Human identification using Face and Fingerprint

M. Jasmine Pemeena Priyadarsini[1], G K Rajini[2], Shaik Naseera[3], N. Sardar Bash[4]
S. Sanjay Kumar[5], M. Karunagaran[6], Kalavagunta Chandra Shekara[7]
[1567]School of Electronics Engineering, VIT University,Vellore, India
[2]School of Electrical Engineering, VIT University,Vellore, India
[3]School of Computing Science and Engineering, VIT University,Vellore, India
[4]International Maritime College Oman, Sultanate of Oman

Abstract : Security systems are becoming an integral part of our environment, having a secure and accurate security system is of utmost importance. This paper suggests a combinational method which uses a faster algorithm, Kanade Lucas Tomasi (KLT) for quick verification and a two-step security system, face, Principal component analysis (PCA) and finger print for a more accurate verification

***Keywords-** Kanade Lucas Tomasi(KLT); Principal component analysis (PCA); Eigen face; feature tracking; Finger print verification ; Image representation; Face recognition.; Minutiae ; Gabo*

1. Introduction

One of the major reasons for not implementing facial recognition in security systems apart from smart phone lock screen and minimalistic security measures is due to the unreliability of the system. Most of the security systems are either security cards or finger print recognition systems, these at times can be a hindrance due to the time it takes to process multiple people.

This paper suggests a combinational security system which seeks to overcome the hindrance and also provide a more accurate security system. In order to process multiple people a fast tracking system is incorporated using Kanade Lucas Tomasi algorithm which fast tracks multiple faces and verifies whether the face is available in the database or not. This tracking recognition system is fast and fairy reliable and can be used as a first step verification in the security system. The idea of this system is quickly assess faces and determine if they are verified or not. After the first step verification system most institutions will need a more secure system for more sensitive areas, to cater to this need a combination of face and finger print recognition system is introduced to effectively and accurately access the person and provide access accordingly. Principal component analysis is the face recognition algorithm which is used to verify the face it uses a approximation method using Eigen faces. Along with this an additional finger print recognition system is used to verify the finger print of the person. When both the fingerprint and the face have to be verified in order to grant access the system becomes far more secure since it can't be faked using prints it also needs the face to verify and grant access.

This combination system saves time as well as provides a more accurate system for security. Create an effective security system which can identify individuals from a database for authentication, identification and screening purposes. The project aims to create three algorithms to provide security solutions for two different scenarios. One to allow fast and accurate face detection to authenticate a certain individual, the second scenario focuses on a more secure program which uses a combination of both face recognition and fingerprint recognition to create a more fail proof security system.

The paper is aimed to bring out the advantage of using a combinational system which can greatly improve the accuracy and reliability of a security system.Fig 1shows the block diagram upon which the paper is based on. This can also be incorporated in domestic security and other security needs.

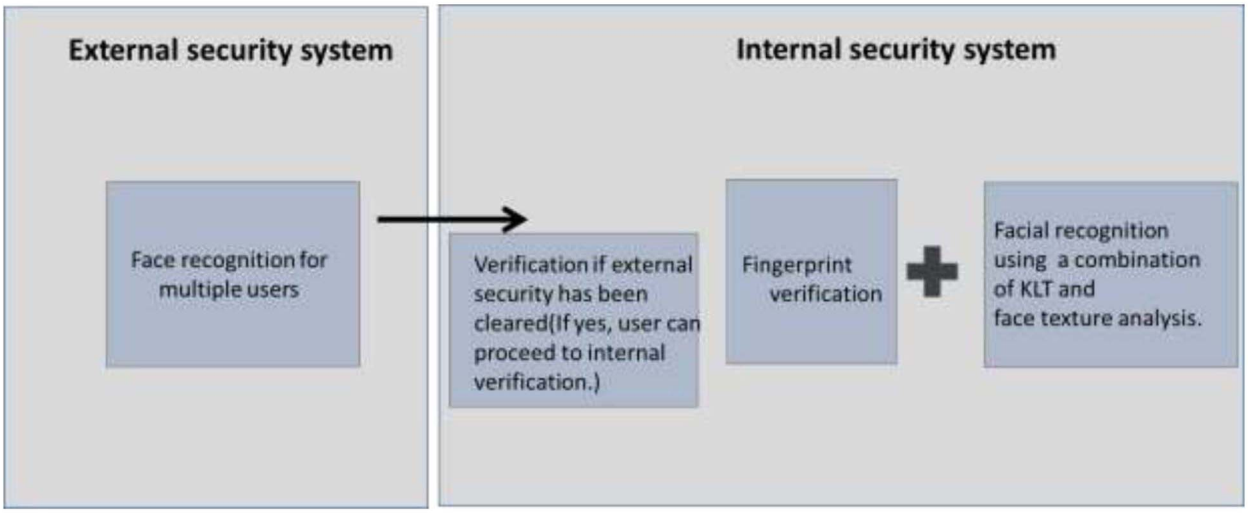

External security system
Internal security system
Face recognition for multiple users
Verification if external security has been cleared(If yes, user can proceed to internal verification.)
Fingerprint verification
Facial recognition using a combination of KLT and face texture analysis.

Figure 1. Block Diagram of the Two Step Verification System

Multiple user face recognition

For this purpose Kanade Lucas Tomasi algorithm is used. the Kanade–Lucas–Tomasi (KLT) feature tracker is an approach to feature extraction. It is proposed mainly for the purpose of dealing with the problem that traditional image registration techniques are generally costly. KLT makes use of spatial intensity information to direct the search for the position that yields the best match. It is faster than traditional techniques for examining far fewer potential matches between the images.

The KLT feature tracker is based on two papers: In the first paper, Lucas and Kanade developed the idea of a local search using gradients weighted by an approximation to the second derivative of the mage.

One-dimensional case

If h is the displacement between two images F(x) and G(x) = F(x+h) then the approximation is made that

$$F'(x)= ((F(x+h) - F(x))/ h) = (G(x) - F(x))/h \qquad (1)$$

The assumptions made are taken from KLT algorithm equations.

The KLT algorithm extracts feature points from an image it uses these points to map the image. These points are stored for comparison with other images. The database which holds all the difference. Fig 2, shows the output.

So that,

$$h = (G(x) -F(x))/ F'(x) \qquad (2)$$

A) The registration problem

The translational image registration problem can be characterized as follows: Given two functions F(x) and G(x), (2) representing values at each location x, where x is a vector, in two images, respectively, we wish to find the disparity vector h that minimizes some measure of the difference between F(x+h) and G(x), for x in some region of interest R.

$$\text{L1 norm} = \sum|F(x+h)-G(x)| \qquad (3)$$

$$\text{L2 norm}= \sqrt{}\sum|F(x+h) -G(x)|2 \qquad (4)$$

Negative of normalized correlation

$$(-\sum F(x+h)G(x))/((\sqrt{}\sum|F(x+h)2)(\sqrt{}G(x)|2)) \qquad (5)$$

The following equations (3),(4) and (5) show how the KLT algorithm chooses feature points to track.

B). KLT algorithm

Figure 2. a) KLT algorithm recognizing the face b) Feature points being assigned

These points are stored and used to identify the face from the database a separate function is used to compare all the pictures in the database and use its feature points as a comparison if the points match a viable match is established. Furthermore the image when cropped is much easier to recognize and the green background makes it easier for the algorithm to track points. This method is used to fast analyze images and recognize the authorized personnel.

3. Finger print verification

This algorithm is widely used for many security reasons. It is now majorly used in smartphones for theft reduction and control. The algorithms used for fingerprint is still retro based and has got minor corrections to its previous algorithms. We have tried to use both minutiae algorithm and Gabor filter for fast, secured and accurate image matching. The more secure internal system consists of a combination of face and finger print recognition system. Finger print verification system is one of the most reliable and secure system for a proper and viable authenticity model.

Core point aligning and positioning using Gabor filters.
Input image is provided and in step by step process we enhance the images for obtaining a high quality image.

Now, the image is divided into parts and background is removed from the given fingerprint image. It is applied by a simple block-wise variance approach, since background mostly has a small variance.

Image is first binary closed ("imclose"), then eroded ("imerode"), to avoid holes in fingerprint image and also undesired effect at the boundary. The image segmentation is continuously processed several times, up to a desired condition is satisfied. This is done in order to avoid undesired boundary effects between fingerprint and background. Satisfying condition: the enhanced image is divided into non-overlapping blocks of given sizes (32 x 32 (or) 64 x 64). The whole enhanced image is filtered with a complex filter. Let Cf max be the maximum value of the filtered image in the current region of interest (previously calculated according to some initial parameters). For each non-overlapping block we calculate the relative maximum Cf_rel. We finally consider a logical matrix F whose element (I,J) is equal to 1 if (I,J) is a block relative maximum and this value is equal or greater than a threshold value (usually 0.65*Cf_max in our simulations); F(I,J) is equal to 0 in all the other cases (i.e. if F(I,J) is not a block relative maximum or a block relative maximum smaller than the threshold value). If the number of non-zero elements of the logical matrix F is above a threshold value, the parameters for image segmentation are re-calculated and the whole process is repeated once again (complex filtering output does not vary, only the region of interest has been changed. Now, fast pixel-wise orientation field computation is performed.

To obtain a logical matrix, orientation field is used If the angle of the orientation is <= PI/2,Pixel (I, J) = 1t Then, the border of this logical matrix is obtained, in the region of interest of fingerprint image.

For a wide set of angles (…,PI/2-3*alfa, PI/2-2*alfa, PI/2-1*alfa, PI/2, PI/2+1*alfa, PI/2+2*alfa, PI/2 +3*alfa, …) alfa is an arbitrary angle.

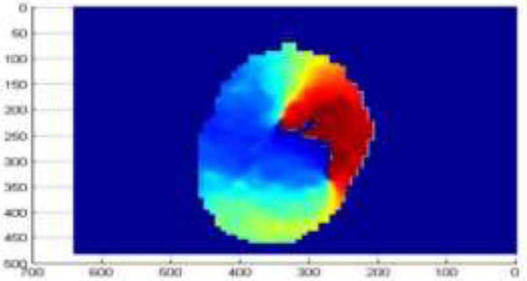


Fig. 3. Then we perform a fast pixel-wise orientation field computation

When a point is located they are taken and used for fingerprint matching.The points are further divided into parts and subsets which fall very close to each other. For N subsets, the individual subsets are provided with certain number of candidates.

The subsets with no. of candidates >=3 is used and the rest are ignored. The subset the core point the candidate with the greatest x-coordinate is taken. This is a good approximation in standard fingerprint image.

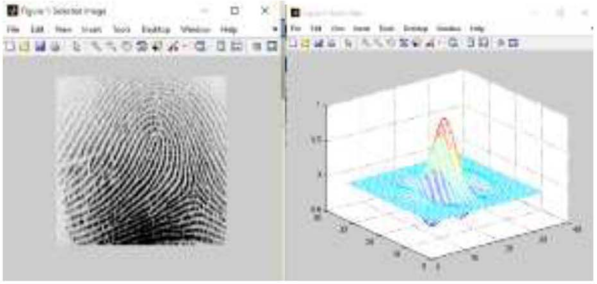


Fig. 4. a) Selected image b) Gabor filter output

The Fig. 5 shows Image visualization achieved by Gabor filter which converts the selected image into a Gabor output.

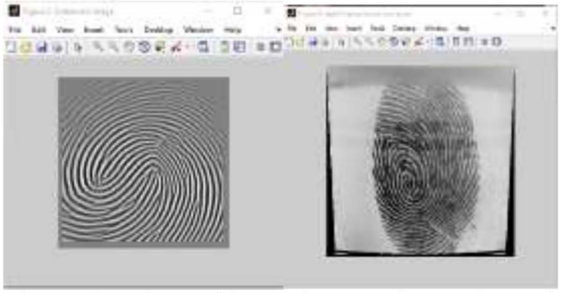


Fig. 5. a) Enhanced image b)Input fingerprint and core point

We can see from Fig. 5 The enhanced image for better recognition. Finger print recognition is the most accurate method of recognition but it can also be surpassed by using fake prints to overcome this we introduce another facial recognition system which requires both the face and finger print to match to provide authentication.

4. Principal Component Analysis

Principal component analysis (PCA) is a facial recognition technique. It is used to find principal component of given set of images, which uses an orthogonal transformation to convert a set of images into eigenfaces or principal component. There are two types of images, training image which is the set of image already present in the database and test image which is used to compare the image from training set.

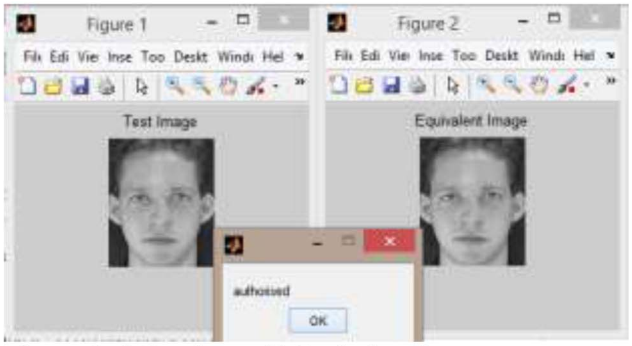
A. Training algorithm

Consider a set of face image of size *m* by *n*. Convert each face image from two dimensional to one dimensional vector. Find average face image vector which is equal to sum of all the image vector by number of images. Now, from the average face image vector subtract each face image vector and stack the vector to form a matrix of size S= [(m x n) x i], where i is number of images. For the new matrix formed, find covariance matrix which is the product of S(*)transpose(S).

Now, find eigenvector and eigenvalues for the above covariance matrix. As the size of the above covariance matrix is very huge, and computation of eigenvector is expensive. So, we calculate the eigenvector of the matrix which is the product of transpose(S)*S which will be of size i x I and find eigenvector. Then pre-multiply this eigenvector with S to get eigenvector of S*transpose(S).

B. Testing algorithm

Normalize every test image by subtracting average face image from test image. Find the weight of all the test images using the above process. Calculate Euclidean distance between the projection of test face image and training face image and choose the image with minimum error from the training set. If the test image is present in training set, then the authentication is confirmed. The Fig. 6. Shows the result.



authoised

Figure 6. a) Test Image b) Equivalent Image

5. Two step Verification system

The two step verification is classified as external and internal system. In external system, we are using only one face recognition algorithm. Which will take less time to process as compared to internal system. In internal system, we are using one face and fingerprint recognition, which will work together for verification. This system will also check whether you have cleared the external system also. The two algorithm used in this system have high precision.

6. Result and Analysis

The two part verification system is able to verify images at a fast pace and is also able to accurately identify the image and finger print in the second step of verification. The first algorithm is not completely perfect but the results obtain are accurate enough but since speed is of more priority a trade of has been made. The Second verification system is slower but the rate of accuracy is much higher. Together the system is able to identify the personnel correctly.

7. Conclusion

The paper discusses the viability of a combinational system, the results clearly show that this is more effective when it comes to speed and accuracy. Also the system gives priority to speed in the first verification system and to accuracy in the second.

Reference

[1] D. Zhang, Z. Zhou, and S. Chen, “Diagonal Principal Component Analysis for Face Recognition,” Pattern Recognition, vol 39, pp. 140-142, 2006.

[2] ORL database: http://www.camorl.co.uk.

[3] P.C. Yuen and J.H. Lai, “Face representation using Independent Component Analysis,” Pattern Recognition, vol. 35, no. 6, pp. 1247-1257, 2002.

[4] K. Lee, Y. Chung, and H. Byun, “SVM based face verification with feature set of small size”, Electronic letters, vol. 38, no.15, pp. 787-789, 2002.

[5] M. Turk and A. Pentland, “Face recognition using Eigenfaces,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 1991, pp.586-591.

[6] S. Chikkerur,C. Wu and Govindaraju, "A Systematic approach for feature extraction in fingerprint images", ICBA 2004

[7] Ravishankar Rao, "A taxonomy of texture description", Springer Verlag

[8] Kenneth Nilsson and Josef Bigun, “Localization of corresponding points in fingerprints by complex filtering”, Pattern Recognition Letters 24 (2003), 2135-2144

[9] Blanz, P. Grother, P.J. Phillips, and T. Vetter, “Face Recognition Based on Frontal Views Generated from Non-Frontal Images,”Proc. IEEE CS Conf. Vision and Pattern Recognition, pp. 454-461, 2005.

[10] Vladimir I Pavlovic, Rajeev Sharma, and Thomas S. Huang. Visual interpretation of hand gestures for human-computer interaction: a review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7):677–695, 1997.

[11] Y. Li, H. Ai, T. Yamashita, S. Lao, and M. Kawade, “Tracking in low frame rate video: A cascade particle filter with discriminative observers of different life spans,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 10, pp. 1728–1740, Oct. 2008.

[12] J.Savitha and Dr.A.V.Senthilkumar, “Efficient Method for Face Recognition from Pose and Expression,” International Journal of Advanced Research in Computer Science and Software Engineering., volume 3, Issue 10, October 2013.