Feature Selection Using Approximation Neighbourhood Strategy Using LU Factorization

K. Pavan Kumar

Asst. Professor, Dept. of IT, PVP Siddhartha Institute of Technology, Kanuru, India.

Abstract- In the olden days security have been provided by using Id cards, pass words called as a token based security. Authentication is the most important property in the real world. Based on the authentication only security will happen. Traditional authentication and security methods are not providing much security because of pass word sharing or stolen by pass words or shared by ID cards. Present days security has been provided based on finger prints, retina, and face. Because these features are unique so that security will be provided effectively. At the same time extracting the features is also very important. Features can be extracted by using traditional methods is not efficient for authentication because are all based on the deterministic process. Now a days for improving the accuracy of algorithms for authentication probabilistic and approximation methods are used for feature selection and extraction. In this paper face and finger can be considered for authentication. This paper can be organized into three ways. 1. Feature selection and extracting the features based on the probabilistic method Lower Upper Factorization (LU) 2. Fusion can be done based on the Principle component analysis 3. Features can be decoded by using Khatri Rao product 4. Distance between training and testing can be calculated using Mean square Error (MSE).

Key words- *Fusion, Probabilistic and Approximation methods, Principal Component Analysis (PCA), LU factorization, Mean Square Error*.

I. INTRODUCTION

For any algorithm modelling (Design) is the most important factor for accuracy and authentication in Biometric system. Once model is defined it is easy to test it in computers as opposed to physical experiment.

In traditional systems pin numbers are used for security. But if there is a problem with pin numbers because of forgotten or stolen by other persons similarly card based security is also. To solve these problems Biometric comes into picture to solve these problems. Now a days all the banking sectors, smart phones, security purpose biometrics are widely used for authentication.

A. Biometrics

Now a days most of the security models are designed with Biometrics [1,2,3]. Because the bio metrics are vary from person to person. No two people are having the same biometrics like face , finger, retina. These traits are used for security and authentication. But these are also having some restrictions even though these traits are much useful for authentication. Same time these features are not stolen or shared. For authentication use these features individually or combination of two or three traits and generate one feature set and stored it in the smart card and compare these with test features.

Biometric systems [4,2,3] can be modelled in two ways. One is detection mode, which can be used for detection of unknown person and second is certification mode in which detected person is certified as authenticated or not. But these systems are also having some limitations though these systems provide better solutions when compared to the traditional ways.

B. Multi Biometric systems

Generally at the time of beginning all the biometric systems are designed by using single features called unimodel biometric systems. But there are some limitations in the unimodal biometrics. Suppose face can be considered as a trait, twins are having similar features. In this case authentication can be done wrongly. Similarly fingers can be considered as tarits if any damage occur for the fingers authentication not done perfectly. At the same time at the time of capturing the Face or finger some noisy is added that will reduce the accuracy of our model.

By solving all these problems multi biometric systems can be used for authentication. Here face and finger or finger and retina or face and palm all these combinations can be used for modelling the systems. even though if any one of the trait is damaged other trait can be helpful for authentication. Now a days most of the systems are designed with multi biometric systems[2,5,6]. Aadhar cards are also having multi biometric systems.

The proposed system can be work in the following levels.

1. Feature extraction level: here features can be extracted using Lower Upper Factorization(LU Factorization).
2. Computational level: feature selection and feature extraction can be combined by using khatri-rao Product
3. Decision level: final decision can be done by comparing the stored features with testing features using distance metrics.

In this process first apply the pre processing for both the training images finger and face then perform the image fusion [7] by using principal component analysis. After apply the fusion features can be extracted using LU factorization. These features can be decoded for the security by using khatrirao Product and stored it in the memory. The same process can be done for the testing and compared with the stored data by using mean square error technique. Based on the distance decision can be taken.

II. FEATURE SELECTION AND EXTRACTION

Feature selection and extracting the features [13,14] from the images is a challenging method. There is number of algorithms exits in the literature. But each algorithm is having its limitation. Approximation techniques [15] are mainly used when the dimensionality of the set is low. Whenever apply the approximation methods features can be selected from the small subset of the vector spaces.

A. LUfactorization

Lower and Upper (LU) decomposition of a matrix is the multiplication of lower and upper triangle matrices. Sometimes it can also be considered as Gaussian Elimination.

Let A be a NxN matrix, it can be written as a product of lower(L) and upper (U) matrices as

$$LU=A$$

$$\text{i.e} \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & 0 \\ u_{31} & 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

It provides N^2 equations for $N^2 + N$ equations. These can be solved using crout's method. To solve this matrix equation

$$Ax=LU(x)=L(Ux)= b$$

First solve Ly=b for y. It can be solved by forward substitution

$$y_1 = \frac{b_1}{l_{11}}$$

$$y_i = \frac{1}{l_{ii}}\left(b_i - \sum_{j=1}^{i-1} l_{ij} - y_j \right)$$

For i=2....N . Now Solve Ux=y for x . It can be obtained by back substitution

$x_N = \frac{y_N}{u_{NN}}$

$$x_i = \frac{1}{u_{ii}}\left(y_i - \sum_{j=i+1}^{N} u_{ij}\, x_j \right)$$

Algorithm

Assign U=A, L=I

```
For k= 1:m-1
    For j=k+1 : m
        L(j,k)=  U(j,k)/U(k,k)
        U(j,k:m)=U(j,k) U(k, k:m)
    End
End
```

Once features can be extracted these features can be encoded by using the approximation reasoning technique khatrirao product [16].

III. IMAGE FUSION

Once pre processing is done the next step is to reduce the image dimensionality and perform the fusion. Here face and finger can be fusion[8,9] by using Principal Component Analysis(PCA)

A. PRINCIPAL COMPONENT ANALYSIS

Principal Component Analysis [10,11,12] is a mathematical method that convert unrelated variables to related variables and also it reduces the highest dimensionality sub space to lowest dimensionality new subspace.

It has the following steps

1. create a trained image data set and calculate the mean value of all the images
2. Measure the difference between mean and training images
3. Find the covariance matrix of the above step 2
4. Calculate the eigen vectors and eigen values of the above covariance matrix
5. Retrieve the largest eigen values and form the eigen faces
6. Find the weights of all the trained images by using this eigen faces and stored them in memory

The above process can be done for both the face images and finger images. Calculate the weights of face and finger images and merge these both weights and crate one single image called fusion image.

B. KHATRI RAO PRODUCT

Let A=(aij) and B=(bij) are two mtrices. The Khatri rao product can be derived as

$$A * B = \left(A_{ij} \otimes B_{ij}\right)_{ij}$$

Where $A_{ij} \otimes B_{ij}$ is of order $m_i p_i X n_j q_j$ and A*B is of order $(\sum m_i p_i) X (\sum n_j q_j)$ and it is a refined form of Kronecker Product.

IV. EXPERIMENTAL ANALYSIS

For the experimental Analysis we use the standard [17,18,19] data bases for testing the performance of the model. At the same time some realistic data collected through cam and finger print scanner are also used. But results shows better results on standard databases. In the verification process used the Mean Square Error(MSE)[20]. It can be calculate the difference between the training images and tested images. Let us consider training images as S and testing images as S^T, then the MSE between these two can be calculated as

$$MSE = \frac{1}{K}\sum_{i=1}^{k} S, S^T$$

The experiments can be done on the standard data bases for the key sizes 8x8,16x16,...,64x64. All these experiments can be done on 2GB RAM, Intel core i3 processor with 500GB HD.

IV.1 FALSE MATCH AND FALSE NON MATCH

If we want to check the performance of the system we need to check the false matching rate and false non matching rate. In the false matching rate the system will treat the correct input as wrong input. In the false non mating the system will treat incorrect as a correct. Based on these two things we can check the performance of any bio metric system. Both these errors can be calculate based on the percentages of matching with the threshold value d. The following table will shows the results obtained by changing the key values.

Table 1: Results for different key sizes

S.No	Key Size	MSE	
		Similar	Dissimilar
1	8x8	0.169890	0.135584
2	16x16	0.183512	0.064725
3	24x24	0.146473	0.088314
4	32x32	0.132550	0.091239
5	40x40	0.143469	0.079459
6	48x48	0. 104538	0.096204
7	56x56	0.117717	0.088881
8	64x64	0.121013	0.075503

Here we consider the threshold value d=0.091. Based on this threshold value false match and false non match can be calculated. For this threshold value all the similar images can be identified but for the key size 8x8 false matching rate can be identified. Because very less features are having for the key size 8x8 false matching can be detected.

V. CONCLUSION

In this paper we proposed a model for feature selection and feature extraction based on approximation neighbourhood strategy. In this feature selection and extractions can be done by LU factorization and extraction features can be fusion by using Principle Component Analysis and calculate the weights of training images by projecting on to the fusion image and decode these features by using khatri rao product and stored in memory. The same can be done for testing images and calculate the distance between training and testing images by using Mean Square Error. The algorithm works for all the key sizes except for the key size 8x8.

VI. ACKNOWLEDGEMENT

I gratefully acknowledge the funding agency, the University Grant Commission (UGC) of the Government of India, for providing financial support, to complete my paper, in the form of MRP-SEM/UGC-SERO

VII. REFERENCES

[1]. Samir Nanavati, Michael Thieme, and Raj Nanavati, Biometrics Indentity verification in the network World, Weily Tech Brief, 2002.
[2]. T. De Bie, N. Cristianini, R. Rosipal, Eigenproblems in Pattern Recognition, Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics, Springer-Verlag, Heidelberg, 2004
[3]. Jain, A.K.; Ross, A., Prabhakar, S. An Introduction to Biometric Recognition. IEEE Trans. Circuits Syst. Video Technol., 14, 4-20, 2004.
[4]. Mary Lourde R and Dushyant Khosla, Fingerprint Identification in Biometric Security Systems, International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, 852-855, 2010
[5]. Arun Ross and Anil K. Jain, Multimodel Biometrics: an Overview, 12th European Signal Processing Conference, 1221-1224,2004.
[6]. Tejas, J.; Sommath, D. Multimodal Biometrics: State of the art in Fusion Techniques. Int. J. Biometrics, 4, 393-417, 2009.
[7]. Deepak Kumar Sahu, M.P. Parsai, "Different Image Fusion Techniques-A Critical Review", International Journal of Modern Engineering Research (IJMER), vol. 2, no. 5, pp. 4298-4301, Sep.–Oct. 2012.
[8]. Shumin Liu, Jiaxuan Zhang, Jiajia Chen, "Multi-focus image fusion using Gaussian filter and dynamic programming", Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2017, pp. 1182-1185, 2017.
[9]. M. R. Metwalli, A. H. Nasr, O. S. Farag Allah, S. El-Rabaie, "Image fusion based on Principal Component Analysis and High-pass Filter", proceedings of IEEE/ICCES 2009 international Conference, DEC. 14-16. 2009.
[10]. Reham Gharbia, "Image fusion techniques in remote sensing", arXiv preprint arXiv:1403.5473,2014.
[11]. Metwalli, M.R, "Image Fusion Based on Principal Component Analysis and High-pass Filter", Computer Engineering & Systems. ICCES International Conference on,2009, pp. 63-70.
[12]. V.P.S. Naidu and J.R. Raol, "Pixel-level Image Fusion using Wavelets and Principal Component Analysis", Defenses Science Journal,2008, Vol. 58, No. 3, pp. 338- 352.
[13]. A. Jović , K. Brkić and N. Bogunović , "A review of feature selection methods with applications",
[14]. Rajkumar Goel , Vineet Kumar , Saurabh Srivastava , A. K. Sinha, "A Review of Feature Extraction Techniques for Image Analysis" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Special Issue 2, February 2017
[15]. P.Pudil, J.Novovičová N.Choakjarernwanit, J.Kittler, "Feature selection based on the approximation of class densities by finite mixtures of special type" Pattern Recognition, Volume 28, Issue 9, September 1995, Pages 1389-1398.
[16]. Shuangzhe Liu And Gotz Trenkler, "Hadamard, Khatri-Rao, Kronecker And Other Matrix Products" International Journal Of Information And Systems Sciences, Volume 4, Number 1, Pages 160–177.
[17]. Face databases – AT&T databases, www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
[18]. Face FERET Databases - http://www.face-rec.org/databases/
[19]. Fingerprint Databases - http://www.advancedsourcecode.com/fingerprintdatabase.asp

[20]. Izquierdo-Fuente, A.; del Val, L.; Jiménez, M.I.; Villacorta, J.J. Performance Evaluation of a Biometric System Based on Acoustic Images. Sensors, 11, 9499-9519, 2011.

Mr. K. Pavan Kumar received his M.Tech (CSE) degree from Acharya Nagarjuna University in 2008.He is pursuing Ph.D(CSE) from Acharya Nagarjuna University. Presently he is working as an Asst.Prof in PVP Siddhartha Institute of Technology. He has 10 years of teaching experience. His intersested areas are, Image Processing, Database Management , Computer Networks systems.