IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Feature Selection using DWT+SVD for Fusion Based Multi model Authentication

Alapati Kavitha[1], M.V Rama Krishna[2], N. Venkata Ramana Gupta[3], PESN Krishna Prasad[4]

[1]M.Tech Scalar, PVP Siddhartha Institute of Technoogy, Kanuru, Vijayawda,A.P, India
[2]Dept of CSE, PVP Siddhartha Institute of Technoogy, Kanuru, Vijayawda,A.P, India
[3]Dept of CSE, PVP Siddhartha Institute of Technoogy, Kanuru, Vijayawda,A.P, India
[4]Dept of CSE, SV College of Engineering, Tirupati,A.P, India

[*]*Corresponding Author:kavithaalapati@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 23/Jul/2018, Published: 31/July/2018

Abstract— Biometric is the process which is used to measure people's distinctive physical and behavioural characteristics with the help of mathematical analysis. The technology is principally used for detection and right to use management, or for distinguishing people WHO area unit beneath police work. Now a days used biometric systems are of face, fingerprints, iris, retina, signature, palm print, identification and so on to see a person's identity. In this paper, we have a tendency to contemplate face and fingerprint features for authentication and confirmation. Victimisation this knowledge we have a tendency to project a model for authentication in multimodal biometry that is typically referred to as Context-Sensitive Exponent Associative Memory Model (CSEAM). CSEAM applied on biometry patterns and afford security for the data. In the first step of this paper, Discrete Wavelet Transformation (DWT) face and finger can be applied at first and then Fusion can be applied . In the second stage Principle Component Analysis (PCA) can be applied at first and then Singular Value Decomposition (SVD) can be applied to extract features. In the third stage these features can be stored for authentication and verification in smart cards). In CSEAM model, exponential Kronecker product applied for verification and authentication on input samples. Verification and authentication can be done using different key sizes. This paper shows better results for the key size of 8x8 by using DWT while comparing to the Pavan Kumar K[1] et all.

Key Words: Biometric, Discrete Wavelet Transformation, exponential kronecker product.

1. INTRODUCTION

In the advanced electronic age, ought to demonstrate and determine people for guaranteeing the protection of a system. Ancient ways of authentication and identification are used for ID cards or PIN. However such identifiers are often stray, purloin, or omit these system fail to distinguish between a right person and fraudulent person. To solve these problems AI[2,18] together with pattern recognition, machine learning, biometric knowledge analysis provide the additional issues for security. The remaining sections discussed about discrete wavelet transformation, Principal component analysis, Singular Value Decomposition, Context sensitive associative memory model and last section discussed about proposed model.

1.1 BIOMETRIC

Usually, passwords and ID cards are accustomed to safeguard to interact the systems. However, the system fails to provide security once a word is accessible to associate degree unauthorized user or a card is taken by associate fake person. So that the emergence of biometry has discussed the issues that plague ancient verification ways.

Biometrics [8, 10, 12] refers to the automated identification of a personal by victimisation bound physiological or activity traits that are related to the person. By victimisation biometry, it is attainable to determine associate degree that are identity supported "who you're," instead of by "what you possess" or "what you remember".

Current biometric systems [8] can detect face, fingerprints, iris, hand pure gesture, retina, signature, palm print, biometric authentication and it determines identity of a person. Whereas biometric systems have their own limitations.

Biometric systems [7, 10 and 12] will run in two models 1) the classification mode, within which the identity of associate degree unknown user is set, and 2) the confirmation mode, based on claimed identity is either a real user or an impostor.

1.2 MULTIBIOMETRIC SYSTEMS

Based on the constraints of unimodel biometric systems are often overcome by victimisation multiple biometric modalities. Such systems are typically referred to as multibiometric systems, correct measure that are supported to be additional reliable because of the incidence of multiple somewhat freelance items of proof. These models shows better performance for different applications.

Multibiometric systems [10, 11, 13] deal with the matter of non-universality. Multibiometric systems offer associate degreeti-spoofing measures by creating it troublesome for an unwelcome person and at the same time satire the multiple biometric traits of a valid user. Thus, a challenge-response variety of authentications are often expedited victimisation multibiometric systems. A spread of things ought to be thought-about once by planning a multibiometric system. It embraces the selection and range of biometric behaviour; the amount within the biometric system at that information provided by multiple traits ought to be integrated; the methodology adopted to integrate the information; and therefore the price versus matching performance trade-off. The selection and range of biometric traits is basically driven by the character of the appliance, the overhead introduced by multiple traits (computational demands and cost), and therefore the correlation is between the traits thought-about. A phone with camera it would be easier to mix the face and speech/ character of a user, whereas in associate degree ATM application it would be easier to mix the fingerprint and face character of the user..

The projected organization is often categorised into three ways: (1) Feature extraction and fusion at feature level, (2) computation level victimisation CSEAM[2], and (3) authentication level. Figure 1 shows the totally three levels

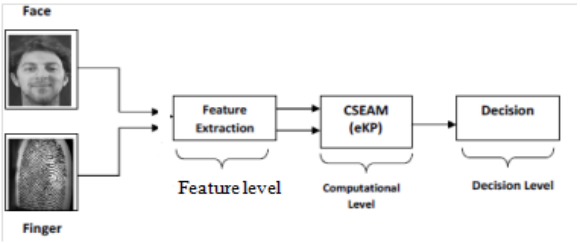

Figure 1: different stages of proposed system

Feature Level: Features can be extracted and the fusion of feature level contains the development of a replacement higher order feature vector which is composed of choice feature components of assorted feature vectors generate victimisation distributed WDT, PCA and SVD. The new feature vector ought to end up to be additional discriminative than every single one.

Computation Level: Here, matching scores of fusions are retrieved by every personage obtained system scores are combined. Combined measures properly regulated and they will combine victimisation. The specified fusion of normalized scores ends up in an additional correct entire system.

Decision level: Finally decision is to be taken by considering the metrics that represents the performance. By sending different types of inputs outputs will be observed. Based on this observation decision is taken.

of inputs outputs will be observed. Based on this observation decision is taken.

1.3 MULTI-BIOMETRIC RECOGNITION

Single biometric verification system handle reedy detector gaining, controlled degrees-of-freedom, or non-universality unrealistic concert rates square measure give up. Such weakness, that represent common eventualities once in operation biometric recognition systems, raise the requirement for multi-biometric recognition[11] or alternative approaches to extend the popularity accuracy. With the fusion of multi biometric shows that get better the meticulousness and irresponsibleness systems.

Here, features can be extracted using Discrete Wavelet transformation (DWT) followed by PCA. After that Singular value decomposition can be applied

II. DISCRETE WAVELET TRANSFORMATION (DWT)

DWT is used for extracting the features from the given images on different scales by applying different filters (Low & High).

In this process

1. For getting the detailed coefficients divide the given images by using DWT upto N levels with decomposition and filtering
2. Obtain the feature from DWT coefficients.

III. PRINCIPLE COMPONENT ANALYSIS (PCA)

Whenever the DWT is applied, features can be extracted in which some of them are useful and some of them are non useful. To reduce the feature space apply the PCA.

PCA [4, 9, 14] could be a method that identify underlying variables (known as principal components) that best separate your data points.

Principal components measure dimensions on

that your information points which are most unfold out. It performs the dimensionality reduction.

PCA algorithm

- Data can be normalized.
- Calculate the covariance matrix and then retrieve the Eigen Values and Eigen Vectors.
- Eigen values can be sorted in decreasing order and get m eigenvectors that represents to

the m topmost eigenvalues. Here m represents the subspace dimension.

- Projection matrix can be constructed with W from the chosen k eigenvectors.
- Model the new dataset X via W to form subspace Z with m dimensional features.

IV. Singular Value Decomposition (SVD)

The singular Value decomposition (SVD)[5,6] could be very much useful for feature extraction. Significantly it can be used for knowledge analysis, for reducing dimensions of pictures, knowledge etc. The SVD of X is computed as

$$X=UDVT = \sum_{k=1}^{r} s_k u_k v_k^T$$

V. Calculation of Exponential of a Matrix

Let A be a matrix, the exponential [17, 23] of A by using Taylor series as:

$$e^A = \sum_{n=0}^{\infty} \frac{A^n}{n!} = I + A + \frac{A*A}{2!} + \frac{A*A*A}{3!} + \cdots$$

Another way of computing the matrix exponential is to calculate the exponential of every diagonal component of the matrix. To get the exponential of a square matrix there is a need of calculate the exponential of every diagonal component of the matrix A victimisation Pade Approximation [17, 22]. Let us consider the matrix A as

$$A = \begin{bmatrix} a_0 & 0 & \cdots & 0 \\ 0 & a_1 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n-1} \end{bmatrix}$$

Then we calculate the diagonal matrix exponential as

$$e^A = \begin{bmatrix} e^{a_0} & 0 & \cdots & 0 \\ 0 & e^{a_1} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & e^{a_{n-1}} \end{bmatrix}$$

Exponential Kronecker Product (eKP):

In [19, 20] represents some detailed aws with reference to operations on Tensor. Assume A and B are two square matrices, then the eKP is delineate as:

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

VI. Context-Sensitive Exponent Associative Memory Model (CSEAM)

Cognitive functions think of the in depth use of knowledge which is kept within the brain, and therefore the checking out the relevant info for finding some drawback could be a terribly advanced task. Mostly human knowledge uses natural search engines, and assumptive to check psychological feature perform ought to perceive the method these brain search engines work. The process is to check multi standard network models, able to solve explicit issues that involve info looking. The building blocks of those multi standard networks square measure the context -dependent memory models. These models work by associating associate degree output to the Kronecker product[21] of associate degree input and a context.

Vector logic [2, 3, 16] can be mathematically shown as the reality values can be mapped to components of a vector area. These operations can be performed by rectangular matrices. Performing the operations on these vectors is easy when compared to the general form. Vector logic can be implemented on rows or columns.

In CSEAM [15], the associative memory can be modelled as exponential Kronecker Product (eKP) that contains a pair of input patterns which can be used to create a model typically referred to as exponent associative memory model (M). Mathematically, it can be drawn as:

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

A and B are represented as Vectors.

VII. Proposed Model

Here, a replica for authentication and verification with Discrete Wavelet Transformation is proposed. Pavan Kumar K et all.[1] proposed a model with feature extraction methods PCA and SVD. For storing the features in smart cards, CSEAM method is used with exponential kronecker Product. First apply the Discrete Wavelet Transformation for extracting better features and later apply PCA and SVD for better feature dimensionality reduction and fusion. Here features can be extracted in two levels. In the first level apply the DWT, features can be extracted with some relevant and non relevant features. In the second level apply the PCA for those, features space can be reduced and only important features can be obtained. For these futures fusion can be applied and projected the training images on the fusion and keys can be generated. Apply kronecker product for these keys (M) and stored in the CSEAM that is used for the authentication or verification. These samples can be used to generate memory MT, so that MT is compared with stored memory M. MT can be computed as:

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

Where A and B are Keys. The difference between the trained images and testing images can be calculated by using Euclidean distance metric. Here threshold value can be defined as d=1.3. If the value is greater than d given images are dissimilar. If the value is less than d images are similar

VIII. EXPERIMENTAL ANALYSIS

The following table shows the experimental analysis when comparing to the Pavan Kumar[1] et all. Table 1 shows the comparison of two methods with graphical representation.

Table1 : comparison between two methods

		PCA+SVD+MSE		DWT+PCA+SVD +Euclidean	
S. No	***Key Size***	***Similar***	***dissimilar***	***Similar***	***dissimilar***
1	8x8	0.0162	0.0488	0.8092	1.8088
2	16x16	0.0011	0.0074	0.7621	1.4665
3	24x24	4.50E-04	0.0067	0.8623	1.4545
4	32x32	4.44E-04	0.0033	0.8973	1.5048
5	40x40	3.92E-04	0.0027	0.9582	1.5216
6	48x48	2.71E-04	0.0018	1.0221	1.5144
7	56x56	2.08E-04	0.0015	1.2282	1.601
8	64x64	1.82E-04	0.0013	1.3768	1.8096

.

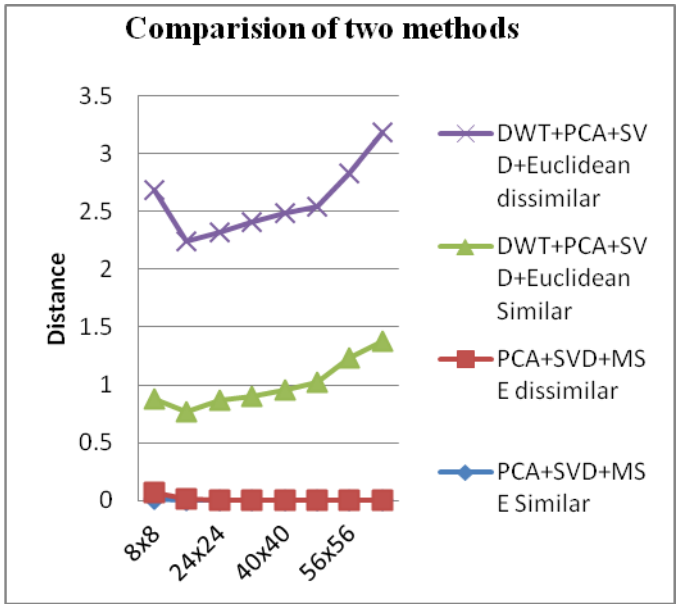

Figure 2.Comparision of Two methods

The above experiments can be executed on 2 GB RAM, 500Gb hard disk, Intel core i3 processor and windows 7 environment. In both the cases key sizes can be varied from 8x8 to 64x64. When using PCA+SVD+MSE combination the threshold can be set as d=0.001. In this the system failed for the key size of 8x8. Where as in DWT+PCA+SVD+Euclidean distance case set d=1.37. In this case the algorithm works well for the key size along with 8x8 also.

IX. CONCLUSION

In this paper, a model was proposed for feature extraction by using discrete wavelet transformation in the first stage. Later apply the PCA and SVD for dimensionality reduction and fusion. After we can apply exponential kronecker product for storing the key features and use the Euclidian distance as a measure for authentication. Whenever apply the PCA, SVD and MSE that will fails for the key size 8x8. Whereas apply the DWT for feature extraction and later apply the PCA and SVD for dimensionality reduction and fusion. Euclidean distance can be used for authentication. So that this proposed method works better for all the key sizes. Hence discrete wavelet transformation works well for feature extraction

REFERENCES

[1] Pavan Kumar K, P. E. S. N. Krishna Prasad, M. V. Ramakrishna and B. D. C. N. Prasad *"Feature Extraction using Sparse SVD for Biometric Fusion in Multimodal Authentication"* , International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4, July 2013,PP. 83-94

[2] Mihee Lee, Haipeng Shen, Jianhua Z. Huang,2 and J. S. *Marron*, "*Biclustering via Sparse Singular Value Decomposition , Biometrics"* 66, 1087–1095, December 2010.

[3] P. E. S. N. Krishna Prasad and B. D. C. N. Prasad, "*Password Authentication using Context-Sensitive Associative Memory Neural Networks: A Novel Approach"*, Proceedings in LNICST-85, Part 2, CCSIT-2012, Bangalore, Springer Heidelberg, 454-468, 2012.

[4] Eduardo Mizraji, "*Modality in Vector Logic*", Notre Dame journal of Formal Logic, Vol. 35, No. 2, 272-283, 1994.

[5] Turk, M. and Pent land, A. (1991), *"Eigenfaces for recognition"*, Journal of Cognitive Neuroscience, vol. 3, no. 1, p.71-86

[6] Roberto Bruunelli and Tomaso Poggio, "*Face Recognition:Features versus Templates"* IEEE Trannsactions on Patten analysis and Machine intelligence Vol.15.No.10, Octomber 1993

[7] Chou-Hao Hsu and Chaur-Chin Chen *"SVD-Based Projection* for *Face Recognition"*, IEEE EIT 2007 Proceedings

[8] 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.

[9] Samir Nanavati, Michael Thieme, and Raj Nanavati, "*Biometrics Indentity verification in the network World"*, Weily Tech Brief, 2002.

[10]H. Moon, P.J. Phillips, "*Computational and* Performance *aspects of PCA-based Face Recognition Algorithms, Perception"*, Vol. 30, 2001, pp. 303-321

[11]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
[12]Arun Ross and Anil K. Jain, "*Multimodel Biometrics: an Overview, 12th European Signal Processing Conference"*, 1221-1224,2004.
[13]Jain, A.K.; Ross, A., Prabhakar, S. "*An Introduction to Biometric Recognition",* IEEE Trans. Circuits Syst. Video Technol., 14, 4-20, 2004.
[14]Tejas, J.; Sommath, D. "*Multimodal Biometrics: State of the art in Fusion Techniques",* Int. J. Biometrics, 4, 393-417, 2009.
[15]Kyungnam Kim, "*Face Recognition using PCA"*,Vision and AI Research group, 2001.
[16]Wayne A. Wickelgren, "*Context-sensitive coding, Associative Memory and serial order in Speech Behaviour, Psychological Review"*, Vol. 76, No. 1, 1-15, 1969,
[17]Juan C. Valle-Lisboa, Florencia Reali, Hector Ansatasi Ab, Eduardo Mizaraji, "*Elman topology with sigma-pi units: An Application to the modelling of verbal hallucinations in Schizophrenia, Neural Networks"*, Elsevier, 18, 863-877, 2005.
[18]Cleve Moler and Charles Van Loan, "*Nineteen Dubious ways to Compute the Exponential of a Matrix, Twenty-Five Years Later, SIAM Review"*, Society for Industrial and Applied Mathematics, Vol. 45, No.1,1-46, 2003
[19]Artur S. d'Avila Garcez, Lu´is C. Lamb and Dov M. Gabbay, "*Connectionist Model logic: Representing Modalities in Neural Networks"*, Theoritical Computer Science, Vol. 371, Issue 1-2,34–53, 2007.
[20]H. V. Henderson, F. Pukelsheim and S. R. Searle "*On the history of the Kronecker product. Linear and Multilinear Algebra",* 14:113-120, 1983.
[21]Lester Lipsky and Appie van deLiefvoort, "*Transformations of the Kronecker Product of Identical Servers to Reduced Product Space"*, 1995.
[22]John W. Brewer, "*Kronecker Products and Matrix Calculus in System Analysis"*, IEEE Transactions on Circuits and Systems, Vol. 25, No. 9, 1978
[23]Wolfgang Hackbusch, Boris N. Khoromskij, "*Hierarchical Tensor-Product Approximations".*

Authors Profile

Ms. Kavitha Pursuing M.Tech degree in Computer Science and Engineering from PVP Siddhartha Institute of Technology(Autonomous) Vijayawada, Andhra Pradesh and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. She received her B.Tech degree in Information Technology from PVP Siddhartha Institute of Technology(Autonomous) Vijayawada, Andhra Pradesh and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. Her interested areas are Image Processing, Database Management Systems, Computer Networks.

Dr. M V Rama Krishna has been working as Professor, department of Computer Science & Engineering, Prasad V. Potluri Siddhartha Institute of Technology (Autonomous) Vijayawada, Andhra Pradesh and is affiliated to Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh. He obtained B.Tech, M.Tech and Ph.D from NIT-Suratkal, Jawaharlal Nehru Technological University, Hyderabad and Acharya Nagarjuna University, Guntur respectively. He has 27 years of Teaching and 4 years of Industry Experience He had published 12 research papers in various International Journals and Conferences. He is a member of ACM and CSI.

Mr. N. Venkata Ramana Gupta has been working as Assistant Professor in Department of Computer Science and Engineering Prasad V. Potluri Siddhartha Institute of Technology (Autonomous) Vijayawada, Andhra Pradesh and is affiliated to JNTU-K, Kakinada. He is pursuing his Ph.D. in Acharya Nagarjuna University. He is APSET Qualified. He obtained M.Tech (Computer Science and Technology with specialization in computer Networks) from Andhra University College of Engineering, Visakhapatnam, AP. He has 19 years teaching experience in teaching computer science subjects. He had published 6 research papers in various International Journals. His areas of interest are Computer Networks, Distributed Systems. He is member of ACM and Life Member of ISTE.

Dr. P E S N Krishna Prasad teaching experience includes over 17+ years and research 9 years in the Academia. He works in a multi-disciplinary environment involving machine intelligence, image processing, biometrics, soft computing, data mining, and information security and applied to various real world problems. He is an author/co-author of 30+ publications in various International conferences and journals with120+ citations Since 2013, He is Technical Committee member in IEEE SMC Society Technical Committee on Soft Computing and senior member IEEE – Region 10 and also CSI State Level Student Coordinator 2016-17 and 2017-18.
He serves/has served the editorial board member of over 15+ International Journals and Program Committee member over 35+ International Conferences and also reviewer over 20+ International Journals under various capacities.

