FEATURE SELECTION IN MULTIMODAL AUTHENTICATION USING LU FACTORIZATION WITH CSEAM MODEL

Y Suresh,K Pavan Kumar, PESN Krishna Prasad, BDCN Prasad

Prasad V. Potluri Siddhartha Institute of Technology,
Kanuru, Vijayawada-7, India

Abstract

Multimodal authentication is one of the prime concepts in current applications of real scenario. Various approaches have been proposed in this aspect. In this paper, an intuitive strategy is proposed as a framework for providing more secure key in biometric security aspect. Initially the features will be extracted through PCA by SVD from the chosen biometric patterns, then using LU factorization technique key components will be extracted, then selected with different key sizes and then combined the selected key components using convolution kernel method (Exponential Kronecker Product - eKP) as Context-Sensitive Exponent Associative Memory model (CSEAM). In the similar way, the verification process will be done and then verified with the measure MSE. This model would give better outcome when compared with SVD factorization[1] as feature selection. The process will be computed for different key sizes and the results will be presented.

KEYWORDS:

Feature selection, LU factorization, CSEAM Model, PCA by SVD, Exponential kronecker Product (eKP), Multimodal Authentication.

1.INTRODUCTION

In recent scenario, agent biometric data verification is one of the critical tasks in the access control that performs the major building block of security. User identification is traditionally based on something that user knows (PIN/Password) and user has(Key/Token/Smart Card). But, these traditional methods can be forgotten, disclosed, lost or stolen. Apart from these strategies, failure rate is to differentiate between an accredited and unaccredited person [12].

Biometrics [4] is a scientific discipline that involves methods of identity verification or identification based on the principle of measurable physiological or behavioural characteristics such as a fingerprint, an iris pattern, palm, vein or a voice sample. In the analysis of security aspect, human patterns are unique. The primary advantage of multimodal authentication strategies

over other approaches of authentication is to process/ combine two or more user patterns with the use of psychological/behavioural patterns.

Nowadays, the biometrics patterns has been adopted throughout worldwide on a large scale and used in different sectors of public/private organizations. As specified in [12], biometric pattern authentication is a layered model consists of identification mode and verification mode [2, 3, 4] and the identification process starts with the enrolment process and consists of Acquisition: Acquisition is the first step in biometric authentication system. Using input device User's sample is obtained; Creation of the characteristics: After first step, biometric measurements are processed. The numbers of biometric samples depends upon the technology that we are using. Sometimes, single metric is sufficient, but most of the cases multiple patterns are required. By using these patters features are extracted; Storage of the characteristics: After feature extraction the feature patterns are stored in a card/database server/on a workstation/directly on authentication terminal.

After enrolment of the user, the user can use the system for successful authentications or identifications. The verification/testing process takes the following steps:

1. Acquisition(s): Biometric measurements should be acquired in order to make comparison with parent patterns.
2. Creation of new characteristics: New characteristics are created from the previous step.
3. Comparison: Currently computed characteristics are computed with the characteristics obtained in the previous step.
4. Decision: The final step in the test phase is the yes/no decision based on a threshold.

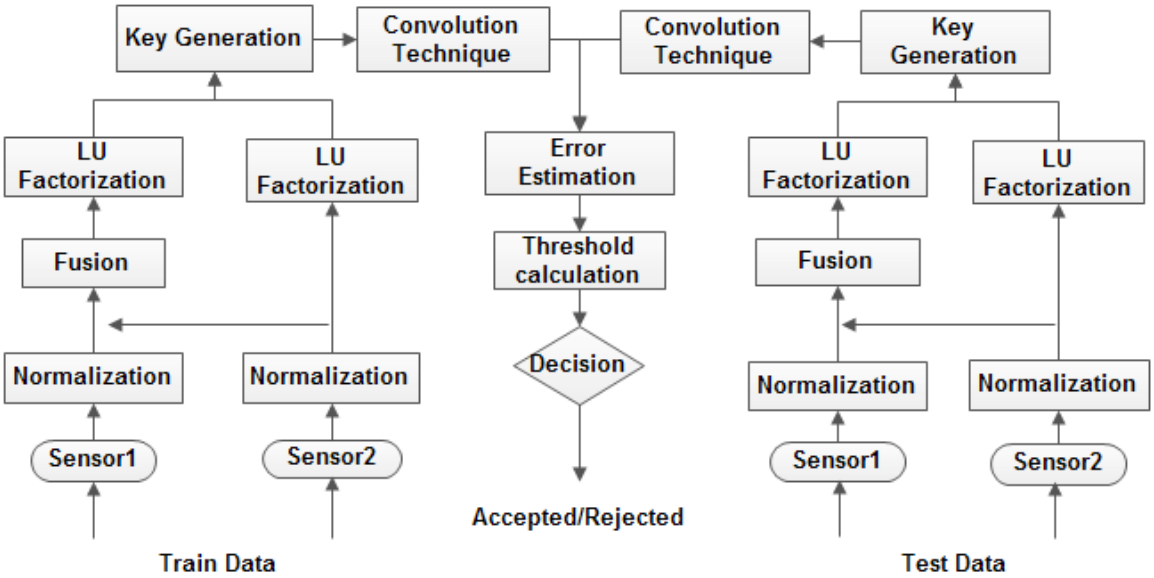
2.MULTIMODAL AUTHENTICATION SYSTEM

In multimodal authentication system, user has to enrol two to three patterns for identification/verification. Such patterns may be noise in capturing and may lead to more error prone. In order, to resolve the noise/ inconsistency, vector logic based models have been considered for minimizing the error rate.

From author's perspective, different strategies, methodologies and models have been proposed for multimodal systems, some of them may be, the user authentication based on speech and face patterns [5] is one of the first multimodal biometric system. Brunelli and Falavigna[5] for normalization and weighted geometric average for fusion of voice and face biometrics that uses hyperbolic tangent (tanh) and also they proposed a hierarchical combination scheme for a multimodal identification system. Kittler et al. [6] conducted with different fusion strategies for human face and voice patterns, including statistical and algebraic metrics. Kittler et al. [6] concluded that the algebraic sum metric is not significantly affected by the statistical estimation errors and covers its superiority and importance. Hong and Jain [7] proposed a multimodal system fingerprint pattern satisfaction is applied after pruning the datasets via face pattern matching. Ben-Yacoub et al. [8] considered several fusion strategies, such as tree classifiers, multilayer perceptions and support vector machines for face and voice biometrics. Ross and Jain [9] fusion the traits of biometric patterns- fingerprint, face and hand geometry with sum, decision

tree and linear discriminant approaches. The authors concluded that sum rule performs outstanding when compared with others.

From these observations, vector logic approach is to be considered for multi-modal biometric



authentication system based on facial and iris pattern. In this paper, both face images and fingerprint patterns are chosen due to their complementary characteristics, physiology, and behaviour.

3.PROPOSED MODEL

The effectiveness of biometric system using two level multimodal authentication problems are discussed in [1]for encoding and decoding of biometric patterns. At level one, input patterns are normalized with PCA by SVD and then keys will be selected using LU factorization from the extracted patterns after processing sensed data with PCA by SVD, at level two using

computational model (CSEAM model [1]),the generated keys will fusion through LU factorization, and at level three the decision process can be analyzed using error estimation strategies. An overview of the computational framework for the proposed model is described in the Fig. 1.

Figure 1. Framework of the Proposed Model

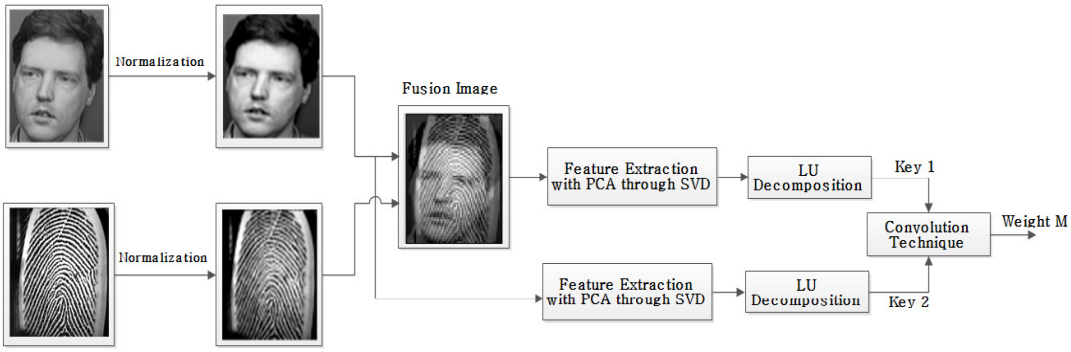


Figure 2. Black diagram of the Proposed Model.

3.1.Feature Extraction Using PCA by SVD

3.1.1 Principal Component Analysis (PCA)

In PCA[10], the directions of the data patterns is the most variation, that is the eigen vectors corresponding to the largest eigen values of the covariance matrix, and project the data patterns onto these directions that might get rid of important non-second order information by PCA. If the matrix of eigen vectors sorted according to eigen value by $\tilde{U}$, then PCA transformation of the data as $Y = \tilde{U}^T X$. The eigen vectors are called principle components [11]. By selecting the first d rows of Y, then the projected data is from n down to d dimensions.

3.1.2 Spectral decomposition of a square matrix:

Any real symmetric matrix A of size mxm may be decomposed uniquely as [10]

$$A = U \Lambda U^T$$

Where U is an orthonormal matrix and it satisfies

$$U^T U = I \text{or} \sum_k U_{ki} U_{kj} = \delta_{ij}$$

and Λ is a diagonal matrix . The eigen vectors of matrix A are columns of the matrix U and the eigen values are the diagonal elements of matrix Λ.

3.1.3 Singular Value Decomposition:

A matrix A of size mxn can be decomposed as [10]

$$A = UDV^T$$

U is a column orthogonal matrix of size mxn and its columns are eigen vectors of AA^T

$$\text{ie} \quad AA^T = UDV^TVDU^T = UD^2U^T$$

V is a orthogonal matrix of size nxn and its columns are eigen vectors of A^TA

$$\text{ie} \quad A^TA = VDU^TUDV^T = VD^2V^T$$

D is a diagonal matrix of size nxn called singular values.

If $U = (u_1u_2 \ldots\ldots u_n) and V = (v_1v_2 \ldots\ldots v_n)$ then

$$A = \sum_{i=1}^{n} \sigma_i u_i v_i^T$$

3.1.4 PCA by SVD:

The main advantage of the PCA by SVD is to apply the projection of the data on the principal components. So the best features will be extracted with less computational complexity. i.e. Let X be a matrix, decompose it by using SVD [10] is

$$X = U\Gamma V^T$$

and the covariance matrix as

$$C = \frac{1}{n}XX^T = \frac{1}{n}U\Gamma^2U^T$$

In this case U is a nxn matrix. The SVD[10] orders the singular values in descending order. If n<m , the first n columns in U corresponding to the sorted eigen values of C and if m$\geq n$, the first m corresponds to the sorted non-zero eigen values of C. The transformed data patterns can thus be written as

$$Y = \tilde{U}^TX = \tilde{U}^TU\Gamma V^T$$

Where $\tilde{U}^T U$ is a matrix of size nxm which is one on the diagonal and zero everywhere else.

4.FEATURE SELECTION USING LU FACTORIZATION

An intuitive models described, where the stimulate association of a matrix are dependent on the context of multiplicative vectorial logic. In this context a remarkable operation that transforms the real matrix over the truly computing data into a triangular matrix. This transformation promoted by the context leads to the LU Decomposition of a matrix representation, which is a mathematical method in the field of Image Processing and signal processing.

The meaningful event in the representation is the activity of the large group of data patterns, naturally represented by high dimensional vectors or diodic matrices. These representations are processed by associative memories (association of input-output pattern pairs) which store the information distributed and superposed over coefficients.

In this paper, the associative memory is computed using the keys which are generated from the fusion patterns by using LU factorization,

$$\mathbf{key1} = \mathbf{LU(A)} = \mathbf{P_A^T L_A U_A}$$

$$\mathbf{key2} = \mathbf{LU(B)} = \mathbf{P_B^T L_B U_B}$$

Where A and B are fusion patterns of two pair biometric samples (face and finger print). The fusion is done by using PCA. The importance of this factorization is here to extract the best features by eliminating noise and lighting effect using Gaussian-distribution models. In the process of computation the exponential kronecker product as associative memory combines the two keys from LU factorization and generates a memory representation M over K, where K is the Kth order kernel that uses Kronecker product as convolution product.

$$\mathbf{M^{(k)}} = \sum \mathbf{g_i (key1_i \otimes key2_i)^T}$$

Where, g=$\sum \mathbf{A_i}$. In this associative model, the memories models are based on a matrix over a multiplicity of vector associations are super imposed.

In general, A⊗B represents the Kronecker product.

$$\mathbf{M^{(k)}} = \sum_{k}' \mathbf{A_i [A_i \otimes \sum_{j(k)}' B_j]^T}$$

Where A is the one key pattern of one fusion set and B is another key patterns of the second fusion set, with i^{th} order convolution.

5.EXPONENTIAL KRONECKER PRODUCT

5.1. Exponential Kronecker Product (eKP):

The exponential function [13] possesses some specific properties in connection with tensor operations. Assuming that A and B are the two matrices, then the eKP[1] is described as:

$$\mathbf{e^A \otimes e^B} = \frac{\mathbf{A^m \otimes B^n}}{\mathbf{m!n!}}$$

The eKP [13,14,15] is having excellent properties that imply the concept of vector logic. The properties are as:

$$e^{A} \otimes e^{B} = \left(e^{A^{T}} \otimes e^{B^{T}}\right)^{T}$$

$e^{A} \otimes e^{B} = e^{A \oplus B}$, is a special property of kronecker calculus.

$$e^{(A \otimes B)} = e^{A} \otimes e^{B}$$

In this paper, the ***eKP*** is represented as Context-Sensitive Exponent associative memory model (CSEAM).

6.DECISION STRATEGY - MSE

6.1. Decision Strategy

In this strategy, the Mean Square Error (MSE) is as for verification of proposed framework with the support of CSEAM model at the training and testing levels.

Mean Square Error

The Mean Square Error (MSE) of an estimator $\hat{X}$ of a parameter X is the function of X defined by $E(\hat{X} - X)^{2}$ and it is denoted as $MSE_{\hat{X}}$.

$$MSE(\widehat{X}) = E\left[(\hat{X} - X)^{2}\right]$$

The MSE is the sum of the variance and the squared bias of the predications. The estimator is,

$$MSE(\widehat{X}) = Var(\hat{X}) + \left(Bias(\hat{X}, X)\right)^{2}$$

7.EXPERIMENT ANALYSIS

Several experiments have been conducted on this framework on the standard datasets from [16, 17] for recognition/verification. In the decision process, the Mean Square Error (MSE) [22] is considered for testing/training patterns based on the error rate, the difference between training and testing memories M and M^{T} computed using CSEAM model respectively.

The experimental results have been considered on the chosen data patterns is listed in the Table1 with various key patterns from selected features using proposed framework such as 8x8,16x16,....,64x64 on similar and dissimilar face and fingerprint patterns.

Matching and non-matching patterns using FMR and FNMR decision method

From the consideration of posters of the multimodal authentication system, FNMR and FMR metrics have been computed for the selected features using LU factorization with CSEAM model. In the process of pattern acquisition, error free data will be considered from the standard benchmark datasets and its FAR/FMR and FRR/FNMR pairs are equivalent.

FMR[1] is the probabilistic estimator of the pattern matching that incorrect the input data to a non-matching data in the chosen dataset. The FMR metric is the ratio of matching whose error value is equal or less than the threshold d: MSE ≤ d, where the threshold d is the set of possible values of the global error.

Similarly FNMR[1] is another probabilistic estimator non-pattern matching of the input data to matching patterns from the datasets that measures % of valid inputs which are incorrectly rejected. The FNMR is computed as the percentage of matching whose error is greater than the threshold d: MSE>d.

No	Key Size	MSE			
		Similar with different poses (SVD with LU)	Similar with different poses (SVD)	Dissimilar with different poses (SVD with LU)	Dissimilar with different poses (SVD)
1	8x8	0.001044	0.0162	0.011948	0.0488
2	16x16	0.000106	0.0011	0.004774	0.0074
3	24x24	0.000273	0.000450	0.002030	0.0067
4	32x32	0.000130	0.000444	0.001630	0.0033
5	40x40	0.000066	0.000392	0.000893	0.0027
6	48x48	0.000049	0.000271	0.000777	0.0018
7	56x56	0.000061	0.000208	0.000372	0.0015
8	64x64	0.000043	0.000182	0.000459	0.0013

Table 1: Mean Square Error (MSE) of various key sizes

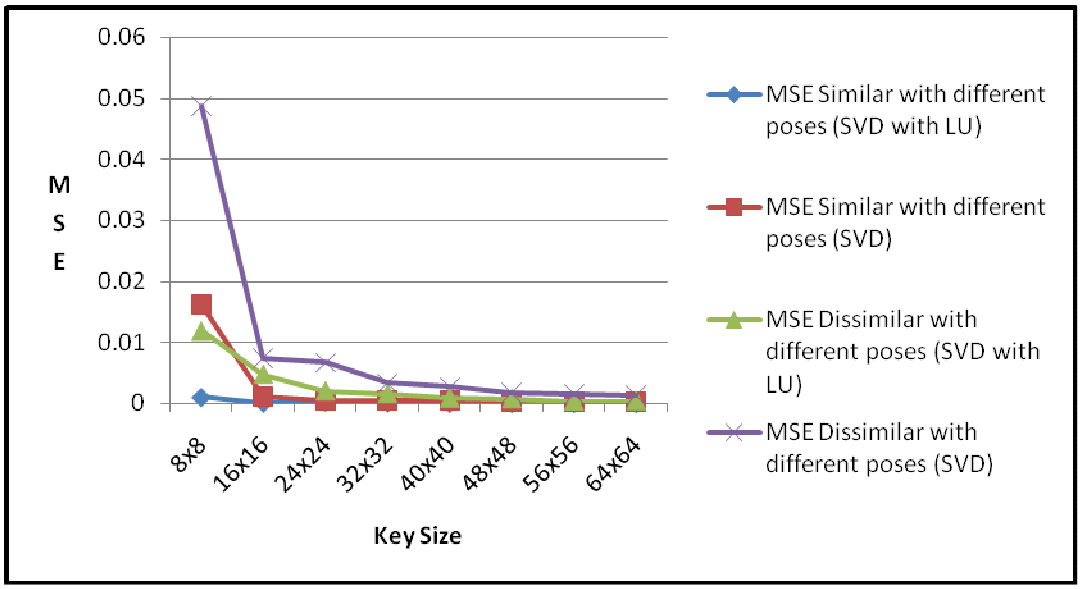


Figure 3: Mean Square Error

From the analysis of experimental results, it is observed that the key size 8x8 has been encountered in rejecting rate when provided similar multimodal data patterns (FMR).

8.CONCLUSIONS

In this paper, an intuitive framework is proposed using cognitive logic for authentication/ verification of the biometrics patterns in multimodal authentication. In this framework the keys have been selected from the extracted features of the fusion patterns using LU factorization technique and then combined using Context-sensitive Exponent associative memory model with the concept of exponential kronecker product (CSEAM).This model is one of the nice strategies in the domain of cognitive logic. This framework returns better and better outcome from the selected datasets [16, 17] and provides more complex security in terms of time and space, since it uses ***eKP*** in the cognitive logic. From the observations of experimental results, the key sizes should be more than 8x8, since while extracting the feature and applying the PCA by SVD, some of the features might be lost. In such cases, the fusion data will be regretted by the proposed framework. For the rest of the cases the proposed framework returns better outcome. This framework is also compared with the selection of key patterns using normal SVD factorization which gives more accurate and efficient recognition.

REFERENCES

[1] PESN Krishna Prasad, K. Pavan Kumar, MV Ramakrishna and BDCN Prasad, "Fusion Based Multimodal authentication in Biometrics using Context-Sensitive Exponent Associative Memory Model: A Novel Approach", CS&IT Conference proceedings pp. 81-90, 2013, DOI:10.5121/csit/2013.3608

[2] Mary Lourde R and DushyantKhosla, Fingerprint Identification in Biometric Security Systems, International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, 852-855, 2010.

[3] 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

[4] Jain, A.K.; Ross, A., Prabhakar, S. An Introduction to Biometric Recognition. IEEE Trans. Circuits Syst. Video Technol., 14, 4-20, 2004.

[5] R. Bruneelli and D.Falavigna, "Person identification using multiple cues," IEEE Trans. PAMI, vol. 17, no.10, pp.955-966, oct.1995.

[6] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Trans. PAMI, vol. 20, no. 3, pp. 226-239, 1998

[7] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. PAMI, vol. 20, no. 12, pp. 1295-1307, 1998.

[8] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification", IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999

[9] A. Ross and A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003

[10] RasmusElsborg Madsen, Lars Kai Hansen and Ole Winther, "Singular Value Decomposition and Principle Component Analaysis", February 2004

[11] Matthew A. Turk, Alex P. Pentland, "Face Recognition using Eigen Faces", IEEE 1991

[12] Vaclav Matyas, ZdenekRiha, "Biometric Authentication —Security and Usability", http://www.fi.muni.cz/usr/matyas/

[13] John W. Brewer, Kronecker Products and Matrix Calculus in System Analysis, IEEE Transactions on Circuits and Systems, Vol. 25, No. 9, 1978

[14] Wolfgang Hackbusch, Boris N. Khoromskij, Hierarchical Tensor-Product Approximations, 1-26.

[15] LubomírBrančík, Matlab Programs for Matrix Exponential Function Derivative Evaluation

[16] http://www.face-rec.org/databases/

[17] http://www.advancedsourcecode.com/fingerprintdatabase.asp

[18] Izquierdo-Fuento, A.; del Val, L.; Jimenez M.I.; Villakorta, J.J. "Performance Evaluation of a Biometric System Based on Acoustic Images. Sensors, 119499-9519, 2011.