ISSN:0975-9646

Biometrics Hybrid System Based Verification

Mahesh Naidu K [#1], Prof Govindarajulu P[*2]

[#1]*Ph.D Research Scholar,Dept of Computer Science,*
SVU College of CM&CS, S.V. University, Tirupati, Andhra Pradesh, India
[*2]*Dept of Computer Science,*
SVU College of CM&CS, S.V. University, Tirupati, Andhra Pradesh, India

Abstract— **Biometric identification systems identify people by personal traits such as the characteristics of their faces, fingerprints, palm prints, veins, eyes or DNA. Since the difficulty and accuracy of biometric identification varies depending on the person and trait, as well as the measuring environment, multi-modal identification or biometrics hybrid system that measures more than one trait is becoming popular. If one measurement fails to provide ample information, the other serves as a backup to support proper identification and decision making. Hybrid biometrics with multi-modal identification also helps prevent impersonation since faking more than one trait is quite difficult. A hybrid biometric system, which is combined with a touch-panel-based fingerprint module and face-identification module are proposed after considering various biometric options for biometrics hybrid system. For fingerprint identification, a user only needs to touch the device screen. At the same time, face images of the user are acquired and enrolled in the face-identification module. The touch-based device can provide high-accuracy authentication, it will also greatly reduce the user's burden during finger pattern acquisition. A simple face-alignment and identification algorithm based on information around the eyes and mouth is used. A performance evaluation of the proposed hybrid biometric system demonstrated that the system can provide biometric authentication and verification with higher reliability and user convenience**.

I. INTRODUCTION

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [1]. Biometric identifiers are often categorized as physiological versus behavioural characteristics [2]. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics [3]. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number[2]. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods [10].

.

II. BIOMETRICS – AS A VERIFICATION SYSTEM

Biometric verification refers to an automatic verification of a person based on some specific biometric features derived from his/her physiological and/or behavioural characteristics. A biometric verification system has more capability to reliably distinguish between an authorized person and an imposter than the traditional systems that use a card or a password. In biometrics, a person could be recognized based on who he/she is rather than what he/she has (ID card) or what he/she knows (password). A biometrics system is a recognition system which operates by acquiring biometric data from an individual, extracting feature sets and comparing it with the template set in the database. Depending upon the application context, the identity of a person can be resolved in two ways: verification and identification. In the former, a person to be identified submits a claim; which is either accepted or rejected. In the latter, a person is identified without a person claiming to be identified.

Biometric technology reliability is increasing all the time, it is constantly being improved. It is reliable already, but the potential for error is consistently being minimized by advances in technology that allow it to utilize much more biometric data to make a positive match. Some of the popular biometrics that is in use in range of environments was considered for integration with proposed solution.

III. BIOMETRICS CURRENTLY IN USE ACROSS A RANGE OF ENVIRONMENTS

A. Fingerprint

Fingerprint is the pattern of ridges and valleys on the tip of a finger and is used for personal verification of people. Fingerprint based recognition method because of its relatively outstanding features of universality, permanence, uniqueness, accuracy and low cost has made it most popular and a reliable technique and is currently the leading biometric technology. There is archaeological evidence that Assyrians and Chinese ancient civilizations have used fingerprints as a form of identification since 7000 to 6000 BC [4]. Current fingerprint recognition techniques can be broadly classified as Minutiae-based, Ridge feature-based, Correlation-based and Gradient based. Most automatic fingerprint verification and identification systems employ techniques based on minutiae points.

Some of the advantages of Fingerprint biometrics are: a. Very high accuracy. b. One of the most economical biometrics c. One of the most developed biometrics d. Easy to use. e. Small storage space required for the biometric template f. It is standardized.

B. Face

Face recognition is an important alternative for selecting and developing an optimal biometric system. Its advantage is that it does not require physical contact with an image capture device (camera). A face identification system does not require any advanced hardware, as it can be used with existing image capture devices (webcams, security cameras etc.). Thus, facial recognition can be considered as a serious alternative in the development of biometric or hybrid biometric systems.

A number of algorithms have been proposed for face recognition. Such algorithms can be divided into two categories: geometric feature-based and appearance-based.

C. Iris

The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. Identity recognition is impacted significantly when scanning images aren't perfect due to lighting, motion, blur, or even physical problems like occluded irises, etc. Some of the other disadvantages of Iris biometrics are: intrusive, a lot of memory for the data to be stored, more expensive.

D. Other Biometrics

Other popular biometrics that are reliable but expensive: Palmprint, DNA and Retinal Scanning. Biometrics such as Voice and Signature are less expensive but not much dependable. In voice recognition sound sensations of a person is measured and compared to an existing dataset [5]. An illness such as a cold can change a person's voice; this will make absolute identification difficult or impossible. A person's voice can be easily recorded and used for unauthorized access or verification. Signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification.

IV. BIOMETRICS HYBRID SOLUTION – VERIFICATION SYSTEM

Methodology

The hybrid biometrics approach is especially important for identification and verification in one-to-many systems. In general, biometric identification systems are very convenient to use as they do not require any additional security information (smart cards, passwords etc.). However, using one-to-many matching routines with only one biometric method can result in a higher false acceptance probability, which may become unacceptable for applications with large databases. Using face identification as an additional biometric method can dramatically decrease this effect. This hybrid biometric approach also helps in situations where a certain biometric feature is not optimal for certain groups of users. For example, people who do labor intensive jobs with their hands may have rough fingerprints; this can increase the false rejection rate if fingerprint identification alone is used.

Fingerprint – Processing

Fingerprint processing has three primary functions: enrollment, searching and verification. Amongst these functions, enrollment which captures fingerprint image from the sensor plays an important role. A reason is that the way people put their fingerprints on a mirror to scan can affect the result in the searching and verifying process. With respect to verification function, there are several techniques to match fingerprints such as correlation-based matching, minutiae-based matching, ridge feature-based matching and minutiae-based algorithm. However, the most popular algorithm is minutiae based matching algorithm due to its efficiency and accuracy.

A. Minutiae features

Minutiae are major features of a fingerprint, using which comparisons of one print with another can be made. The major minutiae features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

B. Fingerprint Enrollment

A fingerprint sensor/scanner is an electronic device, it is used to capture digital image of the fingerprint pattern. The captured image is called a live scan, this is digitally processed to create a biometric template which is stored and used for matching. Biometric template is a collection of extracted features from the fingerprint.

Many fingerprint sensor technology types have been developed, some of the well-known types are: Optical, Ultrasonic, Capacitance. Optical fingerprint scanners are the oldest method of capturing and comparing fingerprints. As the name suggests, this technique relies on capturing an optical image, essentially a photograph, and using algorithms to detect unique patterns on the surface, such as ridges or unique marks, by analyzing the lightest and darkest areas of the image [12]. Ultrasonic and Capacitance based scanners are also in use, popularly used in smartphones. The images captured using Ultrasonic are of 3D nature and even more secure than capacitance sensors. But they are expensive and more required in situations where scope for prosthetics use is detected to gain verification. However, unlike capacitive sensors, optical sensor technology is not susceptible to electrostatic discharge damage. Optical technology based scanners are economical, more evolved and suitable to meet the needs for this solution (Fig 1).

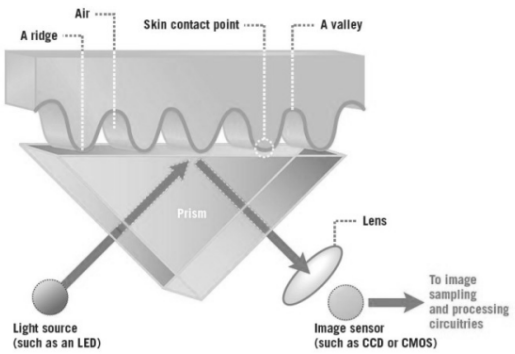

Fig 1. Optical Scanner – Image Capture Flow

Fingerprint thus scanned and extracted are enrolled into database as biometric templates. These biometric templates will build up as searchable database over period of time as candidates are enrolled into local and central databases as needed. The shape of the fingerprint is generally used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the fingerprint, and the presence of the core and the delta. The algorithm uses minutiae, the specific points like ridges ending, bifurcation. Only the position and direction of these features are stored in the image for further comparison.

During minutiae extraction, typically each detected minutiae m_i is described by four parameters:

$$m_i = (x_i , y_i \theta_i , t_i)$$

where:

x_i , y_i – are coordinates of the minutiae point,
θ_i – is minutiae direction typically obtained from l ocal ridge orientation,
t_i – is type of the minutiae point (ridge ending or ridge bifurcation) [15]

The position of the minutiae point is at the tip of the ridge or the valley and the direction is computed to the X-axis (Fig 2)

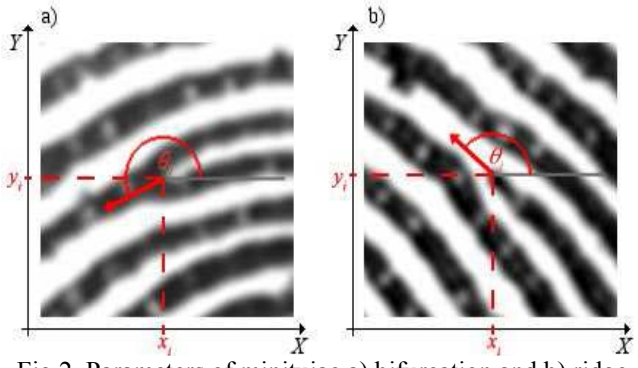

Fig.2. Parameters of minituiae a) bifurcation and b) ridge ending type

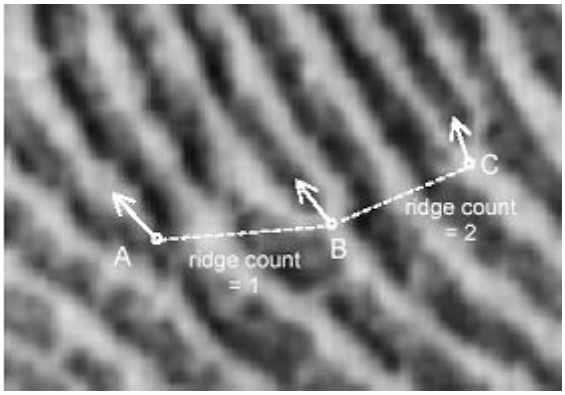

Fig 3. Number of ridges between particular points of the position is counted in the finger print image

The simplest and most used method of feature extraction is based on binarization and ridge thinning. The most commonly used method of minutiae extraction is the *Crossing Number* (*CN*) concept [13, 14]. The binary ridge image needs further processing, before the minutiae features can be extracted. The first step is to binarizate and further to thin the ridges, so that they are single pixel wide. The minutiae points are determined by scanning the local neighbourhood of each pixel in the ridge thinned image, using a 3×3 window (Fig. 4).

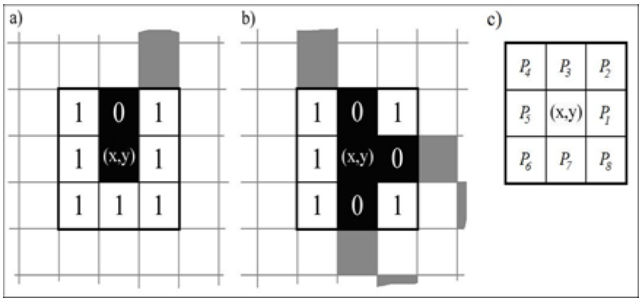

Fig.4. a) Ridge ending and b) bifurcation in c) 3× 3 window.

Using the properties of the *CN* as shown in Table (Fig. 5) the ridge pixel can be then classified as a ridge ending, bifurcation or non-minutiae point [15].

CN	Property
0	Isolated point
1	Ridge ending
2	Continuing ridge
3	Bifurcation
4	Crossing

Fig.5. Properties of the Crossing Number

Fingerprint pattern, minutiae and ridges can also be used in combination to capture and match fingerprints (Fig. 6).

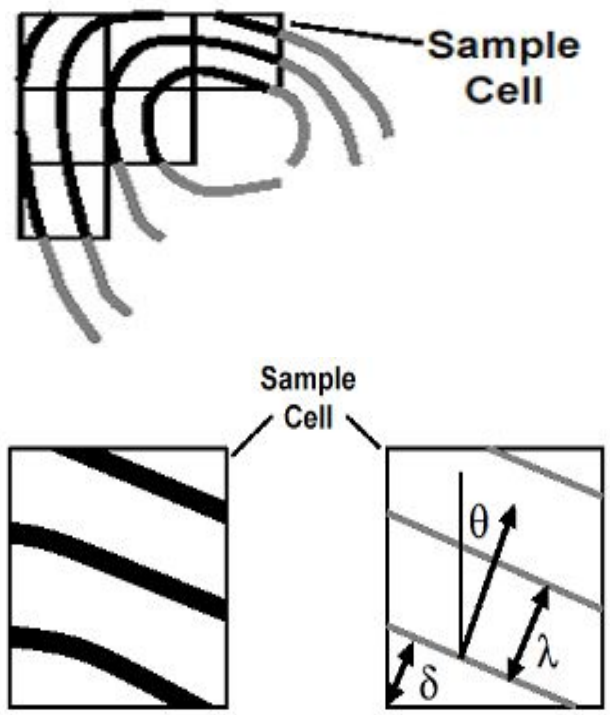

Fig. 6. Pattern matching areas and counting of ridges in specific areas of finger print

Latent Fingerprint images may also be used to do finger print match of a person. This kind of matching is done when there is no need for live scan and immediate search to determine the result. The fingerprint scanned images are extracted and stored to be run against databases as and when needed (Fig. 7).

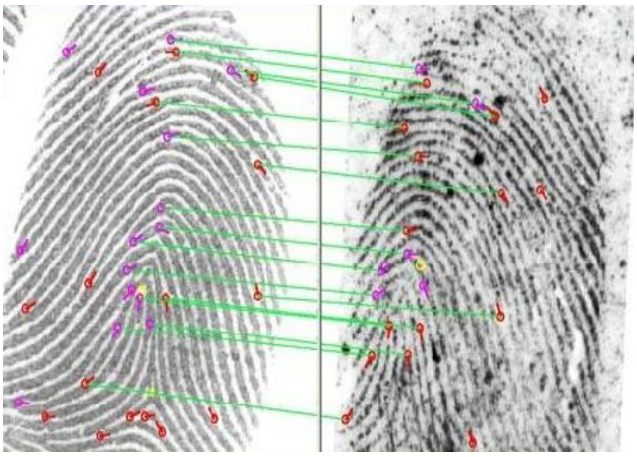

Fig. 7: Matching finger print image with latent finger print using minutiae

C. Fingerprint – Searching and Verification

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for verification and authentication purposes. In order to do this either the original image, extracted as biometric template, must be directly compared with the database of biometric templates with volunteer biometric data or certain features must be compared.

D. Pre-processing

Pre-processing helps in enhancing the quality of an image by filtering and removing unnecessary noises. This process partly removed some noises in an image and helped enhance the edge detection. Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges. By doing so, the thinned ridges of the fingerprint image are marked with a unique identifier, this helps to conduct further operations. After the minutiae extraction step, the false minutiae removal is also necessary.

E. Matching

In a good quality rolled fingerprint image, there are about 70 to 80 minutiae points and in a latent fingerprint the number of minutiae is much less (approximately 20 to 30)[6]. A minutiae-based fingerprint matching system usually returns the number of matched minutiae on both query and reference fingerprints and uses it to generate similarity scores. According to forensic guidelines, when two fingerprints have a minimum of twelve matched minutiae, they are considered to have come from the same finger [7].

Matching algorithm compares two minutiae sets: template $T = \{m_1 , m_2 ,..., m_j \}$ from reference fingerprint and input $I = \{m_1 , m_2 ,..., m_i \}$ from the query and returns similarity score $S(T , I)$.

Face Processing

A. About Face identification

Currently there are many methods of biometric identification - fingerprint, eye iris, retina, voice, face etc. Each of these methods has advantages and disadvantages which must be considered in developing single modal or hybrid biometric systems. Factors that may need to be considered are system reliability, price, flexibility, necessity of physical contact with the scanning device and many others. Selecting a certain biometric identification method or using a hybrid biometric system will help in supporting these often discrepant requirements.

B. Facial Recognition Technology

Similar to fingerprint biometrics, facial recognition technology is extensively used in various systems involving physical access control and secure computer based user accounts. Generally, these systems do extraction of certain features from face images and then perform face matching using those features. A face does not have as many uniquely measurable features as fingerprints and irises, so facial recognition reliability is slightly lower than these other biometric recognition methods. However, it is still suitable for many applications, especially when taking into account user convenience in terms of usage. Facial recognition can also be used together with fingerprint

recognition for developing more reliable and security-critical applications.

In face recognition, problems are caused by different head orientations. Head orientations will not contribute to the errors, if only the information around the eyes is extracted. By doing so, even though some face information may be lost, but to start with we opt for this simpler approach [8]. Firstly, a face image is captured using a web camera. A face is then detected using template matching. The subject's face image is captured by that person coming into the focus area of face panel. Eyes are then automatically localized using a combination of histogram analysis, round mask convolution and a peak searching algorithm. Moments are used to extract the eye information because it is a simple yet powerful extractor. Normalized central moments are invariant to translation, rotation and scaling. A moment of order p+q of an image f_{xy} of N by N pixels with respect to a center (x , y) will be obtained. Other features such as eyes and mouth are extracted based on the observation that they are darker than rest of the face. Then, the eye centers are localized using several cost functions which are designed to take advantage of the inherent symmetries associated with face and eye locations.

Hybrid Biometrics Processing

For the recognition performance evaluation of biometrics hybrid system, a False Acceptance Rate (FAR) and a False Rejection Rate (FRR) tests were performed. These two measurements yield another performance measure, namely Total Success Rate (TSR):

TSR = (1- (FAR+FRR / total number of accesses)) * 100% [9]

The system performance was evaluated by Equal Error Rate (EER) where FAR=FRR. Based on Equal Error Rate criteria where FAR=FRR, a threshold value was obtained for face and finger modules in the biometrics hybrid system.

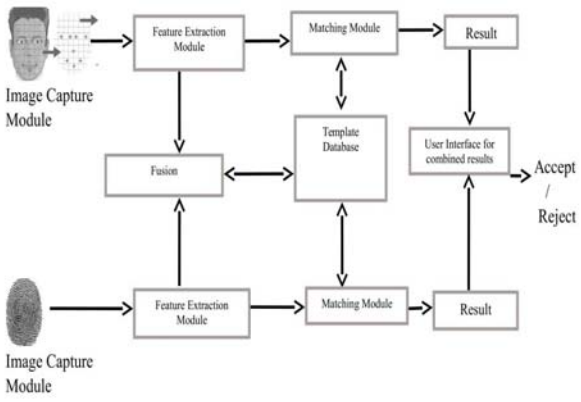

Fig 8: Block Diagram of Face & Finger Biometrics Hybrid System

With the use of multiple modalities or hybrid biometrics fusion techniques were evolved for combining the different modalities. Information integration in a multimodal or biometrics hybrid system can occur in various levels: sensor level, feature level, matching level or decision level. At the sensor or feature level, the feature sets of different biometric modules are combined. Fusion at this level provides the highest flexibility. Fusion at matching level is the most common one, whereby the scores of the classifiers are usually normalized and then combined in a consistent manner. In decision-level fusion, each subsystem determines its own verification and authentication decision and all individual results are combined to a common decision of the fusion system. Decision level fusion will lead to fusion system making final outcome decision. We propose feature level fusion system where in finger and face extracted features are stored in one biometric template in the database. This would make it difficult to independently know the face or finger biometric data location in the database. Depending on the biometric module at use (face, finger or both), extraction and matching will be done only against the required portion of the biometric data in the stored template. Face Matching Module and Finger Matching module will work in parallel without one interfering or affecting the outcome of the other. The results of each module will be displayed to the user, this helps the user in decision making in the event of false acceptance and false rejection situations arising from any one of the modules involved in the biometrics hybrid system. This will greatly arrest the possibility of biometric verification systems results becoming unreliable due to false outcomes. Biometric hybrid systems will increase the user confidence levels in terms of system reliability with very less error rate.

SUMMARY AND CONCLUSIONS

Biometrics Hybrid System technique which combines more than one biometric options in making verification and authentication, may be used to overcome the limitations of mono modal biometrics. The proposed biometrics hybrid system uses Finger and Face biometrics after considering other biometric options by taking into account factors such as ease of use, user convenience, reliability and costing. More user usage and success rate of Biometrics systems in developing countries like India is largely dependent on costing and ease of usage among other factors. Efficiency of proposed Biometrics Hybrid system was evaluated by testing on database after enrolling good number of fingers and face images and subsequently matching modules were run to check the results. It is expected that this system will perform well on large databases as well, it will immensely minimize false results, user is also involved in final decision making in the event of false acceptance and rejection results. This kind of hybrid systems will make it difficult to fake as it involves more than one biometrics as compared to uni-biometric system.

REFERENCES

[1]. Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification".Communications of the ACM, 43(2), p. 91–98.

[2]. Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[3]. "Biometrics for Secure Authentication" (PDF). Retrieved 2012-07-29.

[4]. Maltoni D., Maio D., Jain A. K., AND Prabhakar S., 2003. Handbook of Fingerprint Recognition

[5]. S.Anderson, N. Liberman, E.Bernstein,S. Foster.,E. Cate, & B.Levin Recognition of elderly speech and voice driven document retrieval.IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99, 15-19 March 1999, Phoenix, AZ, USA. IEEE; Signal Process. Soc, 145-8 vol.1, 1999.

[6]. MEHTRE B. M., Fingerprint image analysis for automatic identification, Machine Vision and Applications 6, 2, pp. 124–139, India, 1993.

[7]. GOVINDARAJU V., JEA T., Minutiae-based partial fingerprint recognition, Pattern Recognition, Vol. 38, pp. 1672-1684, USA, 2005.

[8]. Poh, N. and Korczak, J.: "Biometric Authentication System", Res. Rep. LSIIT, ULP, 2001

[9]. J. Haddadnia, M. Ahmadi, and K. Faez, "A hybrid learning RBF neural network for human face recognition with pseudo Zernike moment invariant," in IEEE International Joint Conference On Neural Network (IJCNN ˝02), pp. 11–16, Honolulu,Hawaii, USA, May 2002.

[10]. Weaver, A. C. (2006). "Biometric Authentication". *Computer*, 39 (2), p. 96–97. DOI 10.1109/MC.2006.47

[11]. https://en.wikipedia.org/wiki/Fingerprint_recognition

[12]. http://www.androidauthority.com/how-fingerprint-scanners-work-670934/

[13]. AMENGUAL J., JUAN A., PREZ J., PRAT F., SEZ S., VILAR J., Real-time minutiae extraction in fingerprint images,Proc. of the 6th Int. Conf. on Image Processing and its Applications, pp. 871–875, Ireland, 1997

[14]. BOASHASH B., DERICHE M., KASAEI S., Fingerprint feature extraction using block-direction on reconstructed images,IEEE region TEN Conf., digital signal Processing applications, TENCON pp. 303–306, Australia, 1997

[15]. Łukasz WIĘCŁAW, A minutiae-based matching algorithms in fingerprint recognition systems, Journal of Medical Informatics & Technologies Vol. 13/2009, ISSN 1642-6037