Multi-Biometric Approaches to Face and Fingerprint Biometrics

Dr Shubhangi D C [1] **, Manohar Bali** [2]

[1,2] *Dept of Computer Science And Engineering Poojya Doddappa Appa College,Gulbarga*

Abstract- **This paper presents an efficient Face and Fingerprint recognition algorithm combining ridge based matching for the latter and Eigen Face approach for the former. We assume we recognize the Face first and then the fingerprint recognition in sequence.**

A fast fingerprint authentication method is proposed, based on the core and minutiae detection of the fingerprint. A bank of Gabor filters, orientated to different angles are applied to the image to clean it from noises that can result on false alarms or authentication mistakes. Our approach will be the extraction of the core using the flow field and determining the angle that each vector of the flow field has with respect to the horizontal.

Face is a complex multidimensional visual model and developing a computational model for face recognition is difficult. The paper presents a methodology for face recognition based on information theory approach of coding and decoding the face image. Proposed methodology is connection of two stages – Feature extraction using principle component analysis and recognition using the feed forward back propagation Neural Network.

.

Keywords - **Biometrics, Eigen Faces, Neural Network, Differential Minutia, Face Recognition, Fingerprint Recognition.**

I Introduction

Biometrics based personal identification techniques that use physiological or behavioral characteristics are becoming increasingly popular compared to traditional token-based or knowledge based techniques such as identification cards, passwords, etc. One of the main reasons for this popularity is the ability of the biometrics technology to differentiate between an authorized person and an imposter who fraudulently acquires the access privilege of an authorized person. Among various commercially available biometric techniques such as face, voice, fingerprint, iris, etc, the biometrics techniques offer a reliable method for personal identification, the problem of security and integrity of the biometrics data poses new issues. For example, if a person's biometric data (e.g., his/her fingerprint image) is stolen; it is not possible to replace it as compared to replacing a stolen credit card, identification card or password. Schneier points out that, a biometric based verification system can guarantee that the biometric data came from the legitimate person at the time of enrollment.

In order to promote the wide spread utilization of biometric techniques, an increased level of security of biometric data is necessary. The face is the primary focus of attention in the society, playing a major role in conveying identity and emotion. Although the ability to infer intelligence or character from facial appearance is suspect, the human ability to recognize faces is remarkable. A human can recognize thousands of faces learned throughout the lifetime and identify familiar faces at a glance even after years of separation. This skill is quite robust, despite of large changes in the visual stimulus due to viewing conditions, expression, aging, and distractions such as glasses, beards or changes in hair style.

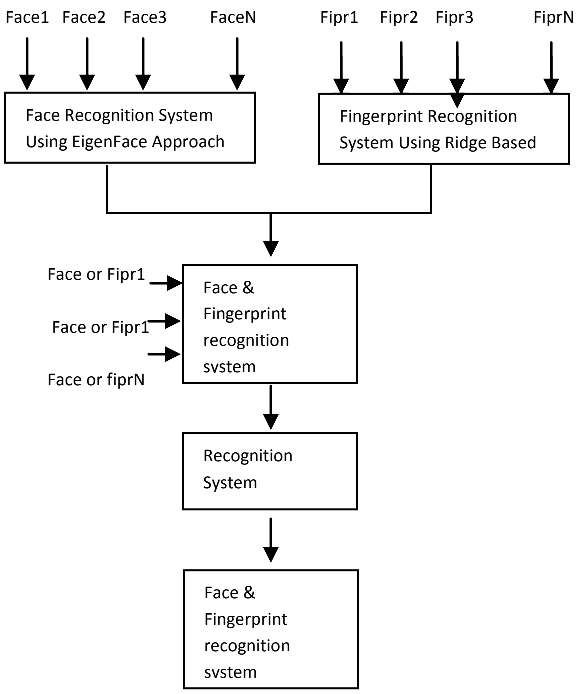
Although it is clear that people are good at face recognition, it is not at all obvious how faces are encoded or decoded by a human brain. Human face recognition has been studied for more than twenty years. Developing a computational model of face recognition is quite difficult, because faces are complex, multi-dimensional visual stimuli. Therefore, face recognition is a very high level computer vision task, in which many early vision techniques can be involved. For face identification the starting step involves extraction of the relevant features from facial images. A big challenge is how to quantize facial features so that a computer is able to recognize a face, given a set of features. Investigations by numerous researchers over the past several years indicate that certain facial characteristics are used by human beings to identify faces.

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

Neural networks have been trained to perform complex functions in various fields of application including pattern recognition, identification, classification, speech, vision and control systems.

II System Architecture

A proposed scheme of Face and fingerprint recognition in parallel is done in following steps.



A Using Eigenfaces to classify the face image.

Much of the previous work on automated face recognition has ignored the issue of just what aspects of the face stimulus are important for face recognition. This suggests the use of an information theory approach of coding and decoding of face images, emphasizing the significant local and global features. Such features may or may not be directly related to our intuitive notion of face features such as the eyes, nose, lips, and hair.

In the language of information theory, the relevant information in a face image is extracted, encoded as efficiently as possible, and then compared with a database of models encoded similarly. A simple approach to extracting the information contained in an image of a face is to somehow capture the variation in a collection of face images, independent of any judgment of features, and use this information to encode and compare individual face images.

In mathematical terms, the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images, treating an image as point (or vector) in a very high dimensional space is sought. The eigenvectors are ordered, each one accounting for a different amount of the variation among the face images.

These eigenvectors can be thought of as a set of features that together characterize the variation between face images. Each image location contributes more or less to each eigenvector, so that it is possible to display these eigenvectors as a sort of ghostly face image which is called an "eigenface".

Fig 1 Eigen Faces

B Training of Neural Network

Neural networks have been trained to perform complex functions in various fields of application including pattern recognition, identification, classification, speech, vision and control systems.

C Simulation of ANN for Recognition

New test image is taken for recognition (from test dataset and its face descriptor is calculated from the eigenfaces (M found before. These new descriptors are given as an input to every network; further these networks are simulated.

Compare the simulated results and if the maximum output exceeds the predefined threshold level, then it is confirmed that this new face belongs to the recognized person with the maximum output.

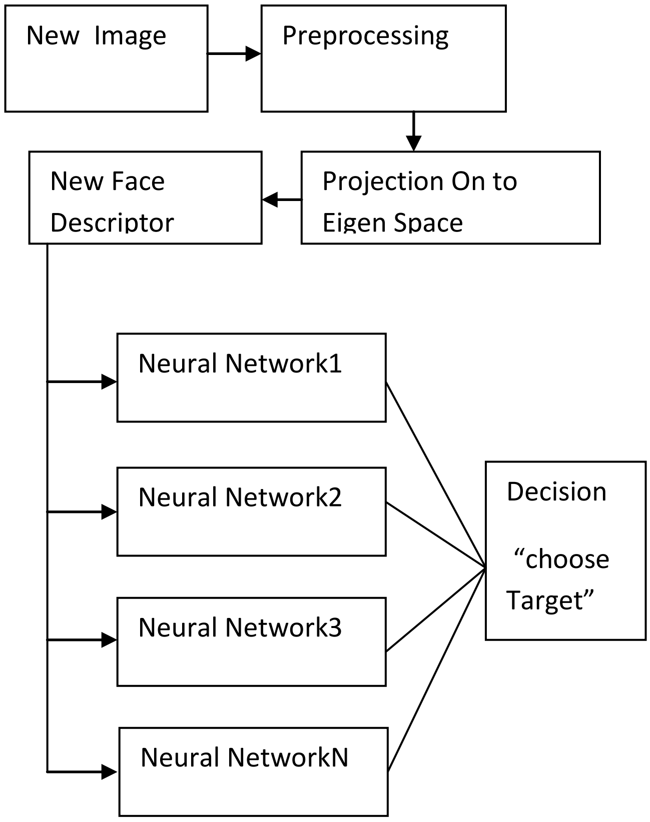


Fig 2 Testing of Neural Network

,

C Reconstruction of face Image using the extracted face descriptor

A face image can be approximately reconstructed (rebuilt) by using its feature vector and the eigenfaces as

$$\Gamma' = \Psi + \Phi f \qquad (1)$$

where

$$\Phi j = \sum_{j=1}^{M} wjuj \qquad (2)$$

Is the projected image.

Eq. (1) tells that the face image under consideration is rebuilt just by adding each eigenface with a contribution of w_i Eq. (2) to the average of the training set images. The degree of the fit or the "rebuild error ratio" can be expressed by means of the Euclidean distance between the original and the reconstructed face image as given in Eq. (3).

$$\text{Rebuild Error ratio} = \left\| \frac{\Gamma^2 - \Gamma}{\Gamma} \right\| \qquad (3)$$

It has been observed that, rebuild error ratio increases as the training set members differ heavily from each other. This is due to the addition of the average face image. When the members differ from each other (especially in image background) the average face image becomes messier and this increases the rebuild error ratio.

III Fingerprint Recognition

Fingerprint recognition (sometimes referred to as dactyloscopy) or palm print identification is the process of comparing questioned and known friction skin ridge impressions from fingers or palms or even toes to determine if the impressions are from the same finger or palm. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike (never identical in every detail), even two impressions recorded immediately after each other. Fingerprint identification (also referred to as individualization) occurs when an expert (or an expert computer system operating under threshold scoring rules) determines that two friction ridge impressions originated from the same finger or palm (or toe, sole) to the exclusion of all others.

A known print is the intentional recording of the friction ridges, usually with black printers ink rolled across a contrasting white background, typically a white card. Friction ridges can also be recorded digitally using a technique called Live-Scan. A latent print is the chance reproduction of the friction ridges deposited on the surface of an item. Latent prints are often fragmentary and may require chemical methods, powder, or alternative light sources in order to be visualized.

When friction ridges come in contact with a surface that is receptive to a print, material on the ridges, such as perspiration, oil, grease, ink, etc. can be transferred to the item. The factors which affect friction ridge impressions are numerous, thereby requiring examiners to undergo extensive and objective study in order to be trained to competency. Pliability of the skin,deposition pressure, slippage, the matrix, the surface, and the development medium are just some of the various factors which can cause a latent print to appear differently from the known recording of the same friction ridges. Indeed, the conditions of friction ridge deposition are unique and never duplicated. This is another reason why extensive and objective study is necessary for examiners to achieve competency.

A Fingerprint Patterns

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

B Patterns

The three basic patterns of fingerprint ridges are the **arch**, **loop**, and **whorl**.

· An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

· The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter.

· In the whorl pattern, ridges form circularly around a central point on the finger.

Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited

Arch   Loop (Right Loop)   Whorl

C Minutia features

Minutiae are major features of a fingerprint, using which comparisons of one print with another can be made. Minutiae include:

· Ridge ending - the abrupt end of a ridge

· Ridge bifurcation - a single ridge that divides into two ridges

· Short ridge, or independent ridge - a ridge that commences, travels a short distance and then ends

· Island - a single small ridge inside a short ridge or ridge ending that is not connected to all other ridges

· Ridge enclosure - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge

· Spur - a bifurcation with a short ridge branching off a longer ridge

· Crossover or bridge - a short ridge that runs between two parallel ridges

· Delta - a Y-shaped ridge meeting

· Core - a U-turn in the ridge pattern

D Image Enhancement

The performance of minutiae extraction algorithms and other fingerprint recognition techniques relies heavily on the quality of the input fingerprint images. Hong, Wan, and Jain proposed an effective method based on Gabor filters. Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains and Jain and Farrokhnia. Gabor filters is defined by a sinusoidal plane wave. The even esymmetric two-dimensional Gabor filter has the following form:

$$G(x, y; f, \theta) = \exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\delta_x^2} + \frac{y'^2}{\delta_y^2}\right]\right\}\cos(2\pi f x')$$

$$x' = x\sin\theta + y\cos\theta$$

$$y' = x\cos\theta - y\sin\theta$$

To apply Gabor filters to an image, the four parameters (? f, sigma(x), sigma(y)) must be specified. Obviously, the frequency of the filter is completely determined by the local ridge frequency and the orientation is determined by the local ridge orientation. The selection of the values sigma (x) and sigma (y) involves a tradeoff. [8]

E Fingerprint Matching Overview

The idea in this paper is to shorten minutiae extraction process in the verification of phase using a small sub-region of the live image. The minutiae extracted from the sub-region must be ‘trustable enough’ to authenticate a person accurately. In the past, a family of vectors were traced between a minutia and the minutiae found, but this process imply more computational time and the risk that the magnitudes of those vectors in a fingerprint with few minutia repeats in a fingerprint with more minutiae, and the process of verification would be affected.

Thinning **Biffurcation Extraction**

F Core Detection

Most of the approaches proposed in the literature for singularity detection operate on the fingerprint orientation image. The most commonly used reference point is the core point. A core point is defined as the point at which maximum direction change is detected in the orientation field of a fingerprint image or the point at which the directional field becomes discontinuous.An elegant and practical method for the core point extraction is based on the Poincare index. Such method is very sensitive to noise and cannot guarantee the detection of a core in type of fingerprints like the arch, that lack a discontinuous of its directional field. The method we are going to use is based on the computation of the orientation field described before, and the application of a filter to detect the maximum direction change of the ridge flow. This approach can even locate an imaginary reference point in an arch type fingerprint image.

The algorithm steps are as follow:

· Divide a fingerprint image, I, of NxN pixels into (N/w) x (N/w), where w is the grid size. Apply to the image the orientation field algorithm explained before, to obtain the matrix of angles *A'*.

· Compute the sin component ?(i , j) = sin(*A'* (i , j))

The sin component possesses an attractive characteristic that it reflects the local ridge direction. A perfectly horizontal ridge has a sin component = 0. On the other hand, the ridge's sin component = 1 if it orientates vertically. Due to the discontinuity property, the sin component value always changes abruptly in areas near a reference point. Because of such finding, the following procedure is added.

· Initialize a 2D array Bi and set all its entries to 0.

· Scan the sin component map in a top-to-bottom, left-to-right manner. For each sin component ?(i,j),

if *A'* (i , j) < *A* threshold and *A'* (i - 1, j) > p / 2 and *A'* (i + 1, j) > p / 2 then

i) Compute the difference D.
ii) Compute the Bi(i,j)

End

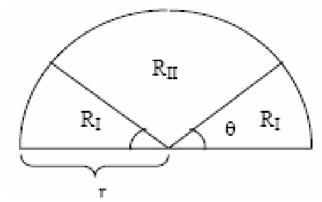
The difference D of the sin component in the region R1 and R2 is defined by a circular mask.

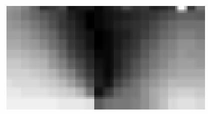
D =? R1? (i, j) - ? R2? (i, j)

The Bi[i][j] entry is used to compute the continuity of a Possible reference point candidate and is defined as:

Bi(i,j) = 1 ; if i = = 1

Bi(i,j) = Bi(i-1,j-1) + Bi(i-1,j) + Bi(i-1,j+1) ; otherwise





4 Experimental Results and Discussion

We assume that initially finger print system works and then the face recognition system in sequence as illustrated in below figures.We assume the environment in Matlab 7.

Startingly we add some fingerprints image to the database(Fig1 & Fig 2). Then we input the fingerprint image for recognition which shows the group number and the Euclidian distance(fig 3).

If the distance is below than 500 we recognize it as a match. Otherwise, we cross check it again if its Euclidian distance is greater than 500. If the input image matches exactly than the distance is equal to zero.

In Face recognition system, we calculate the Eigen faces present in the database (Sample) (Fig5).

Next we convert eigen faces into grey scale images. Finally we input an image to recognize if the input image matches the sample images, the system shows a match. Else it won't enter into the system.

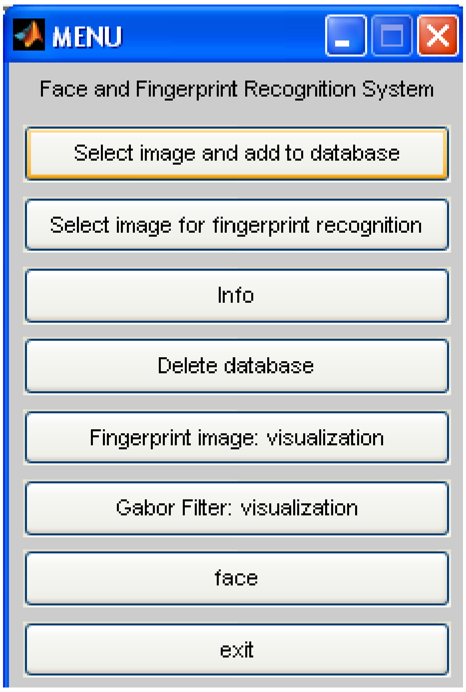


Fig 1 Adding Fingerprint Image To Database

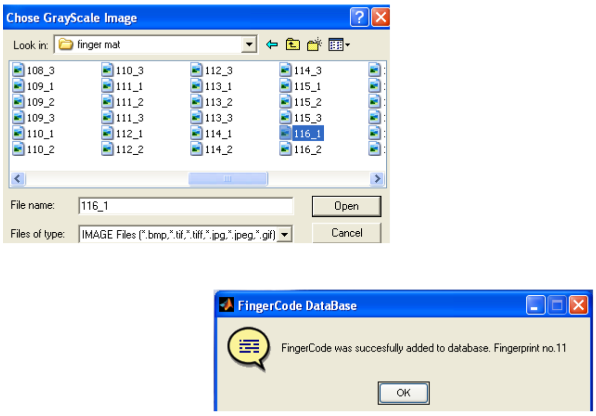


Fig 2 Choose Fingerprint Image

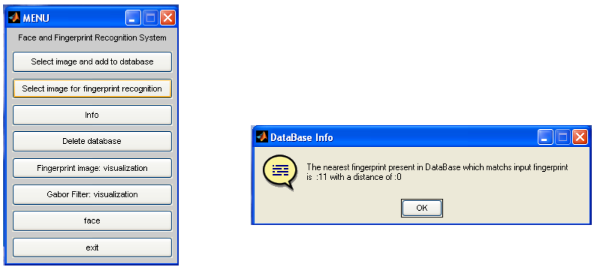


Fig 3 Selecting Input Image

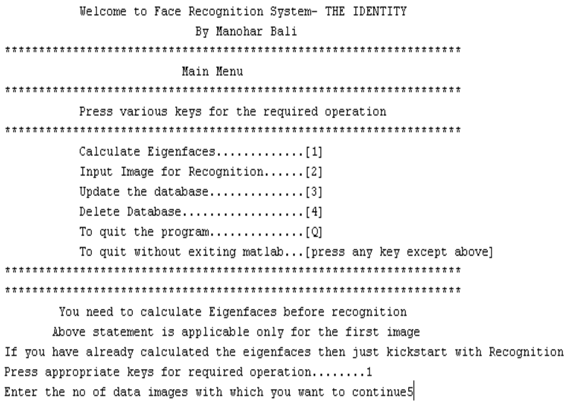


Fig 4 Calculate the Eigen Face of the database

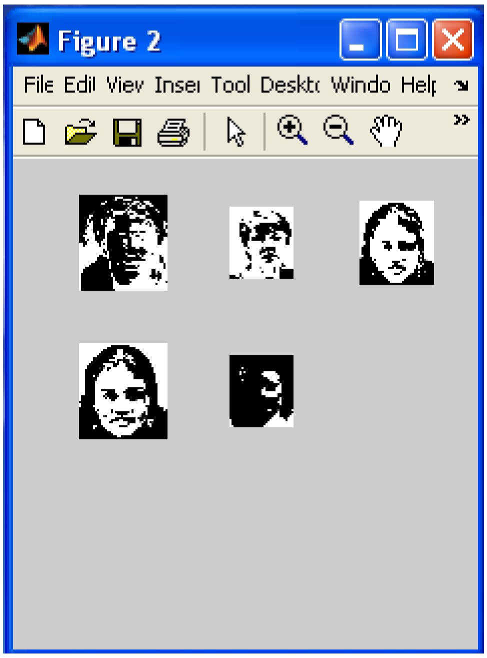


Fig 5 Convert them To grey scale image

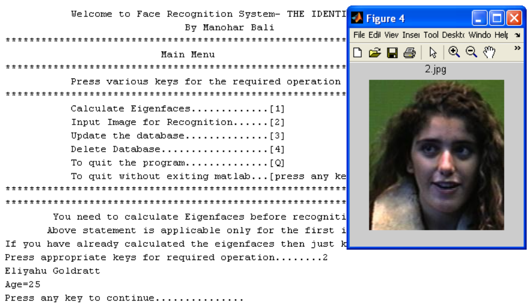


Fig 6 Match !

```
           Welcome to Face Recognition System- THE IDENTITY
                              By Manohar Bali
*******************************************************************
                          Main Menu
*******************************************************************
           Press various keys for the required operation
*******************************************************************
           Calculate Eigenfaces.............[1]
           Input Image for Recognition......[2]
           Update the database..............[3]
           Delete Database..................[4]
           To quit the program..............[Q]
           To quit without exiting matlab...[press any key except above]
*******************************************************************
*******************************************************************
        You need to calculate Eigenfaces before recognition
       Above statement is applicable only for the first image
If you have already calculated the eigenfaces then just kickstart with Recognition
Press appropriate keys for required operation........2
No matches found
You are not allowed to enter this system
Press any key to continue...............
```

Fig 7 No Match !!

IV. Conclusion

We have designed and built an identity verification system based on the fusion of face and fingerprint data. The significance of fusing these two biometrics is more than the improvement in verification accuracy. Enlarging user population coverage and reducing enrollment failure, two very important factors in practical applications, are additional reasons for combining face and fingerprint for verification.

References

[1] Yuille, A. L., Cohen, D. S., and Hallinan, P. W.,"Feature extraction from faces using deformable templates", Proc. of CVPR, (1989)

[2] S. Makdee, C. Kimpan, S. Pansang, “Invariant range image multi – pose face recognition using Fuzzy ant algorithm and membership matching score” Proceedings of 2007 IEEE International Symposium on Signal Processing and Information Technology,2007, pp. 252-256

[3] Victor-Emil and Luliana-Florentina, “Face Rcognition using a fuzzy – Gaussian ANN”, IEEE 2002. Proceedings, Aug. 2002 Page(s):361 – 368

[4] [Howard Demuth,Mark Bele,Martin Hagan, “Neural Network Toolbox”

[5] Kirby, M., and Sirovich, L., "Application of the Karhunen-Loeve procedure for the characterization of human faces", IEEE PAMI, Vol. 12, pp. 103-108, (1990).

[6] Bhanu Bir, Tan Xuejun, Computational Algorithms for Fingerprint Recognition. USA: Kluwer Academic Publishers, 2004

[7] Das, K. *Design and Implementation of an Efficient Thinning Algorithm*. Bachelor of Technology thesis, Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur. April 2000

[8] Jain Anil K et al. Biometrics: Personal Identification in Networked Society. Springer, 1999

[9] Lei, Guo et al. "Characteristic Preserving Binarization for Fingerprint Image". Image and Graphics. August 2007, Pages 401- 408

[10] O’Gorman L., “Overview of fingerprint verification technologies,” Elsevier Information Security Technical Report, Vol. 3, No. 1, 1998.