ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Crypto Multimodal Biometric System for the Privacy Protection of User Identification

M. Devi

PG Scholar, CSE, V.S.B.EngineeringCollege,Karur, Tamil Nadu, India[1]

ABSTRACT—Single biometric systems have a range of issues like noisy information, non-universality, spoof attacks and unacceptable error rate. These limitations will besolved by deploying multimodal biometric systems. Multimodal biometric systems utilize two or additional individual modalities, like face, iris, retina and fingerprint. Multimodal biometric systems increase the recognition accuracy quite uni-modal ways. In this paper, twobiometrics, iris and fingerprint are used as multi-biometrics and show using this biometrics has sensible result with high accuracy. For fusion, decision level is employedand every biometric results weighted for participate in final decision. Fuzzy logicis employed for the resultof every biometric result combination.

KEYWORDS— Fingerprint recognition, Iris recognition, minutiae extraction and multi-biometric.

I INTRODUCTION

The necessity for reliable user authentication techniques has up amidst of heightened problemsconcerning security and fast progress in networking, communication and quality [1].The widely utilised authentication systems that regulate the entry to computer systems or secured locations are password, however it will be cracked or stolen. For that reason, biometry has turned out to be a practicable choice to traditional identification ways in many application areas [3]. Biometrics, expressed because the science of characteristican individual on the basis of her physiological or activity traits, looksto attain acceptance as a rightful technique for getting an individual's identity [1]. Biometric technologies have established their importance in akind of security, access management and monitoring applications. The technologies are still novel and momentarily evolving [2].

Biometric systems possess various benefits over traditional authentication ways, that is,
1) Biometric information cannot be obtained by direct covert observation,
2) It is tough to share and reproduce,
3) It improves user easiness by changethe requirement to con long and random passwords
4) It safeguards against repudiation by the user.

Besides, biometry imparts identical security level to all or any users not like passwords and is tolerant to brute force attacks [3]. Variety of biometric characteristics are being usedthese days, thatcontains DNA, iris pattern, fingerprint, retina, face, ear, keystroke dynamics, gait, hand geometry, thermo gram etc., [14, 15].Biometric systems that usuallyuseone attribute for recognition (that is., uni modal biometric systems) are influenced by some practicalproblems like noisysensorinformation, non-universality and/or lack of distinctiveness of the biometric attribute, unacceptable error rates, and spoof attacks [4]. A probable improvement, multimodal biometric systems prevail over a number of these problems by strengthening the proof acquired from many sources [5] [6]. Multimodal biometric system employs two or additional individual modalities, namely, fingerprint, face, Iris and to enhancethe popularity accuracy of typical uni-modal ways. With the utilization of multiple biometric modalities, it\'s shown that to decrease error rates, by providing further valuable information to the classifier. Diverse characteristics will beused by one system or separate systems that mayperform on its own and their selectionsis alsointegratedalong [7]. The multimodal-based authentication will aid the system in risingthe protection and effectiveness as compared to uni modal identification, and it would become difficult for an adversary to spoof the system owing to two individual biometrics traits.

In recent times, multimodal biometrics fusion techniques have invited considerable attention because the supplementary information between completely different modalities might enhance the recognition performance. Majority of the works have targetedthe eyeduring thisspace [8-10]. In most cases, they will be classified into three groups: fusion at the feature level, fusion at the match level and fusion at the decision level [6] [11]. Fusion at the feature level includes the incorporation of feature sets concerning multiple modalities. But, fusion at this level is tough to accomplish in real time as a result of the subsequent grounds:

(i) The feature sets of multiple modalities are also mismatched.

(ii) The association between the feature areas of diverse biometric systems is also unknown;

(iii) Concatenating two feature vectors mightcause a feature vector with very high dimensionalityresulting to the curse of dimensionality problem [12].

II.REVIEW OF RELATED RESEARCHES

A realistic and safe approach to incorporate the iris biometric into cryptographic applications has been presented by Feng Hao et al. This approach employed a periodic binary string, called as biometric key that was created from a subject's iris image with the help of auxiliary error- correction data, which does not disclose the key and can be stored in a tamper-resistant token, like a smartcard. The reproduction of the key revolves on two aspects: the iris biometric and the token. The assessment was done by using irissamplesfrom70 different eyes, with10 samples from each eye. This resulted with the genuine iris codes with a 99.5 percent achievement rate, which up shot with140 bits of biometric key which is sufficient for a128-bitAES.A technique presented by B.Chenand V.Chandran , coalesced entropy based feature extraction process with Reed- Solomon error correcting codes which generate deterministic bit-sequences from the output of an iterative one-way transform. The technique was assessed using 3D face data and was proved to generate keys of suitable length for128-bit Advanced Encryption Standard (AES).

III. ENROLLMENT AND VERIFICATION OF UNIMODAL BIOMETRICS

Unimodal biometrics makes use of single source of biometricsfor personal identification. The biometricsthat is taken into consideration is fingerprint biometrics [14]. The biometric system operates in two modes particularly, enrolment and authentication. The features are extracted exploitation singular point detection and minutiae extraction. Singular purpose makes use of core and delta and minutiae extraction is done with ridge endings and ridge bifurcations.

Unimodal biometric systems perform identification based on single source of biometric information. These systems are affected byseveralissues like noisydevicedata, non- universality, lack of individuality, lack of invariant illustration and susceptibleness to circumvention. As a result of these issues, the unimodal biometric systems error rate is kind of high that makes them unacceptable for security applications. A number of these issues are eased by exploitation two or additional unimodal biometrics as multi-biometric systems. The design of a multi-biometric system depends on the sequence through that every biometrics are non inheritable and processed. Generally these architectures are either serial or parallel. Within the serial design, the results of one modality affect the process of the next modality. In parallel style, totally different modalities operate severally and their results are combined with applicable fusion methodology. The proposedsystem of this paper is parallel style. Multi-biometric systems use 5totally differentstrategies for resolution single biometric disadvantages:
Multi-sensor: exploitation two or additional sensors for gettingknowledge from one biometric. (Fingerprint image with two optical and alter sound sensors).

Multi-presentation: many sensors capturing many similar body elements. (Multi fingerprint image from multi finger of 1 person).
Multi-instance: constant device capturing many instances of constantpiece. (Different position face image).
Multi- rule: constantdeviceis employedhowever its input is processed by totally different algorithm and compares the results. Multi-modal: exploitationtotally different sensors for variousbiometrics and fusion the results. (Like fusion iris and fingerprint code as multi-biometrics).

In the registration stage, the fingerprint image was collected exploitation optical fingerprint device. Once fingerprint is non-inheritable, next stage is to pre-process the fingerprint and to extract the feature exploitation minutiae extraction and it hold on within the information. In authentication stage, the fingerprint question is given that undergoes image segmentation, image binarization and image minutia shown in figure1, that either accepts or rejects the user's identity by matching against anexisting fingerprint database.

A. Image Segmentation

The original image is given and therefore the image undergoes image segmentation [13]. The fingerprint enhancement algorithm is image segmentation. Segmentation is that themethod of partitioning a digital image into multiple segments and generally used to find objects and boundaries in image. In segmentation uniquelya locality of Interest (ROI) is beneficial to be recognized for every fingerprint image. The image spacewhile not effective ridges and furrows is 1st discarded since it solely holds background information.

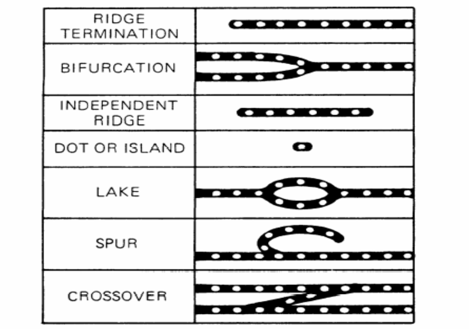


Fig.1. Varietyofminutiatypesonfingerprintimage

B. Image Binarization

After activity segmentation the buzzspace are going to be removed. Within the image binarization, the grey scale image is remodelled into a binary image by computing the mean of every 32-by-32 input block matrix and transferring the constituent value to one if larger than the mean or to zero if smaller. This improves the distinction between the ridges and valleys in an exceedingly fingerprint image and consequently facilitates the extraction of minutiae.

C.Image Minutiae

Most minutiae extraction algorithms treat binary imageswherever the black pixels that represent ridges, and therefore the white pixels that represent valleys. Minutiae-based fingerprint illustration [11] may assist privacy problems since one cannot reconstruct the first image from victimisationsolelyminutiaeinfo. The minutiae area unit comparatively stable and sturdy to contrast; image resolutions and world distortion area unit compared to different fingerprint representations. Two fingerprint match if their minutiae points match. Most minutiae extraction algorithms treat binary imageswherever the black pixels that represent ridges and the white pixels that represent valleys.

IV. FEATURE LEVEL FUSION USING MULTIBIOMETRICS

Multi biometrics is a combination of one or more biometrics, which is taken into consideration in this paper are fingerprint and Iris. Using feature level fusion the features are extracted separately and combined into a single biometric feature set. Instead of storing the original template in the database, secure sketch is generated and stored in the database to provide protection to the template [8], which is achieved by two well-known biometric cryptosystem fuzzy vault and fuzzy commitment. The most important thing in an information fusion system is to determine the type of information that should be consolidated by the fusion module. In feature level fusion which is shown in figure 3, the data or feature set originating from multiple sensors are first pre-processed and features are extracted separately from each sensor, form a feature vector.

These features are then concatenated to makeone new vector. Feature level fusion will use same feature extraction formula or totally different feature extraction formula on different modalities whose feature must be amalgamated. The composite feature vector is then used for classification method. The fingerprint features are extracted using fingerprint minutiae and iris features are extracted using binary strings. The fingerprint image canendure processes of image segmentation, filtering of image usingGabor filter, noise removal and image binarization to extract the fingerprint features templates which are extracted separately are fused with the random key which is given as input using ECC and stored in the database. In the verification stage, the fused single vector is compared with the vector which is stored in the database and key is regenerated. If the key which is not public matches, then the user is valid or it is decided that user is invalid.

V. FINGERPRINTMETHODINTHISRESEARCH

In most identification methods both bifurcations and terminates are considered the same and they are stored as one features. So in these systems each minutia is determined, identified and stored with three parameters X, Y and its tangent angle. In these methods because of storing two decimal number X and Y and since a floating number for tangent have big database and also one pixel coordinate for each minutia is stored, acquiring numbers are changed and in comparing part, the result is changed with the change in minutia position due to rotating in our shifting finger. Usually in the previous methods for Pixel spatial problem, spatial pixel to a threshold is accepted so that this method reduces the accuracy of the system.

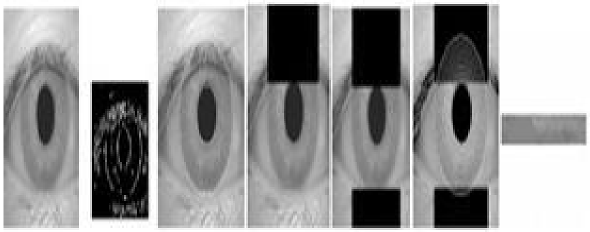
In this research, another method is used and solves the problem via simplest code and hence accuracy result is achieved. With using the proposed method, two 64 bits code is acquired, one for terminates and the other for bifurcations and by fusion them, a 128 bits unique code will be achieved. In identification phase after obtaining128bits code from new fingerprint image, and comparing it against hamming distance with codes in database and finding the code with minimum difference, it is accepted consequently and saves the difference number for one input in our fuzzy logic engine.

VI. IRIS RECOGNITION

Iris is a circular diaphragm which is located between cornea and lens of the human eye. The function of iris is to control the amount of light entering through the pupil. The average diameter of iris is 12mm and pupil size can be10% to 80% of the iris diameter. The iris consists of a number of layers; the lowest layer is the epithelium layer which contains dense colour cells and determines the colour of iris. Stromal layer consists of blood vessels and the external visible surface is a multi-layered iris that consists of two zones and each zone of ten differs in colour. These two zones are divided by the collarets which make a zig zag pattern. The iris formation happens in the third month of embryonic life and unique patterns are formed during the first year of life. These patterns are random and do not rely upon genetic issue and also the solely characteristic that obsessed on biology is that the pigmentation. Image process techniques is utilized to convert iris pattern to distinctive code which may be keep during an information and permits comparisons between templates. The generalmethod for deed and storing iris options with iris picturesis listed as follow:

1. Image acquisition: take photo of iris with good resolution and quality.
2. Segmentation: process the acquiring image for separation of iris from eye image.
3. Normalization
4. Feature extraction and Feature encoding,
5. Storing extracted codes in database and comparing acquiring iris images with codes in database.

But in this research, another way is used for segmentation and extraction of iris region. In most previous methods iris edges are found with common edge detection algorithms, but here this algorithm is used.



Taking iris photo an important part in iris recognition and in most images tried to take images with maximum iris region with max opened eyes and no Latency lid on the iris. With using these iris images (CASIA standard database) a rectangle tangent is created to the periphery of the iris surrounding, remove out of rectangle, find an image with maximum part iris and an important advantage with iris in center of image. With having this kind of image first the image size and center pixel can be found with dividing row and column to two and marked this pixel. Certainly the pixel is in the pupil region and its clear pupilis the darker part in eye, so it can move right to the pixel with a high amount of difference intensity and mark it, move left to the pixel with a high amount of difference intensity and mark it and find the center of these points. Do the same and find top and bottom and center of them. Now with these center and peripheral acquired points we can find the real pupil center with center point and maximum distance drawing a pupil circle performing the same task to find the iris region and extract iris from eye image. With Gabor filter features and iris code can be extracted.

After comparing extracted code of a new iris image with codes in database and hamming distance algorithm, the code with minimum difference can be found which can be accepted consequently and save the difference number for an input in our fuzzy logic engine.

VII.FUSION

No trait can supply 100% correctness. Further, the results generated from the one- traits are good but the problem arises when the client is not able to give his iris image due to problem in exposure to light weight. As eye is the most perceptive organ of human body, the problem becomes critical when there exist some eye diseases. Thus in such a situation an individual will not be identified using the iris patterns and the biometric scheme comes to a standstill. Likewise, the difficulty faced by fingerprint recognition scheme is the occurrence of blemishes and slashes. The blemishes add noises to the fingerprint image which will not be enhanced completely using enhancement module. Thus, the scheme takes loud fingerprint as input which is not able to extract the minutiae points correctly and in turn, leads to untrue acknowledgement of an individual. Thus to overcome the troubles faced by one-by-one traits of iris and fingerprint, a novel blend is proposed for the acknowledgement scheme. The integrated scheme also supply anti spoofing measures by making it tough for an intruder to spoof multiple biometric traits simultaneously. By using weighted sum of score technique scores generated from individual traits are combined at matching score level. Let MSIris and MSFinger be the equivalent scores obtained from iris and fingerprint features respectively. The steps engaged are:

A. Score Normalization

This step brings both matching scores between 0 and 1 [14]. The normalization are done by,

$$N_{Iris} = \frac{MS_{Iris} - \min_{Iris}}{\max_{Iris} - \min_{Iris}}$$

$$N_{Finger} = \frac{MS_{Finger} - \min_{Finger}}{\max_{Finger} - \min_{Finger}}$$

Where minIris is the minimum score and maxIris is the maximum scores for iris acknowledgement and minFinger and maxFinger are the corresponding standards obtained from fingerprint trait.

B. Generation of Similarity Scores

Note that the normalized score of iris which is obtained through Wavelet presents the data of dissimilarity between the characteristic vectors of two given images while the normalized score from fingerprint presents a image measure. So to fuse both the score, there is a need to make both the scores as either similarity or dissimilarity assess.
In this paper, the normalized score of iris is altered to similarity measure by,

$$N'_{Iris} = 1 - N_{Iris}$$

C. Fusion

Fusion is performed by combining the biometric template extracted from every pair of fingerprints and irises representing a user. The matching score is calculated through the hamming distance calculation between two final fused templates. The template which is obtained in the encoding process will need a corresponding matching metric that provides a measure of the similarity degree between the two templates. Then the result of compared with an experimental threshold to decide whether or not the two representations belong to the same user.The scores of two normalized similarity, N'_{Iris} and N_{Finger} are fused linearly using sum rule as

$$MS = \alpha * N'_{Iris} + \beta * N_{Finger}$$

where α and β are two heaviness values that can be very resolute using some function. The combination of linear and exponential function is utilised in this paper. The worth of heaviness is allotted linearly if the worth of equivalent score is less than the threshold; else exponential weightage is given to the score. The value of MS is utilised as the equivalent score. So the candidate will be acknowledged only if MS is found to be more than the granted threshold value otherwise it is rejected.

VIII EXPERIMENTAL RESULTS

The results are tested on iris and fingerprint images collected by the authors. The database consists of three iris images (200×3) and two fingerprint images (200×3) per person with total of 200 persons. The iris images are acquired using CCD camera with uniform light source. However, fingerprint images are acquired using an optical fingerprint scanner. For the purpose allowing comparisons two levels of experiments are performed. At first level iris and fingerprints algorithms are tested individually. At this level the individual results are computed and an accuracy curve is plotted as shown in Figure 1. At this level the individual accuracy for iris and fingerprint is found to be 94.36% and 92.06% respectively as shown in Table 1.

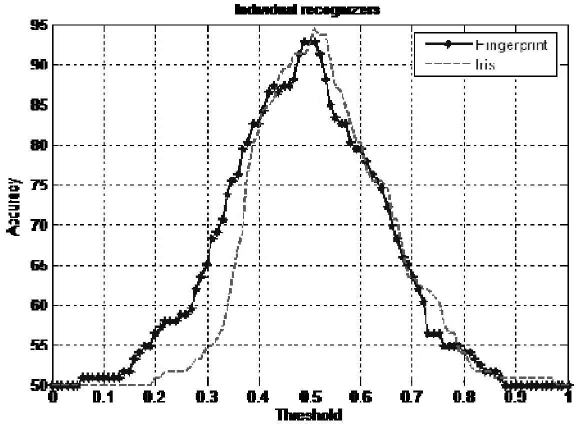


Figure 1 Accuracy plots of individual recognizers

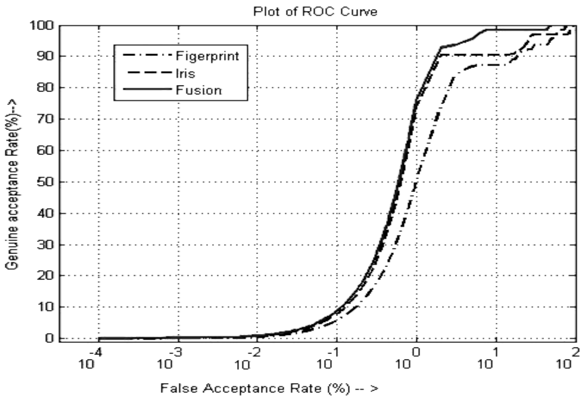


Figure 2 Accuracy graph for combined classifier

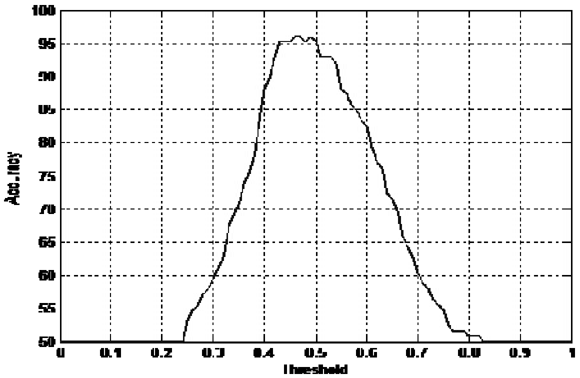


Figure 3 ROC Curve for Fingerprint, Iris and Fusion

However in order to increase the accuracy of the biometric system as a whole the individual results are combined at matching score level. At second level of experiment the matching scores from the individual traits are combined and final accuracy graph is plotted as shown in Figure 2. Table 1 shows the accuracy and error rates obtained from the individual and combined system. The overall performance of the system has increased showing an accuracy of 96.04% with FAR of 1.58% and FRR of 6.34% respectively. Receiver Operating Characteristic (ROC) curve is plotted for Genuine Acceptance Rate (GAR) against False Acceptance Rate (FAR) for individual recognizers and combined system as shown in Figure 3. From the plot it is clear that integrated system is giving highest GAR at lowest FAR.

Histograms for genuine and imposter data are shown in Figure 4 below. The distribution of genuine and imposter data shows that at threshold of 0.5 the system would give minimum FAR and FRR rates with maximum accuracy of 96.04%.

IX. CONCLUSION

Securing the data system becomes most difficult task as a result of the inflatedvariety of thievery. The traditional security system uses word or security key for authentication; however those word and security key may besimplytaken by the theft. To avoid these problems, biometrics of someoneis employed to secure the system. But, if the biometrics is takenonly once, it may beemployed bytheft to access the system till it exists. This provides largeproblem for the researchers to develop a brand new secure technique. One resolutionto the currentdrawback is usage of over one life science for securing the system. This can beas a result ofit'slargelynot possible for the theft to steal over one biometrics. This paper used fingerprint and iris biometrics to secure the system. The features obtained from this biometricsare combined exploitation fusion technique. From these fusedfeatures, cryptanalytickeys generated that is safer than different techniques. Theexperimental result shows that the proposed security themeleads tohigher security than the existing techniques. The experimental results show that the accuracy of system would increase on combining the traits. The system is giving an overall accuracy of 96.04% with FAR and FRR of 1.58% and 6.34%.

REFERENCES

[1] Ross, & A. K. Jain, Information Fusion in Biometrics, *Pattern Recognition Letters, 24*(13), 2003, 2115-2125.

[2] W. Yunhong, T. Tan, & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, *Proceedings of Fourth International Conference on AVBPA*, Guildford, UK, 2003, 805-813.

[3] S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, *Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA)*, Rye Brook, NY, 2005.

[4] G. Feng, K. Dong, D. Hu, & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, *International Conference on Bioinformatics and its Applications*, Hong Kong, China, 2004, 701-707.

[5] L. Flom, & A. Safir, Iris Recognition System, U.S. Patent No. 4641394, 1987.

[6] J. G. Daugman, High confidence visual recognition of persons by a test of statistical independence, *IEEE Transactions on Pattern Analysis and Machine Intelligence,15*(11), 1993, 1148–1161.

[7] W. W. Boles, & B. Boashah, A Human Identification Technique Using Images of the Iris and Wavelet Transform, *IEEE Transaction on Signal Processing, 46*(4), 1998, 1185-1188.

[8] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, & S. McBride, A Machine vision System for Iris Recognition, *Machine Vision and Applications,9*(1), 1996, 1-8.

[9] A. E. Hassanien, & J M. Ali, An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, *Advanced Modeling and Optimization Journal*, *5*(2), 2003, 93-104.

[10] H. C. Lee, & R. E. Gaensslen, Eds., *Advances in Fingerprint Technology* (New York, Elsevier, 1991).

[11] Federal Bureau of Investigation,*The Science of Fingerprints (Classification and Uses)* (Washington, D.C., US Govt. Printing Office, 1984).

[12] L. Hong, Y. Wan, & A.K. Jain, Fingerprint Image Enhancement: Algorithm and Performance Evaluation, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *20*(8), 1998, 777-789.

[13] Raymond Thai, Fingerprint Image Enhancement and Minutiae Extraction, *Technical Report,*The University of Western Australia, 2003.

[14] A. K. Jain, K. Nandakumar, & A. Ross, Score Normalization in multimodal biometric systems. *The Journal of Pattern Recognition Society*, *38*(12), 2005, 2270-2285.

[15] Nageshkumar.M, Mahesh.PK and M.N. ShanmukhaSwamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[16] KornelijeRabuzin and Miroslav Baca and MirkoMalekovic, "A Multimodal Biometric System Implemented within an Active Database Management System", Journal of software, vol. 2, no. 4, October 2007.

[17] M Baca and K. Rabuzin, "Biometrics in Network Security", in Proceedings of the XXVIII International Convention MIPRO 2005, pp. 205-210 , Rijeka,2005.