Research Article

Secure Data Access Computing Model on Mobile Cloud Data using Fusion of Finger Print and Face biometric authentication based on Discrete Combinational models

A.Amali Mary Bastina[1], Dr.N.Rama[2]

Abstract

Secure data access model on Mobile cloud data has received a lot of attention recently and is viewed as a promising trait. Biometric based authentication to secure access of the mobile cloud data have undergone fast development towards data protection and preventing malicious data threats. In this work, multimodal biometric based authentication technique as fusion model has been projected for data security. The key characteristics of finger print and face patterns include its uniqueness to each individual, unforgettable, non-intrusive and cannot be taken by an unauthorized person. In related methods, feature selection methods explore intrinsic finger print and face on single feature method, but their performance remains undesirable in terms of computational cost. However the extracted features from the both finger print and face pattern are huge with high redundancy. On employment of fusion concept on feature extraction techniques through weighted average strategies, equal error rate is minimized to obtain the optimum weight. In this paper, we propose a combinational model composed differential evolution technique to enhance the recognition of finger print and face patterns to authenticate the user towards data access. The system has been trained in selecting high relevant features on using the extraction techniques such as principle component analysis and linear discriminant analysis. Feature fusion carried out as concatenation on PCA and LDA technique using discriminant correlation analysis feeds the proposed feature selection models by optimal subset of features. The proposed system uses differential model to determine the less no of optimal features for multimodal authentication. Multimodal authentication performed using Multivariate linear regression on less no of optimal features. The analysis of empirical results shows that proposed system produces the best accuracy reflected by 100 percent accuracy on comparing with existing single model biometric authentication models. Further Proposed model has been evaluated and the results shows remarkable efficiency with existing state of art approaches.

Keywords: Finger print Recognition, Face Detection, Principle Component Analysis, Linear Discriminant Analysis, Multivariate Linear Regression, Differential Evolution, Discriminant correlation analysis

1. Introduction

[1]Department of computer Science, Loyolo College, Chennai
[2]Department of computer Science, Presidency College, Chennai

A.Amali Mary Bastina[1], Dr.N.Rama[2]

Currently, the rapidly advanced cloud-assisted mobile multimedia services motivate the owner to share their multimedia data via the cloud platform. However, the data security and privacy concerns would arise while enjoying the rich computation and storage resources for saving the overhead of mobile devices. In particularly, once the multimedia data is outsourced to the cloud, the data owner has to rely on the cloud server to enforce the access control. But the cloud server cannot be fully trusted and it would acquire the owner's privacy and recommend advertisement endlessly. A well adoptable approach is to encrypt the multimedia data before offloading it to the cloud. Whereas, the adoption of traditional cryptology or identity-based encryption might lead to complicated key distribution and management here are various biometric technologies currently available, such as iris, fingerprint, face, voice, and finger-vein.

Fusion of Fingerprint [1] and Face [2] are easy to be acquired and difficult to be forged because of existence inside. However, the clear observation of fingerprint and face patterns is affected by shades and changes in illumination, which causes the degradation of recognition accuracy. The existing feature-based methods for fingerprint and face recognition, such as local binary pattern [3] and Discriminative Binary Descriptor [4] have reduced recognition accuracy if noise caused by shades and changes in illumination in images are not properly corrected during pre-processing. Feature extraction method have been employed to explore intrinsic finger features but their remains undesirable on extraction of large features which leads to high redundancy and high computational cost. Taking aforementioned consideration into account, a new combinational model has been proposed in this paper.

In order to enhance the recognition rate of fingerprint and face based authentication system, fusion concept has been employed on feature fusion and fusion selection separately using various techniques. Initially four extraction techniques such as principle component analysis [5] and linear discriminant analysis [6] have been used to select high relevant features. Selected features undergo concatenation on PCA and LDA technique for feature fusion. Discriminant Correlation Analysis has been provided with Features of the biometric and fusion of multimodal biometric has been attained. Further feature selection models have been proposed to generate optimal subset of features using differential evolution. Finally multivariate linear regression has been used to prediction of the user towards data access on less no of optimal features.

The rest of this paper is organized as follows. Section 2 presents the related work based Local Binary Patterns and Discriminative Binary Descriptor. The proposed model and its components are discussed in section 3. The experimental results and analysis are discussed in section 4. Finally, the conclusion of this work and future improvement are presented in section 5.

2. Related works

In this section, finger vein recognition which has been carried through many feature based techniques such as Local Binary pattern and Discrete Binary Patterns has been discussed in detail on various aspects, detailed process description is as follows

2.1. Finger Print Recognition using Local Binary Patterns

In this model, finger print features are extracted with line patterns orientation on horizontally and vertically with most discriminative ability on texture representation. It is then

analysed with the discriminative ability of LBP histograms from different orientations[7]. Finally matching score-level fusion using sum rule is applied to achieve the final matching score for the recognition to have better performance.

2.2.Face Recognition using Discriminative Binary Descriptor

In this model, feature are extracted using LBP or Gabor descriptors, extracted feature has been mapped using discriminative feature learning method to enhance the discriminative ability of the local features extracted[8]. The discrimination of the feature is attained through multi-directional pixel difference vectors for each pixel and its neighbouring pixel. Finally finger vein recognition is carried using classifier on the histogram of the finger vein features.

3. Proposed model

The Proposed model for fusion of finger print and face authentication for secure access of mobile cloud data consist of following phases , such as feature extraction , feature reduction , feature fusion , Feature selection and finally feature classification on the optimal set of features. As initial step, finger print and face image acquired will undergo pre-processing includes the steps of binary thresholding, in-plane rotation compensation, and detection of finger and face region-of-interest. The overall flowchart of the multimodal authentication system for secure data access has proposed in this study is shown in Figure 1.
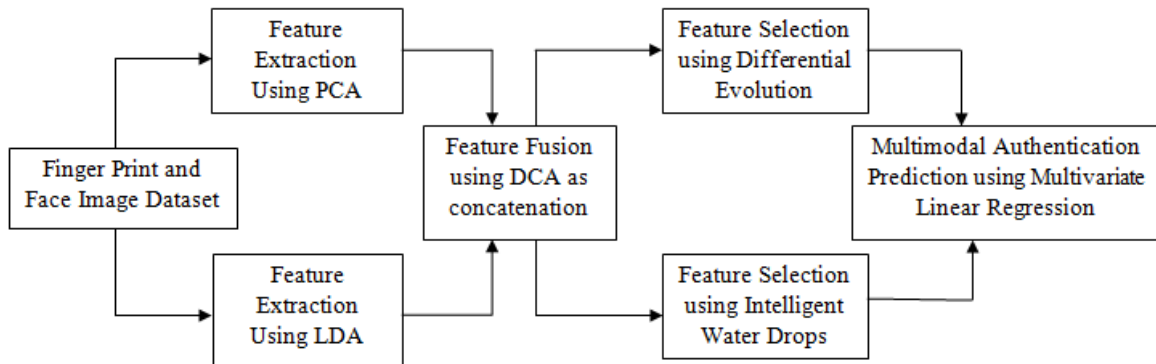

Figure 1: Architecture of the Proposed Combinational model for Multimodal Authentication

Pre-processed image will undergo feature extraction with four techniques for selecting relevant features. Those extracted feature will be concatenated for feature fusion. Concatenated feature employed to feature selection to select optimal subset features for multimodal authentication. Differential Evolution is to determine the less no of optimal features for fusion of biometric recognition. Finally Multivariate Linear Regression classifier is used for feature classification or recognition.

3.1.Feature Extraction

A.Amali Mary Bastina[1], Dr.N.Rama[2]

The feature extraction phase aims to extract the relevant features of fingerprint and face through following dimensionality reduction and normalization technique such as

3.1.1. Principle Component Analysis

Principal component analysis (PCA) is employed for feature extraction produces the most distinguishing features. PCA is implemented to generate a set of training data for the face and fingerprint image for recognition application that can be separated as far as possible and the same classes of patterns are compacted as close as possible. It is used for analyzing the image objects, identifying patterns and expressing the object to highlight their differences on face and fingerprint. It describes the object of the image in terms of variance.

Each principle component of the image describes the greatest amount of variance. Since the patterns can be hard to find in data of high dimension, PCA can find these patterns in the data by reducing the number of dimensions, without much loss of information. Finally it consists of feature vectors of the fingerprint and face patterns. Given M fingerprint or face images of size N x N, first represent each image to a 1D vector U. Vector composed of variance values. Variance for particular object X in a image is computed as follows

$$\text{var(x)} = \frac{\sum_{i=1}^{n} a(xi - x)(xi - x)}{n-1}$$

Covariance is computed for the X and Y object of the face and fingerprint which changes together with mean for secure data access is as follows

$$\text{Cov(x,y)} = \frac{\sum_{i=1}^{n} a(xi - x)(yi - y)}{n-1}$$

Covariance Matrix for secure data access is a N*N Matrix, where each element is given by

$$M_{ij} = \text{Cov(x,y)}$$

Eigen Vector of M_{ij} is a vector composed of principle feature set with values as eigen value for classification or recognition.

3.1.2 Linear Discriminant analysis

Linear discriminant analysis is used to identify an optimal solution vector as the best projection direction based on the fisher criterion function so that after projection in this direction of the feature fusion, the homogeneous samples in the original data set composed of face and fingerprint image are as close as possible and the heterogeneous samples are separated as far as possible. LDA algorithm is essentially looking for the effective transformation feature vector. The optimal solution fusion vector is obtained on reduction of the feature space through usage of scatter matrix on face and fingerprint. Given M fingerprint and face images of size N x N, first compute the mean vector for the image.

$$\text{Mean Vector for Single face object Mi } = \frac{1}{n} \binom{n}{k} x^k \sum_{x \varepsilon C}^{n} x, n_i$$

$$\text{Total Mean Vector for all finger print and face objects M} = \frac{1}{n} \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} N$$

Scatter Matrix for with Vector Scatters of face $F_w = \sum_{i=1}^{c} s_i \frac{ni}{n}$

Scatter Matrix for between vector Scatters $F_b = \frac{1}{2} \binom{n}{k} x^k \sum_{i=1}^{c} P_i P_j (k_i - k_j)(k_i - k_j)^T$

where $(k_i - k_j)$ is vector instance difference.

Covariance to the mean vector of fusion obtained is computed as $C_i = \frac{1}{n} \binom{n}{k} x^k \sum_{x \varepsilon C}^{1} (x - k_i)(x - k_i)^T$

Total Covariance of Scatter matrixes to yield optimal fusion feature set is $C_T = \frac{1}{N} \sum (k_i - k_j)(k_i - k_j)^T$

Important consideration of LDA technique is to minimize F_w while maximizing F_b on the data for securing. This can be achieved by maximizing the ratio $|F_b| / |F_w|$. Further feature weight gets maximized when eigenvectors of $f_b f_w$ form the column vector of the projection matrix of fingerprint and face fused for secure user authentication .

$$W = [W_1, W_2 \ldots \ldots W_{c-1}]$$

Where W_i are the eigenvectors of the fb and fw corresponding to the set of decreasing eigenvalues λ_i

Linear discriminant analysis has been employed to produce the optimal set of features through normalization on pair wise similarities of the correlated features extracted on the variance of the object and dimensionality reduction of face and fingerprint on estimating the linear combination of features on two or more vectors of multibiometric authentication.

3.2. Feature Level Fusion

The Primary focus of feature fusion for secure authentication is to combine relevant information from two or more feature vectors into a single one with more discriminative power than any of the input feature vectors of face and fingerprint biometric. Feature level fusion has been effective in combining perceptually salient image features extracted from the principle component analysis and linear discriminant analysis models in low dimensional space to yield concatenated feature using discriminant Correlation analysis [9] on vector associations in the reduced feature set of face and fingerprint. These two homogenous vectors are processed pragmatically to produce the fused vector of same order.

$$Y_{PCA} = [w_{PCA1}, w_{PCA2}, w_{PCA3} \ldots w_{PCAn}]$$

Where Y_{PCA} is the vein feature Vector extracted by the PCA

$$Y_{LDA} = [w_{LDA1}, w_{LDA2}, w_{LDA3} \ldots w_{LDAn}]$$

Where Y_{LDA} is the vein feature Vector extracted by the LDA

n is the number of training samples.

A new feature vector has been generated by serially combining or concatenating the Principle Component Analysis extracted features Y_{PCA} and corresponding linear discriminant Analysis extracted features Y_{LDA} on computation of the distance vector of d^{PCA} and d^{LDA} of each vector extracted. These two vectors are combined according to combination rule by maximizing pair wise correlation. In this work vector combination rule employed is considered as sum of the feature vectors

Combined Distance Vector by Mean Vector

$$d= \{\frac{d1PCA+d1LDA}{2} ... \frac{dNPCA+dNLDA}{2}\}$$

Combined Distance Vector by Appending the d^{PCA} Vector $+d^{LDA}$ Vector

$$d=\{d_1{}^{PCA},......,d_N{}^{PCA}, d_1{}^{LDA}, ... d_N{}^{LDA}\}$$

3.3. Feature Selection

Feature Selection is employed to determine the optimal features subset by eliminating the least important feature in order to increase the classification accuracy and to reduce the computation cost. In this work, a novel combinational model has been employed for feature selection using Differential Evolution model and Intelligent Water Drops model to generate the less no of optimal features for authentication of user for secure data access of mobile cloud data.

3.3.1. Differential Evolution Model (DE)

a. Description of Differential evolution

Differential Evolution is a stochastic population-based optimization algorithm for its efficient search capability of the feature using iterative process. It is mainly a four step process- Initialisation, Mutation, Recombination and Selection on the effective computation of the relevant feature for authentication of the user for data access in the mobile cloud. In the initialisation stage a set of population vectors normally equal to three times of data dimension are chosen in a uniformly random fashion [10]. Each of these parameter vectors undergoes mutation, recombination and selection to generate a trial vector. In mutation stage, for a given parameter vector, three parameter vector has been randomly selected that they distinct to each other on face and fingerprint fused vector. In recombination stage each element of the trial vector is generated depending on the value of cross over rate ε (0,1)

Computing objective Function

In this section, objective function of the Differential Evolution based feature selection has been constructed on basis of assumption of secure data access constraints in the mobile cloud. Initial assumption is that the good feature of the fusion vector should have least variation or distance value between the feature instances of the vector of face and fingerprint which considered as intra vector variation. The objective function for determining the intra vector variation of the finger and face image fusion is as follows

Objective Function of Feature selection $O^k{}_i(x_k) = \sum\limits_{k=0}^{n} \binom{n}{k} x^k a^{n-k} v_i{}^j(x_k) - v_i{}^j(x_{m+1}))$

Where $v_i^j(x_k)$ denotes the value of jth feature in the fusion vector and n is the number of the features in the fusion vector of the multimodal biometric. Each population of the DE algorithm as parameter vector which plays an important role in finding the optimum feature subset for authentication.

3.4. Feature Classification using Multivariate Linear Regression

The optimal feature subset obtained on feature selection has been classified using Multivariate Linear Regression classifier for authentication of the user for secure access in the mobile cloud. It is a non parametric method [12]. The method is considered to be the instance based as it predicts the class label for the feature sample by finding k closest points of the features selected. The k closest points are predicted by the distance weighting estimation to train feature samples as classes and predict the class label for the sample.

Let X is the optimal feature vector for which the nearest neighbour has to compute which represent the class; each class is T_{ij} may be estimated by distance measure of Euclidean distance. The distance estimation is carried out using Euclidean distance. Distance between the feature samples is T_{ij} which can be represented as

$$D_i(y)=\|y-T_{ij}\|^2$$

Where T_{ij} is Nearest Neighbour is to optimal feature vector for authentication of user.

Determine the category of the features such that category which represents most of the features. In this conclude T_{ij} belongs that particular category. In this category is collection of feature or its values to represent individual.

Euclidean distance between two features in fused vector is $E_d= \sqrt{(\Delta x)2 + (\Delta y)2}$

4. Experimental Analysis

In this work, fusion of multimodal biometric for secure access of mobile cloud data using a new combinational model has been experimented. The results for the experiment have been computed and its performance has been evaluated on various setting through K fold cross validation is described in detail in below sections.

4.1. Experimental Environment and Dataset Description

The experiment was carried out using MATLAB R2018 on window 7 Intel Core i7 CPU with operating frequency of 2.53G Hz and a usable memory of 8GB .The dataset used in this work was acquired from 100 subjects with 20 fingers and face from each subject which produces 500 samples. The images have been taken in three sessions, four images each time, at least one week between each session. The image in the database has 1024*780 resolutions and saved as a 12-bit bitmap.

4.2. Training

Images of 25 subjects among 100 subjects are used for training in the 10 fold validation [13]. Training of the fingerprint and face recognition model, the fingerprint and face

A.Amali Mary Bastina[1], Dr.N.Rama[2]

patterns extracted using single dimensional feature vectors through principle Component Analysis and Linear Discriminant Analysis. Table 1 and Table 2 compare the recognition performance of the existing method using PCA_LDA_Euclidean and PCA_LDA_Cosine as state-of-the-art methods. The state- of-the-art methods are compared by dividing them into non-training-based and training-based methods.

Table 1: Performance Comparison of Existing model using PCA –LDA-Euclidean distance

Threshold	0.1	0.2	0.01	0.03	0.05
Accuracy	0.969543	0.971698	0.968586	0.968586	0.968586
FRR	5.813953	2.970297	7.5	7.5	7.5
FAR	2.702703	0	0	0	
Precision	98.78049	97.0297	100	100	100
Recall	94.18605	97.0297	92.5	92.5	92.5

In this section, we present experiments to show the effectiveness of the proposed method in combining feature sets extracted from PCA and LDA model on fusion of multimodal biometric images. Since the adjacent pixels in an image are usually correlated [14], the information redundancy can be reduced by downsampling the feature images. In our experiments, the feature images are down sampled PCA and LDA by factor of n. In this n can be any number between 1 to 5.

Table 2: Performance Comparison of Existing model using PCA –LDA -Cosine

Threshold	0.1	0.2	0.01	0.03	0.05
Accuracy	100	100	100	100	100
FRR	0	0	0	0	0
FAR	0	0	0	0	0
Precision	100	100	100	100	100
Recall	100	100	100	100	100

N - Dimensional feature vector is extracted from each point and the final feature vector is constructed by concatenating the feature vectors of PCA and LDA. However Fused Feature vector [15] improves the recognition which further undergoes feature selection using DE and IWD. Initially parameter setting for the feature selection model using DE and has been tabulated as follows

4.3.Testing phase

For evaluating the performance of the proposed fingerprint authentication on portion of image considered as test image. So, to investigate the differences among fingers appear better than ring fingers in correct classification rate (CCR) but lower than other fingers in FAR[18]. Hence, the fingerprint images from different fingers are viewed as from different individuals in the processing.

4.4.Comparative Results of Feature Selection and Feature Recognition

In this section, the following experiments are conducted for acquired image. Furthermore, two vectors of the features are concatenated With DCA based feature fusion method. Our proposed algorithm exhibits more outstanding performance than the existing method. In table 3 provides the performance of finger and face authentication technique on various performances metric such as Accuracy, Recall and Precision.

Table 3: Performance comparison of classifier for multimodal Biometric authentication on optimal feature

Classifiers	Accuracy (%)	Recall (%)	Precision (%)	FRR (%)	FAR (%)
Euclidean	96	93.6	100	6.25	1.54
KNN	100	100	100	0	0

The MLR classifier is applied to feature selected using DE to recognize the fingerprint and face on the query images. In cosine, the number of neighbors (K) has been used in evaluating the performance accuracy of the mentioned models and is set by one in order to reduce the noise (increase the probability of close neighbor) of the classifier [20].

Table 4: Performance Comparison Based on IWD

Number of user	Number of training samples	Testing	Classification accuracy	Training Time	Testing Time
10	30	20	99	1.5	0.6
40	120	80	100	5	3.3

In addition, DE produced feature set provides the enhanced classification accuracy on employing MLR classifier for finger vein recognition. Performance evaluation for different subject is tabulated in table 5.

Table 5: Performance Comparison Based on DE

Number of users	Number of Training samples	Testing	Classification accuracy	Training Time	Testing Time
10	30	20	100	1.2	0.8
40	120	80	100	4.8	3.2

Compared to IWD, DE produces the better recognition results with Cosine distance classifier on recognition of user for authentication of secure data access in the mobile cloud environment on every aspect of the recognition performance measures.

Conclusion

A.Amali Mary Bastina[1], Dr.N.Rama[2]

We designed and implemented a new combinational model for Multimodal biometric authentication of user to secure data access in mobile cloud environment. In this work, enhanced multimodal authentication system has been obtained on inclusion of feature extraction techniques such as principle component analysis, linear discriminant analysis which produced high relevant features. Moreover those features are concatenated to generate feature fusion through discriminant correlation analysis. Further Differential Evolution has been derived as population based optimization technique to provide optimal subset of features for classification. Finally Multivariate Linear Regression classifier has been applied to categorize the obtained feature and to classify the test or query images. From the experiments, the DE are significantly improved the performance of classification with accuracy of 100% on user authentication.

References

[1] F. Liu, Y. Yin, G. Yang, L. Dong, and X. Xi, "Finger print recognition with superpixel-based features," in Proc. Int. Joint Conf. Biometrics (IJCB), Florida, USA, Sep./Oct. 2014, pp. 1–8

[2] J. Yang, Y. Shi, and G. Jia, "Face Image Matching Based on Adaptive Curve Transformation," Pattern Recogn., 2017.

[3] B. A. Rosdi, C. W. Shing, and S. A. Suandi, "Finger vein recognition using local line binary pattern," Sensors, vol. 11, no. 12, pp. 11357– 11371, 2011.

[4] J.-D. Wu and C.-T. Liu, "Finger-vein pattern identification using principal component analysis and the neural network technique," Expert Syst. Appl., vol. 38, no. 5, pp. 5423–5427, 2011.

[5]. Fan Z,Xu Y,Zhang D. Local linear discriminant analysis framework using sample neighbors. IEEE Transactions on Neural Networks, 2011, 22(7):1119-1132

[6]. Kumar, K. V & Negi, A "Novel approaches to principal component analysis of image data based on feature partitioning framework" in Pattern Recognition Letters, 29, 254–264, 2008

[7]. Shazeeda and Bakhtiar Affendi Rosdi "Finger Vein Identification based on the Fusion of Nearest Neighbor and Sparse Representation based Classifiers" Indian Journal of Science and Technology, Vol 9, 2016

[8]. Haiying Liu; Lu Yang; Gongping Yang; Yilong Yin "Discriminative Binary Descriptor for Finger Vein Recognition"IEEE Access, Vol.6, 2017

[9]. Mohammad Haghighat,Mohamed Abdel-Mottaleb, Wadee Alhalabi "Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition" in IEEE Transaction on information forensic and security,2016

[10]. Kingshuk Chakravarty, Diptesh Das, Aniruddha Sinha, Amit Konar "Feature Selection by Differential Evolution Algorithm - A Case Study in Personnel Identification"in IEEE Congress Evolutionary Computation, 2013

[11]. Hamed Shah-Hosseini"Intelligent water drops algorithm: a new optimization method for solving the multiple knapsack problem" in International Journal of Intelligent Computing and Cybernetics, 2008

[12] N. a. Samsudin and A. P. Bradley, "Nearest neighbour group-based classification," Pattern Recognition, vol. 43, no. 10, pp. 3458-3467, Oct. 2010.

[13] J. Chai, H. Liu, B. Chen, and Z. Bao, "Large margin nearest local mean classifier," Signal Processing, vol. 90, no. 1, pp. 236-248, Jan. 2010.

[14] A. M. Martinez and A. C. Kak, "PCA versus LDA," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 23, no. 2, pp. 228– 233, 2001

[15] C. Liu, and Y. Kim, "An efficient finger-vein extraction algorithm based on random forest regression with efficient local binary patterns," in Proc. Int. Conf. Image Process., Phoenix, spet. 2016, pp. 3141–3145

[16] J. Yang, Y. Shi, and G. Jia, "Finger-vein Image Matching Based on Adaptive Curve Transformation," Pattern Recogn., 2017.

[17] G. Yang, X. Xi, Y. Yin, "Finger vein recognition based on (2D)2 PCA and metric learning," BioMed Research International, vol. 2012, no. 2012, pp. 324249-324258, May.2012.

[18] H. Qin, L. Qin, C. Yu, "Region growth-based feature extraction method for finger-vein recognition," Optical Engineering, vol. 50, no. 5, pp. 057208-057208, May.2011

[19] N. Miura, A. Nagasaka, T. Miyatake, "Extraction of finger-vein patterns using maximum curvature points in image profiles," IEEE transaction on Information and Systems, vol. 90, no. 8, pp. 1185-1194, Aug.2007.

[20] H. C. Lee, B. J. Kang, E. C. Lee and K. R Park,"Finger vein recognition using weighted local binary pattern code based on a support vector machine," Journal of Zhejiang University SCIENCE C, vol. 11, no. 7. pp. 514-524, Jul. 2010.