

FUSION BASED MULTIMODAL BIOMETRIC AUTHENTICATION WITH ANAMOLY INTRUSION DETECTION SYSTEM

M.Thenmozhi , P.Gnana Skanda Parthiban

ABSTRACT—Biometrics is a technology for authenticating a person's unique identity beyond doubt. Multimodal biometric technology provides potential solutions for user-to-device authentication. This paper proposes combined authentication and IDSs. Multi-biometric systems are emerging as a trend which helps in overcoming limitations of single biometric solutions, such as distinctiveness ability and lack of universality. It aims to fuse two or more physical or behavioral traits to provide optimal False Acceptance Rate (FAR) and False Rejection Rate (FRR), thus improving system accuracy and dependability. The results of fusion of individual modalities indicate an improvement in the overall performance of the biometric authentication system. Authentication works only at the point of entry it lacks the capability to monitor the entire system. In this paper Multimodal biometrics is deployed to work with intrusion detection systems (IDSs) that have the capability to monitor the system where majority of attacks takes place.

Index Terms—Authentication, Fusion, iris and finger knuckle biometrics, Intrusion Detection System, Multimodal biometric system, Pattern Recognition.

I. INTRODUCTION

Biometric technologies refer to identifying individuals based on their unique biological or behavioral traits. Traditional authentication procedures, based on the simple username–password approach were insufficient to provide a suitable security level for the applications requiring a high level of protection for data and services. Biometric-based authentications systems represent a valid alternative to traditional approaches. Unimodal biometric systems, operating on a single biometric feature, have many limitations, which are as follows [1] Noise in sensed data, Intra-Class Variation. Multimodal biometric systems are a recent approach developed to overcome these problems. These systems demonstrate significant improvements over unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing. Multibiometrics data can be combined at different levels: fusion at data-sensor level, fusion at the feature extraction level, fusion at the matching level, and fusion at the decision level. In this paper, a weighted summation rule fusion technique has been used to integrate iris and finger knuckle features. The fusion process is effective, because fused scores provide much better discrimination than individual scores. Authentication is effective in preventing unauthorized access to the system but lacks capabilities to monitor the system where majority of attacks takes place. Attacks could be done by the employees who have legitimate access to the system but they could use the privilege to do harm. In this paper Multimodal biometrics is deployed to work with intrusion detection systems (IDSs) that have the capability to monitor the system where majority of attacks takes place. The paper is organized as follows. Section II presents the main related works. Section III describes the proposed system.

Section IV shows the achieved experimental results. Finally, some conclusions and future works are reported in Section V

II. RELATED WORKS

This section briefly outlines different approaches for unimodal and multimodal biometric systems. Multimodal biometric systems are based on different biometric features and/or introduce different fusion algorithms for these features. An unimodal fingerprint verification and classification system is presented in [6]. This system works based on a feedback path for the feature-extraction stage, followed by a feature-refinement stage to improve the matching performance. Ratha *et al.* [8] proposed a unimodal distortion-tolerant fingerprint. The proposed algorithm has been tested with a large private database with the use of an optical biometric sensor. Concerning iris recognition systems in [8], the Gabor filter and 2-D wavelet filter are used for feature extraction. This method is invariant to translation and rotation and is tolerant to illumination. The classification rate on using the Gabor is 98.3% and the accuracy with wavelet is 82.51%. In the approach proposed in [15], multichannel and Gabor filters have been used to capture local texture information of the iris, which are used to construct a fixed-length feature vector. Conti *et al.* [15] proposed a multimodal biometric system using two different fingerprint acquisitions. The matching module integrates fuzzy-logic methods for matching-score fusion. Experimental trials using both decision-level fusion and matching-score-level fusion were performed. Experimental results have shown an improvement of 6.7% using the matching score- level fusion rather than a monomodal authentication system. Yang and Ma [7] used fingerprint,

palm print, and hand geometry to implement personal identity verification. Unlike other multimodal biometric systems, these three biometric features can be taken from the same image. They implemented matching score fusion at different levels to establish identity. Woodard and Flynn [3] have examined the fine features of finger surface for its use in the biometric system. Authors have presented promising results by using curvature and a shape-based index from finger surface features extracted from 3-D range images. However, the work detailed in [15] does not exploit the texture information that can be simultaneously extracted from the intensity images of hands. Malassiotis *et al.* [13] have also illustrated the utility of 3-D finger geometry features by using peg-free imaging. This approach has illustrated promising results while combining the color and 3-D information to authenticate user hands in the cluttered background. The finger shape information is generally believed to be less discriminative and only suitable for small-scale user identification. The limited number of cross-sectional 3-D measurements and absence of any finger texture information in [15] poses further limitations on the scalability of this approach for its real usage. Ribaric and Fratric [15], [16] employed appearance-based features from the finger and palm surface images for personal identification. However, the authors in [16] and [15] have employed a scanner for imaging which is very slow and, hence, not suitable for online user authentication. Also, in [16], the geometrical features from the acquired images were not utilized which could offer further performance improvement [15] when utilized in conjunction with palm texture features. The work, detailed in [16] and [15], is promising but it relies on crease and wrinkle details on the palm side of the fingers which are quite limited. "Anomaly" detection and "Misuse" detection are two main techniques that HIDS use. Anomaly detection refers to intrusions that can be detected based on anomalous behaviour and use of computer resources. Anomaly detection usually uses methods of statistic analysis methodology, artificial neural network technology, data mining technology, and artificial immune technology. Misuse intrusion detection refers to the detection of intrusions by precisely defining them ahead of time and watching for their occurrences [17]. Misuse intrusion detection usually use methods of expert system, TCP/IP protocol analysis, and pattern matching.

III. PROPOSED SYSTEM

Biometric technology can be used to automatically and continuously identify or verify individuals by their physiological or behavioral characteristics.

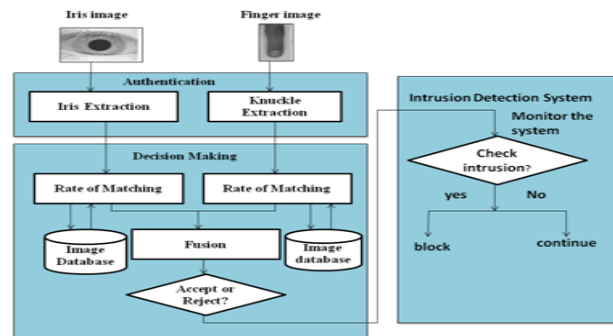
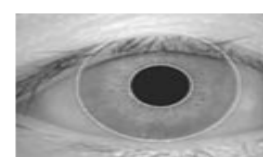
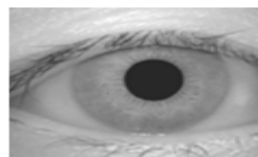


Fig 1. proposed system architecture

In this paper Iris and finger knuckle images are pre-processed to extract the Region of interest, based on singularity regions, surrounding some meaningful points. Based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold, each biometric system outputs a binary decision: accept or reject. Intrusion detection is one of the high priority and challenging tasks for network administrators and security professionals. More sophisticated security tools mean that the attackers come up with newer and more advanced penetration methods to defeat the installed security systems [4] and [5]. Thus, there is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems. As shown in Fig. 1, the proposed system is composed of three main stages: the authentication, decision making and Intrusion Detection System. Iris and finger knuckle images are pre-processed to extract the respective features.

A. IRIS RECOGNITION

The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitised image of the eye, and encode it into a biometric template, which can be stored in a database. As shown in fig.2. Iris segmentation process is composed of three tasks: iris segmentation, iris normalization and matching. The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life.



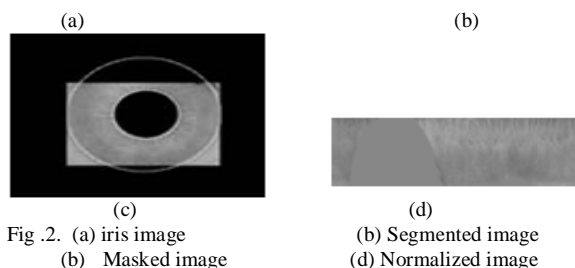


Fig. 2. (a) iris image
(b) Masked image

1. SEGMENTATION

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. Two circles can approximate the iris region, one for the iris/sclera boundary and another, for the iris/pupil boundary (interior to the first). The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern. A technique is required to isolate and exclude these artifacts as well as to locate the circular iris region. Here the circular Hough transform was used for detecting the iris and pupil boundaries. This involves employing canny edge detection to generate an edge map.

2. NORMALISATION

Once the iris region is successfully segmented from an eye image, the next step is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The normalisation process will produce iris regions, which have the same constant dimensions. For normalisation of iris regions, a technique based on Daugman's rubber sheet model is employed. The homogenous rubber sheet model, which remaps the iris image from Cartesian coordinates to a doubly dimensionless non-concentric polar coordinate.

3. FEATURE ENCODING AND MATCHING

In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made. Feature encoding is implemented by convolving the normalized iris pattern with 1D Log-Gabor wavelets. The 2D normalized pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal in which each row corresponds to a circular ring on the iris region. Since maximum independence occurs in the angular direction, the angular direction is taken rather than the radial one, which corresponds to columns of the normalized pattern.

The intensity values at known noise areas in the normalized pattern are set to the average intensity of surrounding pixels to prevent influence of noise in the output of the filtering. The output of filtering is then phase quantized to four levels using the Daugman method.

HD-Based Matching: The matching score is calculated through the HD calculation between two final templates. The result of the measure is then compared with an experimental threshold to decide whether or not the two representations belong to the same user. If two patterns X and Y have to be compared, the HD is defined as the sum of discordant bits in homologous position (XOR operation between X and Y bits). In other words

$$HD = \frac{1}{N} \sum_{j=1}^N XOR(x_j, y_j)$$

where N is the total number of bits.

B.FINGER KNUCKLE EXTRACTION

The image-pattern formed from the finger-knuckle bending is highly unique and makes this surface a distinctive biometric identifier. As shown in fig.3. Finger knuckle extraction process is composed of three steps: knuckle extraction, normalization, matching process. Each acquired hand image is first subjected to thresholding operation to obtain the binarized image.

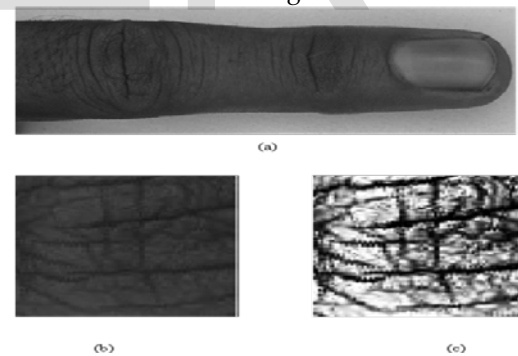


Fig.3. (a) Finger image (b) Segmented finger knuckle image
(c) Enhanced knuckle image

1. NORMALIZATION

The normalization of image is essential because their varying ranges and order. In this paper the normalization has been done using a scheme called min-max normalization and thereby the normalized feature vector is obtained,

$$x_{ik}^f = \frac{x_{ik} - \min(x_{ik})}{\max(x_{ik}) - \min(x_{ik})}$$

where

$x_{ik} = x_{i1}, x_{i2}, \dots, x_{in}$ is the feature vector with the N values and x_{ik}^j is the corresponding normalized feature vector.

2. EXTRACTION OF KNUCKLES

Once the finger image is loaded, the knuckle regions are located for the extraction of reliable features. An approach is used for extracting knuckle regions from the segmented finger. In this approach the canny edge detector is first applied on the extracted finger image. The density of the high intensity pixels in the resultant image is used for knuckle extraction. The knuckle region, have the high intensive and density pixels. This region can be centrally extracted on either side of the central line. Therefore, a region with mostly edge elements along the finger symmetry line, is extracted centrally from the base part of the finger

3. MATCHING KNUCKLE IMAGES

The knuckle images present a random texture which is observed to be quite unique in each user. The information content from the extracted knuckle image consists of certain local and global features which are observed to be quite stable. This Information from knuckle images can be extracted by registering the variations in an ensemble of knuckle images, independent of any judgment of creases or lines. This information can then be used to authenticate individual users. In this paper Linear Discriminant Analysis is used for generating matching scores from the knuckle images

C.FUSION

The two normalized similarity scores N_{Iris} and N_{Fk} are fused linearly using sum rule as

$$S = (w_1 * N_{Iris} + w_2 * N_{Fk}) - \sum_{n=0}^N E_n$$

where w_1 and w_2 are two weight values that can be determined using some function. The value of weight is assigned linearly if the value of matching score is less than the threshold; otherwise exponential weight is given to the score. The value of S is used as the matching score. E is the error rate. So if S is found to be more than the given threshold value the candidate is accepted otherwise it is rejected.

D. INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is usually located and operated at the host, where it captures local suspicious events. Intrusion detection system involves detecting

unusual patterns of activity or patterns of activity that are known to correlate with intrusions. Log files record the behavior of computer system and aim at recording the action of operating system, applications, and use behaviors. Log system is particularly important in intrusion detection and log file analysis tool have become an indispensable tools for daily inspection and maintenance of the system running.

BEHAVIORAL BASED INTRUSION DETECTION SYSTEM

A Behavioral based intrusion detection system references a baseline or learned pattern of normal system activity to detect the intrusive activities.

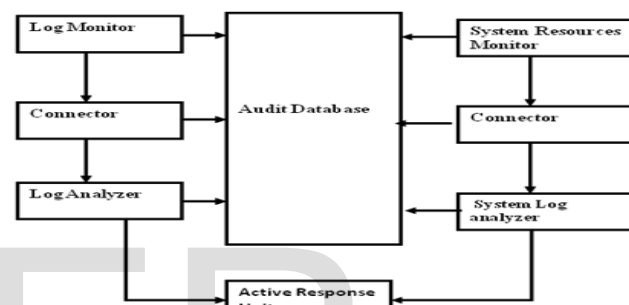


Fig .4. The structure of HIDS

The following table illustrates some intrusion detection measures that should be done to provide a full secure system. In this paper host-based intrusion detection system is proposed shown in fig.4, which monitors the file and system resources and makes responses if any intrusion is detected. Monitoring process could be done by comparing user activities with the system log file.

1. FILE-ANALYZER

Most operating systems provide a file system, as a file system is an integral part of any modern operating system. This layer, the File-Analyzer monitor is directed towards monitoring the files and folders on a host server that could be of interest to any intruder and this is determined to a large extent by the administrator. The administrator decides on the important files or directories to monitor so that the proposed IDS does not monitor all the files and folders on the machine as this would cause a large overhead on the system resources.

Login and Session Activity
<ul style="list-style-type: none"> • Login frequency • Login frequency at different positions • Time consumed by each session • Website output
Resources utilization
<ul style="list-style-type: none"> • Password failed times when login • The implementation of commands and procedures • Operating frequency • Utilization of procedure resources
File operating activity
<ul style="list-style-type: none"> • The frequency of file read, write, create, and delete • Records read and write • Read, write, create and delete file

Table.1. some measures that intrusion detection can use

2. SYSTEM RESOURCES ANALYZER

Programs often need certain system resources such as memory or disk space, and they request them as needed from the operating system. This layer is designed to periodically scan through the system log for latest entries and compare with the threshold value that must have been defined by the user. This enables the system resources layer to detect intrusions on system resources. Data flows from the user who relates with the system by specifying the system resource to be monitored, specify the threshold values. This layer sends this information (the threshold values and the signatures) to the database. The agent collects this information from the database for analysis to determine if the incoming events have exceeded the defined threshold values for the system resource in question. If the agent flags alerts to the threshold values being exceeded, the system responds by alerting the user through text – based messages.

IV.EXPERIMENTAL RESULTS

The performance of the user authentication approach detailed in previous sections was evaluated on the biometric data.

A. Recognition Analysis of the Multimodal System

The multimodal recognition system performance evaluation has been performed using the well-known FRR and FAR indexes. For an authentication system, the FAR is the number of times that an incorrectly accepted unauthorized access occurred, while the FRR is the number

of times that an incorrectly rejected authorized access resulted. The matching scores obtained from the biometric matchers were combined using weighted summation fusion rule. The score has been obtained weighting the matching scores (0.65 for iris and 0.35 for fingerknuckle) of each unimodal biometric system.

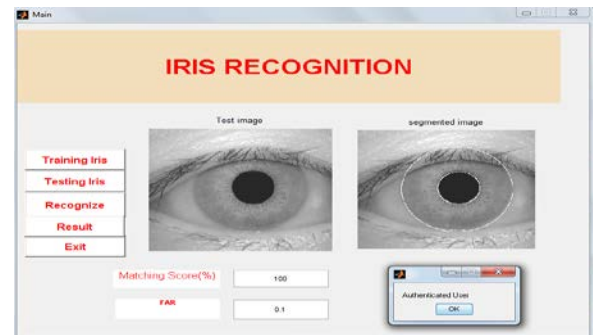


Fig.5. iris authentication using a graphical user interface

Finger knuckle extraction process is composed of three steps: knuckle extraction, normalization, matching process. Based on a comparison of the matching score between the input sample and the enrolled template with a decision threshold, biometric system outputs a binary decision: accept or reject.

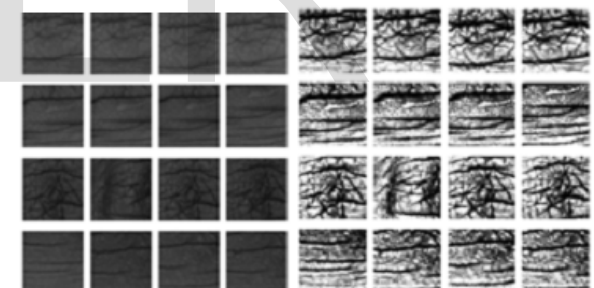


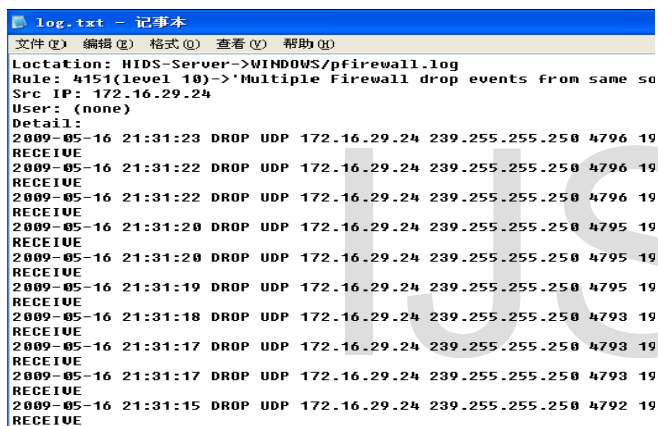
Fig.6. (a) Finger knuckle samples from four users (b) corresponding enhanced image

To easily manipulate the images from the database an interface has been built that allows the user to choose between different options. As shown in fig.5 the first option is to select images from the database. The second option performs the segmentation. The third option obtains the matching score by similarity measure algorithm hamming distance.

W_1	S_1	W_2	S_2	E	$W_1.S_1$	$W_2.S_2$	$W_1.S_1+W_2.S_2$	Fused Score $S=W_1.S_1+W_2.S_2-E$	If $S>Threshold$ "1" Else "0"
0.5	95.34	0.5	92.41	0.04	47.67	46.205	93.875	93.834	Authorized user(1)
0.5	54.86	0.5	43.32	0.04	27.43	21.66	49.09	49.049	Un authorized user(0)

Table 2. Matching score fusion

Table.1 shows the results of fusion of matching score. Where w_1, S_1 is the weight and matching score for iris authentication and w_2 and s_2 will be the weight and score for finger knuckle authentication. The corresponding scores get fused and errors get subtracted from the fused score. A threshold is set and based upon the threshold decision will be made.



```

log.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Location: HIDS-Server->WINDOWS/pfirewall.log
Rule: 4151(level 10)->'Multiple Firewall drop events from same so
Src IP: 172.16.29.24
User: (none)
Detail:
2009-05-16 21:31:23 DROP UDP 172.16.29.24 239.255.255.250 4796 19
RECEIVE
2009-05-16 21:31:22 DROP UDP 172.16.29.24 239.255.255.250 4796 19
RECEIVE
2009-05-16 21:31:22 DROP UDP 172.16.29.24 239.255.255.250 4796 19
RECEIVE
2009-05-16 21:31:20 DROP UDP 172.16.29.24 239.255.255.250 4795 19
RECEIVE
2009-05-16 21:31:20 DROP UDP 172.16.29.24 239.255.255.250 4795 19
RECEIVE
2009-05-16 21:31:19 DROP UDP 172.16.29.24 239.255.255.250 4795 19
RECEIVE
2009-05-16 21:31:18 DROP UDP 172.16.29.24 239.255.255.250 4793 19
RECEIVE
2009-05-16 21:31:17 DROP UDP 172.16.29.24 239.255.255.250 4793 19
RECEIVE
2009-05-16 21:31:17 DROP UDP 172.16.29.24 239.255.255.250 4793 19
RECEIVE
2009-05-16 21:31:15 DROP UDP 172.16.29.24 239.255.255.250 4792 19
RECEIVE

```

Fig.7. The intrusion information detected by log analysis

Figure.7 is the sample screenshot that illustrates intrusions that were detected by log analysis technology. The pseudo code monitor the file activity and system resources and an output value is given. If the output value equals to 0, then it is normal, else if the output value equals to 1, then it is abnormal.

V.CONCLUSION AND FUTURE ENHANCEMENTS

In the proposed scheme iris recognition and Finger Knuckle recognition is employed to improve the biometric authentication. The fusion process is effective, because fused scores provide much better discrimination than individual scores. The proposed Intrusion Detection system that can be used in any single Host for detection of unwanted activities such as tampering with important files, unauthorized connection, unauthorized elevation of permissions etc. Combining continuous authentication and

Intrusion detection could be an effective approach to improve the security performance.

Some of the future enhancements that can be incorporated to improve the security and performance of the system are given below:

- (1) Other biometric features like face, fingerprint, palm print etc can be used in this research, which may provide better results.
- (2) Cryptographic techniques can be incorporated in this research, which would increase the security.
- (3) Implement this work in a distributed environment.

REFERENCES

- [1] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern Recogn. Lett.*, vol. 24, pp. 2115-2125, 2003. DOI: 10.1016/S0167-8655(03)00079-5.
- [2] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. Berlin, Germany: Springer-Verlag. ISBN 978-0-387-22296-7.
- [3] D. L. Woodard and P. J. Flynn, "Finger surface as a biometric identifier," *Comput. Vis. Image Understanding*, vol. 100, pp. 357-384, Aug. 2005.
- [4] Dorothy Denning, "An Intrusion Detection Model", *IEEE Transactions on Software Engineering*, February 1987, pp.2- 222.
- [5] G. Vigna and C. Kruegel, "Host-based Intrusion Detection Systems," in *The Handbook of Information Security, Volume III*, John Wiley & Sons, December 2005.
- [6] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on fingerprint identification and Iris recognition," in *Proc. 3rd Int. IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008)*, pp. 1-5. DOI: 10.1109/ICTTA.2008.4530129.
- [7] F. Yang and B. Ma, "A new mixed-mode biometrics information fusion based on fingerprint, hand-geometry and palm-print," in *Proc. 4th Int. IEEE Conf. Image Graph.*, 2007, pp. 689-693. DOI: 10.1109/ICIG.2007.39.
- [8] J. Cui, J. P. Li, and X. J. Lu, "Study on multi-biometric feature fusion and recognition modl," in *Proc. Int. IEEE Conf. Apperceiving Comput. Intell. Anal. (ICACIA)*, 2008, pp. 66-69. DOI: 10.1109/ICACIA.2008.4769972.
- [9] L. Ma, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Trans. Image Process.*, vol. 13, no. 6, pp. 739- 750, Jun. 2004.
- [10] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," in *Proc. 5th IEEE Workshop Appl. Comput. Vis.*, Dec. 4-6, 2000, pp. 29-34. DOI: 10.1109/WACV.2000.895399.
- [11] Sandeep Kumar, Eugene H. Spaffor, "An application of Pattern Matching in Intrusion Detection", Technical report 94-013, Purdue University, Department of computer sciences, March 1994.
- [12] S. K. Dahel and Q. Xiao, "Accuracy performance analysis of multimodal biometrics," in *Proc. IEEE Syst., Man Cybern. Soc., Inf. Assur. Workshop*, 2003, pp. 170-173. DOI: 10.1109/SMCSIA.2003.1232417.
- [13] S. Malassiotis, N. Aifanti, and M. G. Strintzis, "Personal authentication using 3-D finger geometry," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 12-21, Mar. 2006.

[14] S. Prabhakar, A. K. Jain, and J.Wang, "Minutiae verification and classification," presented at the Dept. Comput. Eng. Sci., Univ. Michigan State, East Lansing, MI, 1998.

[15] S. Ribaric and I. Fratric, "A biometric identification system based on eigenpalm and eigenfinger features," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 11, pp. 1698–1709, Nov. 2005.

[16] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, "Fuzzy fusion in multimodal biometric systems," in *Proc. 11th LNAI Int. Conf. Knowl.- Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007)*, Part I LNAI 4692. B. Apolloni *et al.*, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 108–115.

[17] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification on iris patterns," in *Proc. 15th Int. Conf. Pattern Recogn.*, 2000, vol. 2, pp. 805–808.



M.Thenmozhi received a B.E degree in Computer Science and Engineering (2010) and M.E. degree in Computer Science and Engineering (2012) from the Anna University, Chennai. From 2012, she is working as a Assistant Professor at the CSE department, Syed Ammal Engineering College, Ramanathapuram. Her original research interests were in Data Mining, Image Processing and Network Security.



P.Gnana Skanda Parthiban received a B.E degree in Electrical & Electronic Engineering (2006) from Anna University, Chennai and M.E. degree in Embedded System Technologies (2009) from the Anna University, Coimbatore. From 2009, he is working as a Assistant Professor at the ECE department, Mohammed Sathak Engineering College, Kilakarai, Ramanathapuram. His original research interests were in Embedded System, Microprocessor Design.