.

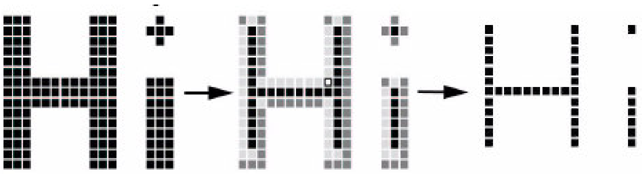
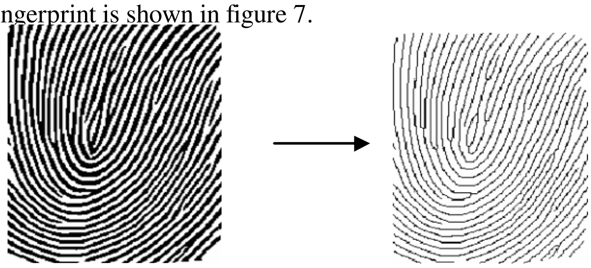


Figure 6: An example of skeletonization

Skeleton modeling makes it easier to find minutiae and removes a lot of redundant data, which would have resulted in longer process time and sometimes different results. [7] There are a lot of different algorithms for skeleton modeling that differ slightly. The result of a skeletonized (or thinned) fingerprint is shown in figure 7.



Binarized image *Skeletonized image*

Figure 7: The skeletonizing step

II.2. CLASSIFICATION

Fingerprints are classified into categories based on information in the global pattern of ridges. A recognition procedure consists in retrieving one or more fingerprints in a large database corresponding to a given fingerprint, whereas a classification procedure consists in assigning a fingerprint to a pre-defined class. In this chapter it is described how this works.

Most automatic systems for fingerprint comparison are based on minutiae matching. Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice only *ridge ending* and *ridge bifurcation* minutiae types are used in fingerprint recognition. Examples of minutiae are shown in figure 8.

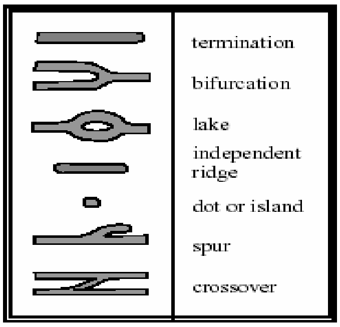


Figure 8. Examples of minutiae

Although a wide variety of classification algorithms has been developed for this problem, a relatively small number of features extracted from fingerprint images have been used by most of the authors. In particular, almost all the methods are based on one or more of the following features: ridge line flow, orientation image, singular points and Gabor filter responses. Ridge line flow is usually represented as a set of curves running parallel to the ridge lines. An orientation image is used in most classification approaches because it contains all the information required for the classification. A Gabor filter is a common directional filter which has both frequency-selective and orientation-selective properties.

II.3 FINGERPRINT MATCHING

This chapter describes how an input fingerprint is compared with one of the template fingerprints, stored in a database.

There are two basic types of fingerprint matching techniques: graph based and minutiae based. For modern embedded fingerprint recognition systems, the minutiae-based matching is popular because, on the one hand, the minutiae of the fingerprint are widely believed the most discriminating and reliable features, and on the other hand, the template size of the biometric information based on minutiae is much smaller and the processing speed is higher than that of graph-based fingerprint matching.

These characteristics are very important for saving memory and energy on the embedded devices. Lots of work has been done for minutiae-based fingerprint matching. Some of them use the local structure of the minutiae to describe the characteristics of the minutiae set. This approach has high processing speed and robustness to rotation and partial prints. However, the local structure usually has less distinct features because it only represents some parts of the whole minutiae set. Prints from different fingers may have quite a few similar local structures by coincidence while prints from the same finger may only have very few similar structures due to the presence of false minutiae and the absence of genuine minutiae. Alignment-based matching algorithms take use of the shape of the ridge connected to minutiae [8]. This might improve the system accuracy. However, this approach results in a larger template size because the associated ridges for each minutia must be saved. Some other researches combine the local and global structures [9]. The local structure is used to find the correspondence of two minutiae sets and increase the reliability of the global matching. The global structure of minutiae reliably determines the uniqueness of a fingerprint.

The approach in [10] is similar to our work. However we propose a definition of the local structure of a minutia, which is proven efficient for low quality input fingerprints and a low accurate minutiae extraction.

A minutiae m is described by the triplet m={x, y, θ}, where x, y indicate the minutiae location coordinates and θ denotes the minutiae orientation, which is the orientation evaluated for the minutiae location from the orientation image obtained during the enhancement process. The minutiae type is not being used during the matching process since minutiae type can be inverted due to enhancement and binarization steps.

Let T and I be the representation of the template and input fingerprint, respectively. Let the minutiae sets of the two fingerprints be given by:

$$T=\{m_1,m_2,...,m_m\} \qquad m_i=\{x_i,y_i,\theta_i\}, i=1..m$$
$$I=\{m_1',m_2',...,m_n'\} \qquad m_j'=\{x_j',y_j',\theta_j'\}, j=1..n$$

A minutia *mj'* in I and a minutia *mi* in *T* are considered to be matched if their spatial and orientation differences are within specified thresholds *ro* and θ*o*. Minutia matching was carried out by using the approach given in [11].

In this approach the minutiae sets are first registered using a derivative of the Hough transform, followed by fingerprint matching using spatial and orientation-based distance computation. The matching algorithm returns a percentage match score, which is then used to take the match-no match decision based on the security criterion.

III. EXPERIMENTAL RESULTS

An Authentec AF-2 CMOS imaging sensor was used to collect fingerprint samples. The sensor has an accuracy of 8 bits/sample. Porting the minutiae extraction processing to the embedded device introduces some extra error due to the time constraints and finite word length limitations [12]. All these embedded device constraints require a robust matching algorithm.

Due to the variations existing within any biometric signal, a biometric signal, a biometric authentication or recognition system cannot give an absolute answer about the individual's identity; instead it provides the individual's identity information with a certain confidence level; this contrary to traditional authentication systems (for example a password system) where the match has to be exact and an absolute "yes" or "no" answer is returned. The biometric signal variations of an individual are usually referred to as intraclass variations; whereas variations between different individuals are called interclass variations.

Generally, the identity of a submitted biometric signals either a genuine type or an impostor type; hence, there are two statistical distributors of similarities scores, which are called genuine distribution and impostor distribution. Each type of input identity has one of two possible results, "accept" or "reject", from a biometric matcher. Consequently, there are four possible outcomes:

- a genuine individual is accepted;
- a genuine individual is rejected;
- an impostor individual is accepted;
- an impostor individual is rejected.

The first and fourth outcomes are correct while the second and third outcomes represent the error situations. The second outcome is referred to as "false reject" and the corresponding error rate is called false reject (FAR); the third outcome is referred to as "false accept" and the corresponding error rate is called false reject rate (FRR).

Our proposed method is based on the local structure of the minutiae. One of the important parameters is the number of neighbors taken as the local structure for each minutia. If the number is too small, which means that the matching condition is quite loose, some un-matched minutiae pairs are very likely to satisfy the matching condition, which may lead to a high FAR (False Accept Rate). On the other hand, if the number is too large, the matching condition becomes too strict. Many matched pairs may fail because the fingerprint image is sometimes uncompleted and the minutiae detection is not very precise. This may result in a high FRR (False Reject Rate). To select the proper number of neighbors taken as local feature, experiments were done for a local structure of 4,5,6 and 7 neighbors. For each case, different marked neighbor pair thresholds were investigated. Since the baseline accuracy needed for modern biometric systems is 1% FRR and 0.01% FAR [13], table 1 presents whether or not the selection can reach this standard. The image set consists of 10 fingerprints per finger from 10 different fingers for a total 100 fingerprint images.

Table 1. Possibility to achieve baseline accuracy for different local structure definition and threshold.

Neighbor Num / TH_A	4	5	6	7
2	No	No	No	No
3	No	Yes	Yes	No
4	—	No	No	No
5	—	—	No	No
6	—	—	—	No

Figure 5 shows the result from two different local structure definitions, which both can achieve the baseline accuracy. The X-axis is the FRR and the Y-axis shows the FAR.

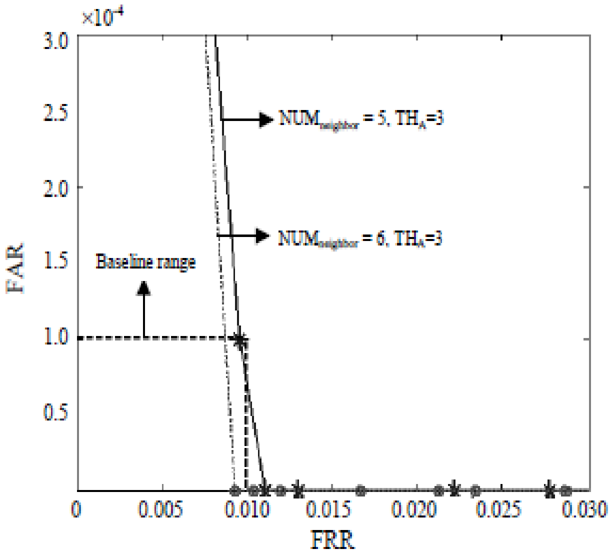


Figure 8. Results from two different local structure definitions

After analyzing the above result, we define the number of neighbors as 6 and the marked neighbor pair threshold THA is set to 3. By doing this, we obtain a FRR of 1% and a FAR of less than 0.1 FAR.

IV. SOFTWARE IMPLEMENTATION

Besides studying the most important fingerprint identification algorithms, software algorithm implementation was done in Visual Basic 6.0. The application meets all requirements of the initial goal.

V. CONCLUSIONS AND FEATURE WORK

In this paper, we present a multimodal system that combines biometric methods (fingerprint identification) and classical methods (password) used to control the access to a computer, directory or folder. Such data security is obviously higher than that obtained using conventional methods or unimodal biometric systems.

In the multimodal system implemented classical control methods operate only at the beginning, when we want to open a program or file. After that minutiae-based biometric matching algorithm is used for fingerprint identification.

The most significant disadvantages of the biometric recognition system is that they cannot be easily recalled. For example, if one of the fingers is used, once it is compromised, it never can be used again since it is almost impossible that a fingerprint can be changed, which means it is compromised forever. Moreover, since one person only has a limited number of fingers, different applications might use the same fingerprint. A person's biometric stolen from one application could also be used in some other applications [14]. By properly defining the local structure of the minutiae, we achieve 1% FRR and less than 0.01% FAR.

In the future we are developing a multimodal system obtained by using other biometric methods such as iris identification in combination with fingerprint identification method and other classical methods used to control the access.

REFERENCES

[1] S. Pankant, S. Prabhakar, A.K. Jain - *On the Individuality of Fingerprints*, IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 805-812, Hawaii, December 11-13, 2001

[2] Qinzi Zhang, Kai Huang, Hong Yan - *Fingerprint Classification Based on Extraction and Analysis of Singularities and Pseudoridges*, in Conferences in Research and Paractice in Information Technology, Vol. 11, 2002

[3] http://www.bromba.com/faq/fpfaqe.htm#beweisen - shows generalities about fingerprints and sensors designed for fingerprint reading;

[4] Prabhakar, S., Pankanti, S., and Jain, A. K., Biometric Recognition: Security and Privacy Concerns*,* IEEE Security and Privacy Magazine*,* Vol. 1, No. 2, pp. 33-42, March-April 2003.

[5] Anil K. Jain, Sharath Pankanti - *Automated Fingerprint Identification and Imaging Systems,* in Advances in Fingerprint Technolofy. Elsevier, New York, second edition, 2001

[6] http://www.bromba.com/technole.htm - presents details about the fingerprint preprocessing step;

[7] Ankie van der Zanden - *Matching Fingerprints-* Business Mathematics and Informatics Free University, Amsterdam, *Delft, July 2005*

[8] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar - *Handbook of Fingerprint Recognition*, Springer, pp 88, 2003

[9] Jiang, X., Yau, W., Fingerprint minutiae matching based on the local and global structures, Proceedings 15th International Conference on Pattern Recognition. ICPR-2000. IEEE Comput. Soc. Part, vol.2, 2000, pp.1038-1041 vol.2. Los Alamitos, CA, USA.

[10] Chaoqiang Liu, Tao Xia, Hui Li – A hierarchical Hough Transform for Fingerprint matching, Centre for Wavelets, Aproximation and Information processing, pp 373-379, National University of Singapore 2004

[11] David Marius, Borda Monica - Multimodal access control systems which combines classical access control methods with biometric methods, ISETC 2010 9th International Symposium on Electronics and Telecomunications, Timisoara, November 11-12, 2010;

[12] Yang, S., Sakiyama, K. and Verbauwhede, I., A Secure and Efficient Fingerprint Verification System for Embedded Systems, 37th Asilomar Conference on Signal, Systems, and Computers, Nov. 2003, Pacific Grove, CA.

[13] Anderson, R.J., Security Engineering, A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2007.

[14] Prabhakar, S., Pankanti, S., and Jain, A. K., Biometric Recognition: Security and Privacy Concerns, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[8] Jain, A., Lin, H. and Bolle, R., On-line fingerprint verification, IEEE Transactions on Pattern Analysis & Machine Intelligence, vol.19, no.4, April 2007, pp.302-14. Publisher: IEEE Comput. Soc, USA

.