Multimodal Biometric Authentication System For Accurate Identity Verification

Nageswara Rao Thota[1], Srinivasa Kumar Devireddy[2]

Abstract

Biometrics refers to the automatic identification of an individual based on his/her physiological or behavioral traits. Unimodal biometric authentication systems perform person recognition based on a single source of biometric information and are affected by problems like noisy sensor data, non-universality and lack of individuality of the chosen biometric trait. Some of the limitations imposed by unimodal biometric systems (that is, biometric systems that rely on the evidence of a single biometric trait) can be overcome by using multiple biometric modalities. Such systems, known as Multimodal biometric systems, are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. A multimodal biometric authentication system integrates information from multiple biometric sources to compensate for the limitations in per-formance of each individual biometric system. This paper proposes the multimodal biometric authentication system for identity verification using four traits i.e., face, fingerprint, iris and signature. The proposed system is designed for applications where the training database contains a face, iris, fingerprint and/or signature for each individual. The final decision is made by fusion at "matching score level architecture" in which feature vectors are created independently for query images and are then compared to the enrollment templates which are stored during database preparation for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module. Multimodal system is developed through fusion of face, fingerprint, iris and signature recognition. This system is tested on a database and the overall accuracy of the system is found to be more than 97% accurate with FAR and FRR of 2.46% and 1.23% respectively.

Keywords: Biometrics, Multimodal, Face, Fingerprint, Iris, Signature, Fusion, Matching score

1. Introduction

Traditionally Passwords (Knowledge based Security) and ID cards (token-based security) have been used to restrict access to secure systems. However, security can be easily breached in these systems when a password is revealed to an unauthorized user or a card is stolen by an impostor. Furthermore, simple passwords are easy to guess by an impostor and difficult passwords may be hard to recall by a legitimate user. The emergence of biometrics has addressed the problems that plague traditional verification methods. "Biometrics" means "life measurement", but the term is usually associated with the use of unique physiological characteristics to identify an individual. One of the applications which most people associate with biometrics is security. However, biometrics identification

[1] Dept. of BES, Nalanda Institute of Engineering & Technology, Siddharth Nagar, Kantepudi(V), Sattenapalli(M), Guntur (Dt.), A.P, India. email : tnraothota@yahoo.co.in

[2] Dept. of CSE&IT, Nalanda Institute of Engineering & Technology, Siddharth Nagar, Kantepudi(V), Sattenapalli(M), Guntur (Dt.), A.P., India. email : srinivaskumar_d@yahoo.com

has eventually a much broader relevance as computer interface becomes more natural. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [1]. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits till date are facing numerous problems; some of them are inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments etc.

i) ***Noise in sensed data.*** A fingerprint with a scar and a voice altered by a cold are examples of noisy inputs. Noisy data could also result from defective or improperly maintained sensors (for example, accumulation of dirt on a fingerprint sensor) and unfavorable ambient conditions (for example, poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

ii) ***Intra-class variations.*** The biometric data acquired from an individual during authentication may be very different from the data used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor, or when sensor characteristics are modified (for example, by changing sensors, that is, the sensor interoperability problem) during authentication.

iii) ***Distinctiveness.*** While a biometric trait is expected to vary significantly across individuals, there may be large similarities in the feature sets used to represent these traits. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

iv) ***Non-universality.*** While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges. Thus, there is a Failure To Enroll (FTE) rate associated with using a single biometric trait. There is empirical evidence that about 4% of the population may have poor quality fingerprints that cannot be easily imaged by some of the existing sensors.

v) ***Spoof attacks.*** An impostor may attempt to spoof the biometric trait of a legitimately enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits like fingerprints are also susceptible to spoof attacks.

One way to overcome these problems is the use of multi-biometrics. Driven by lower hardware costs, a multi biometric authentication system uses multiple sensors for data acquisition. This allows capturing multiple samples of a single biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi source or multimodal biometrics). This approach also enables a user who does not possess a particular biometric identifier to still enroll and authenticate using other traits, thus eliminating the enrollment problems and making it universal. A unimodal biometric system [2] consists of three major modules: sensor module, feature extraction module and matching module. The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module may not be reliable. This problem can be solved by installing multiple sensors that capture different biometric traits. Such systems, known as multimodal biometric authentication systems [3], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications. However, multimodal systems address the problem of non-universality: it is possible for a subset of users who do not possess a particular biometric. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. By asking the user to present a random subset of biometric traits, the system ensures that a live user is indeed present at the point of acquisition. However, an integration scheme is required to fuse the information presented by the individual modalities.

This paper proposes an efficient multimodal biometric authentication system which can be used to reduce/ remove the above mentioned limitations of unimodal authentication systems.

2. Overview

Multimodal biometric Authentication systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of reducing false non-match and false match rates, providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

Ross and Jain [2] have presented an overview of Multimodal Biometrics and have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies and design issues. A multimodal system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next modality is used. Therefore, multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities is used simultaneously in order to perform recognition. The levels of fusion proposed [2] for multimodal systems are broadly categorized into three system architectures.

- Fusion at the Feature Extraction Level
- Fusion at the Matching Score Level
- Fusion at the Decision Level

In *Fusion at the Feature Extraction Level*, information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system.

In *Fusion at the Matching Score Level*, feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score which is passed to the decision module.

In *Fusion at the Decision Level*, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote. This architecture is rather loosely coupled system architecture, with each subsystem performing like a single biometric system.

A substantial amount of work has been carried out on the combination of multiple classifiers. Most of such work focuses on fusing 'weak' classifiers for the purpose of increasing the overall performance (Tolba & Rezq) [3]. A hybrid fingerprint matcher [4] which fuses minutiae and reference point location classifiers has been proposed by Ross, Jain & Riesman. It has been reported that the performance of the hybrid matcher is better than individual classifiers. Apart from fusion of multi classifiers, much work has also been done to combine traits/different modalities at various levels. Yunhong, Tan & Jain proposed the fusion of iris and face modalities [5] and reported that besides improving verification performance, the fusion of these two has several other advantages. Dass, Nandakumar & Jain have proposed an approach to score level fusion in multimodal biometric systems [6]. Experimental results have been presented on face, fingerprint and hand geometry using product rule and coupla method. It is found that both fusion rules show better performance than individual recognizers. Common theoretical framework [7] for combining classifiers using sum rule, median rule, max and min rule are analyzed by Kittler et al. under the most restrictive assumptions and have observed that sum rule outperforms other classifiers combination schemes. Guiyu Feng et. al. presents a novel fusion strategy for personal identification using face and palmprint biometrics [8]. The work considers the feature level fusion scheme. The purpose of the proposed paper is to investigate whether the integration of face and palmprint biometrics can achieve higher performance that may not be possible using a single biometric indicator alone. Both Principal Component Analysis (PCA) and Independent Component Analysis (ICA) are considered in this feature vector fusion context. It is found that the performance improved significantly.

3. Multimodal Biometric Authentication System

The multimodal biometric authentication system is developed using four traits i.e., face, fingerprint, iris and signature. In Face Recognition, the input face image is recognized using Elastic Bunch Graph matching algorithm. In Fingerprint Verification, the input image is enhanced to bring out obscure information based on Gabor filtering and matching is done by combination of Reference Point and Minutiae matching algorithms. In

Iris Recognition, the input image is localized by finding the pupillary and outer iris boundary and is matched using combination of Haar Wavelet and Circular Mellin operator. In Signature Verification, feature vector consists of Global and Local features of signature image and is matched using Euclidean Distance. The modules based on the individual traits returns an integer value after matching the database and query feature vectors. First of all the fusion is done at classifier level i.e., for face, fingerprint and iris, multiple classifiers are combined at matching score level followed by fusion at multiple modalities level. The final score is generated by using sum of score technique at matching score level which is passed to the decision module. The brief description of various recognition algorithms are presented below:

3.1 Face Recognition

Face Recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of distinguishing features of the face [9][10][11]. The recognition algorithm takes facial image, measures the unique characteristics and computes the template corresponding to each face. Using templates, the algorithm then compares that image with another image and produces a score that measures how similar the images are to each other.

Feature Extraction Using EBGM AND KDDA

Elastic Bunch Graph Matching (EBGM)

Face recognition using elastic bunch graph matching [12] is based on recognizing novel faces by estimating a set of novel features using a data structure called a bunch graph. Similarly for each query image, the landmarks are estimated and located using bunch graph. Then the features are extracted by convolution with the number of instances of Gabor filters followed by the creation of face graph. The matching score (MS_{EBGM}) is calculated on the basis of similarity between face graphs of database and query image.

Kernel Direct Discriminant Analysis (KDDA)

Face recognition using KDDA [11] is based on computation of feature space F (from training set) and projection of input pattern into the feature space to calculate significant discriminant features. For each of the *m* features in the database and *n* features in the query image, reference features are chosen depending on the distance and rotation between the positions of features in the feature space. The matching score for each transformation of database and query feature vectors are calculated with respect to reference feature chosen using bounding box technique. MS_{KDDA} is defined by the maximum of all matching scores divided by the maximum number of features.

Combination of EBGM AND KDDA

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the face recognition system.

3.2 Fingerprint Recognition

The fingerprint recognition system has been developed by the fusion of Reference Point and Minutiae Matching Techniques [13][14]. The key steps involved are fingerprint enhancement, feature extraction using Reference point Algorithm and Minutiae Matching approach and computation of matching score. The goal of fingerprint enhancement [15] is to increase the clarity of ridge structure so that minutiae and the reference points can be easily and correctly extracted.

Feature Extraction using Reference point and Minutiae Matching Approach

Reference Point Algorithm [4] gracefully handles local noise in a poor quality fingerprint. The detection should necessarily consider a large neighborhood in the fingerprint image. For an accurate localization of the reference point, the input image is segmented to remove any kind of noise present in the image. Further Sobel Operator is applied to obtain gradient of segmented image. The Orientation Field is estimated along with the Y component. A specific pattern in which the value of Y - Component is the point of maximum curvature. The finger code is generated by drawing concentric circles of fixed radius centered at reference point. The image is segmented into 5 tracks and 16 sectors from the detected reference point. The size of the feature vector is 512 values. The distance (D_{Ref}) for the database and query feature vectors is calculated using Euclidean distance method.

Minutiae Matching

The input fingerprint image is enhanced using Gabor Filters. The enhanced image is further binarized and thinned using a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The thinned image is used to detect minutiae points [4] by locating ridge ending and bifurcations using Crossing Number (*CN*) method. The matching score MS_{MIN} between the database and query image is computed using Elastic matching approach [13].

Combination of Reference Point and Minutiae Matching Algorithm

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the fingerprint system.

3.3 Iris Recognition

The iris image acquired from a 3CCD camera is localized by finding the center of pupil from the spectrum image. The radius of the pupil is the distance between the pupil center and nearest non-zero pixel. The outer iris boundary is detected by drawing concentric circles of different radii from the pupil center and the intensities lying over the perimeter of the circle are summed up. The annular region lying between pupil and iris boundary is transformed to polar co-ordinates [16] to take into consideration the possibility of pupil dilation and appearing of different size in different images. From the normalized strip the eyelids are detected and removed.

Feature Extraction using Haar Wavelet and Circular Mellin operator Haar Wavelet

Haar wavelet is widely used in texture recognition algorithms [17]. The input signal *S* (polarized iris image) is decomposed into approximation, vertical, horizontal and diagonal coefficients using the wavelet transformation and coefficients for the fourth and fifth levels are chosen to reduce space complexity and discard the redundant information. The iris code is generated by assigning one to the positive coefficient values and zero to negative values.

Circular Mellin Operators

These "Circular Mellin" operators are invariant to both scale and orientation [18] of the target and represent the spectral decomposition of the image scene in the polar-log coordinate system. Features in iris images are extracted based on the phase of convolution of polarized iris image with mellin operators. The iris code is one for positive phase values and zero for negative phase values.

The iris codes generated using Haar Wavelet and Circular Mellin operators are matched using Hamming Distance approach.

Combination of Haar Wavelet and Circular Mellin Operator

The individual matching scores generated by above mentioned classifiers are converted from distance to similarity score and are fused at matching score level for better performance of iris recognition.

3.4 Signature Verification

In biometrics terminology, the signature is a behavioral characteristic [19] of a person and can be used to identify/ verify a person's identity. The signature recognition algorithm consists of three major modules i.e., preprocessing and noise removal, feature extraction and computation of Euclidean distance. Offline signature acquisition is carried out statically, unlike online signature acquisition, by capturing the signature image using a high resolution scanner. A scanned signature image may require morphological operations like normalization, noise removal by eliminating extra dots from the image, conversion to grayscale, thinning and extraction of high pressure region.

Feature Extraction using Global and Local Features

The features of the signature images can be classified into two categories - global and local [20]. Global features include the global characteristics of an image. Ismail and Gad have described global features [21] as characteristics which identify or describe the signature as a whole. Examples include: width/height (or length), baseline, area of black pixels etc. They are less responsive to small distortions and hence are less sensitive to noise as well, compared to local features which are confined to a limited portion of the signature. In contrast to global features, they are susceptible to small distortions like dirt but are not influenced by other regions of the signature. Hence, though extraction of local features requires a huge number of computations, they are much more precise. However, the grid size has to be chosen very carefully. It can neither be too gross nor be too detailed. Examples include local gradients, pixel distribution in local segments etc. Many of the global features such as global baseline, center of gravity, and distribution of black pixels have their local counterparts as well. The difference/distance (D_{Sign}) between the two features sets are computed using weighted Euclidean distance measure.

3.5 Fusion

The different biometrics systems can be integrated at multi-classifier and multi-modality level to improve the performance of the verification system. However, it can be thought as a conventional fusion problem i.e. can be thought to combine evidence provided by different biometrics [16] to improve the overall decision accuracy. The multimodal biometric authentication system is being developed at multi-classifier and multi-modalities level. At multi- classifier level, multiple algorithms are developed and combined for traits like face, fingerprint and iris. The following steps are performed for fusion at classifier level:

S1: Given a query image as input, features are extracted by the individual recognizers and then an individual comparison algorithm for each recognizer compares the set of features and calculates the matching scores or distances corresponding to each recognizer for various traits.

S2: The scores/distances obtained in S1 are normalized to a common range between 0 to 1.

S3: These scores are then converted from distance to similarity score by subtraction from 1 if it is a dissimilarity score. For example the dissimilarity scores, in case of fingerprint recognition using reference point algorithm (D_{Ref}), iris recognition using Haar Wavelet (D_{Haar}) and Circular Mellin operator (D_{Mellin}) are converted to similarity scores (MS_{Ref}, MS_{Haar}, MS_{Mellin})

S4: The matching scores are further rescaled so that threshold value becomes same for each recognizer.

S5: Then the combined matching score is calculated by fusion of the matching scores of multiple classifiers.

$$MS_{Face} = \frac{MS_{EBGM} + MS_{KDDA}}{2}$$

$$MS_{Finger} = \frac{MS_{Ref} + MS_{MIN}}{2}$$

$$MS_{Iris} = \frac{MS_{Haar} + MS_{Mellin}}{2}$$

The multimodal biometric authentication system is developed by integrating four traits i.e., face, fingerprint, iris and signature at matching score level. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module. The same steps for fusion at classifiers level are followed for multiple modalities level i.e., matching scores is computed for each trait (face, fingerprint, iris and signature) followed by normalization to the common scale and distance to similarity score conversion for all the four traits. The matching scores are further rescaled so that the threshold value becomes common for all the subsystems. Finally, the sum of score technique is applied for combining the matching scores of four traits i.e., face, fingerprint, iris and signature. Thus the final score MS_{Final} is given by,

$$MS_{Final} = \frac{1}{4}\left(MS_{Face} + MS_{Finger} + MS_{Iirs} + MS_{Sign}\right)$$

where MS_{Face} = matching score of face, MS_{Finger} = matching score of fingerprint, MS_{Iris} = matching score of iris, and MS_{Sign} = matching score of signature. The final matching score (MS_{Final}) is compared against a certain threshold value to recognize the person as genuine or an imposter.

4. Experimental Results

The reliability of the proposed multimodal biometric authentication system is described with the help of experimental results. The system has been tested on a database of 250 individuals. The training database contains a face, iris, two fingerprint images and one or two signature image(s) for each individual. The face image has been taken under controlled environment using a digital camera. The face images of frontal view are obtained under different orientations and lightning conditions. The fingerprint images are acquired using optical sensor at a resolution of 500 dpi. The iris image is acquired using 3-CCD Camera and the signature is acquired on a custom made template. The multimodal system has been designed at multi-classifier and multi-modal level. At multi-classifier level, multiple algorithms/classifiers are combined to generate better results. At first experiment, the individual systems were developed and tested for FAR, FRR and Accuracy. Table 1 and Figure 1 shows FAR, FRR and accuracy of these systems.

Table 1 : The accuracy, FAR and FRR of Individual Recognizers

Trait	Algorithm	FAR %	FRR%	Accuracy
Face	EBGM	0.59	22	88.70
Fingerprint	Reference Point	11	6	91.05
Iris	Haar	3.42	8.45	92.50
Signature	Global and Local Features	10	8	91.00

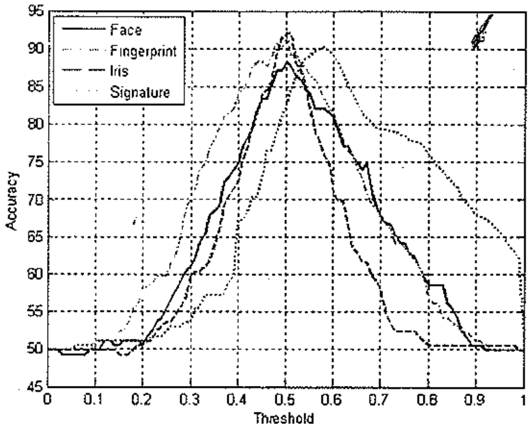

Figure 1 : Accuracy Graph for Individual Trait

In the next experiment, multiple classifiers are combined at matching score level for face, fingerprint and iris traits. For face recognition system, EBGM and Haar algorithms are combined together. Reference point and minutiae matching algorithms are combined for fingerprint recognition system whereas Haar and circular Mellin algorithms are combined for iris recognition. The results are given in Table 2 along with the graph (Figure 2).

In the last experiment, all the traits are combined at matching score level using sum of scores technique. The overall accuracy of the system is more than 97% with FAR and FRR of 2.46% and 1.23% respectively (as shown in Figure 3).

Table 2 : The Accuracy, FAR and FRR of Fingerprint and Iris after Fusion of Multi Classifiers

Trait	Algorithm	FAR %	FRR %	Accuracy %
Face	EBGM+KDDA	0.59	11.49	93.82
Fingerprint	Ref. Point + Minutiae	8	5	93.05
Iris	Haar + Circular MellinOperator	8.49	0.87	95.37

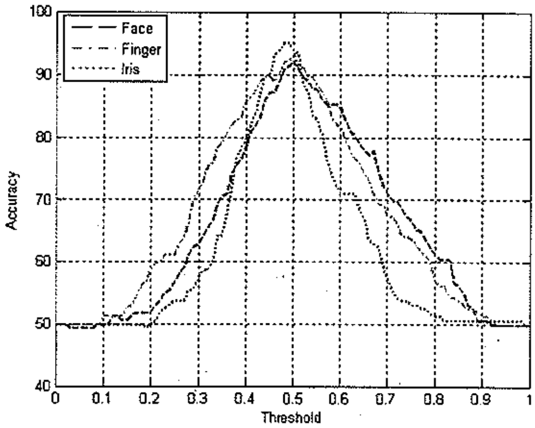

Figure 2 : Accuracy Graph Showing Fusion of Multi-Classifiers at Matching Score Level

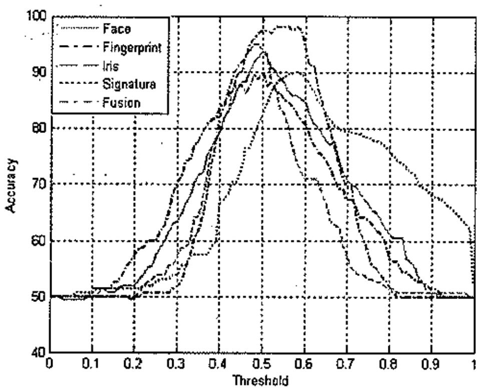

Figure 3 : Accuracy Curve Showing Performance of Multimodal Biometric Authentication System

5. Conclusion

Biometric systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of lack of biometric data for particular trait. Thus the individual scores of four traits (face, fingerprint, iris and signature) are combined at classifier level and trait level to develop a multimodal biometric authentication system. The performance table and accuracy curve shows that multimodal authentication system performs better as compared to unimodal biometrics with accuracy of more than 97%.

References

[1] L. Hong, A. Jain & S. Pankanti, *"Can Multibiometrics Improve performance, Proceedings of AutoID 99"*, PP. 59-64, 1999.

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

[3] A.S. Tolba & A.A. Rezq, *"Combined Classifier for Invariant Face Recognition"*, Pattern Analysis and Applications, 3(4), PP. 289-302, 2000.

[4] A. Ross, A.K. Jain & J.A. Riesman, *"Hybrid fingerprint matcher"*, Pattern Recognition, 36, PP. 1661–1673, 2003.

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

[6] S.C. Dass, K. Nandakumar & A.K. Jain, *"A principal approach to score level fusion in Multimodal biometric authentication system"*, Proceedings of ABVPA, 2005.

[7] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, *"On combining classifiers"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), PP. 226–239, 1998.

[8] G. Feng, K. Dong, D. Hu & D. Zhang, *"When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy"*, ICBA, PP. 701-707, 2004.

[9] I. Craw, D. Tock & A. Bennett, *"Finding Face Features"*, Proceedings Second European Conference Computer Vision, PP. 92-96, 1992.

[10] C. Lin & Kuo-Chin Fan, *"Triangle-based approach to the detection of human face"*, Pattern Recognition, 34, PP. 1271-1284, 2001.

[11] Juwei Lu, K.N. Plataniotis & A.N. Venetsanopoulos, *"Face Recognition Using Kernel Direct Discriminant Analysis Algorithms*, IEEE Transactions on Neural Networks", 14 (1), PP. 117-126, 2003.

[12] D.S. Bolme, J.R. Beveridge, M.L. Teixeira & B.A. Draper, *"The CSU Face Identification Evaluation System: Its Purpose, Features and Structure"*, Proceedings 3rd International Conference on Computer Vision Systems, 2003.

[13] N.K.Ratha, K.Karu, S.Chen & A.K.Jain, *"A Real-time Matching System for Large Fingerprint Database"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 18 (8), PP. 799-813, 1996.

[14] A.K.Jain, L.Hong & R.M.Bolle, *On-line Fingerprint Verification*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4), PP. 302-313, 1997.

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

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

[17] C. H. Daouk, L. A. El-Esber, F. D. Kammoun & M. A. Al-Alaoui, *"Iris Recognition"*, Proceedings of the 2nd IEEE International Symposium on Signal Processing and Information Technology, PP. 558-562, 2002.

[18] G. Ravichandran & M. M. Trivedi, *"Circular-Mellin Features for Texture Segmentation"*, IEEE Transactions on Image Processing Vol. 4, PP. 1629-1640, 1995.

[19] J. J.Brault & R. Plamondon, *"Segmenting Handwritten Signatures at Their Perceptually Important Points"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 15.

[20] M. Ammar, T. Fukumura & Y. Yoshida, *"A new effective approach for off-line verification of signature by using pressure features"*, 8th International Conference on Pattern Recognition, PP. 566-569, 1986.

[21] M. A. Ismail, S. Gad, *"Off-line Arabic signature recognition and verification"*, Pattern Recognition, 33 PP. 1727-1740, 2000.

Author's Biography

Nageswara Rao Thota received his M.Sc.(Mathematics) degree from Acharya Nagarjuna University, Guntur in 1997, M.Phil degree from Madurai Kamaraj University, Madurai, Tamilnadu in 2000. Now He has completed M.Tech Computer Science from Acharya Nagarjuna University in 2008. He is currently working as a faculty member in the department of Basic Engineering Sciences, Nalanda Institute of Engineering & Technology, Guntur. His research interests are in the areas of Image Processing and Content Based Image Retrieval.

Srinivasa Kumar Devireddy received the B.E. degree in Computer Science & Engineering from Karnataka University, Dharwad in 1992 and M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani in 1995. He is currently working as a faculty member in the department of Computer Science & Engineering, Nalanda Institute of Engineering & Technology, Guntur. He is a member of IEEE guided many projects in image processing and content based Image Retrieval. His research interests are in the areas of Biometrics, Image Processing and Content Based Image Retrieval.