Feature Extraction using Sparse SVD for Biometric Fusion in Multimodal Authentication

Pavan Kumar K[1], P. E. S. N. Krishna Prasad[2], M. V. Ramakrishna[3] and B. D. C. N. Prasad[4]
[1 2, 3 & 4]Prasad V. Potluri Siddhartha Institute of Technology, India
[1]pavanpvpsit@gmail.com, [2]surya125@gmail.com, [3]krishna1959@gmail.com and [4]bdcnprasad@gmail.com

ABSTRACT

Token based security (ID Cards) have been used to restrict access to the Secured systems. The purpose of Biometrics is to identify / verify the correctness of an individual by using certain physiological or behavioural traits associated with the person. Current biometric systems make use of face, fingerprints, iris, hand geometry, retina, signature, palm print, voiceprint and so on to establish a person's identity. Biometrics is one of the primary key concepts of real application domains such as aadhar card, passport, pan card, etc. In this paper, we consider face and fingerprint patterns for identification/verification. Using this data we proposed a novel model for authentication in multimodal biometrics often called Context-Sensitive Exponent Associative Memory Model (CSEAM). It provides different stages of security for biometrics fusion patterns. In stage 1, fusion of face and finger patterns using Principal Component Analysis (PCA), in stage 2 by applying Sparse SVD decomposition to extract the feature patterns from the fusion data and face pattern and then in stage 3, using CSEAM model, the extracted feature vectors can be encoded. The final key will be stored in the smart cards as Associative Memory (M), which is often called Context-Sensitive Associative Memory (CSAM). In CSEAM model, the CSEAM will be computed using exponential kronecker product for encoding and verification of the chosen samples from the users. The exponential of matrix can be computed in various ways such as Taylor Series, Pade Approximation and also using Ordinary Differential Equations (O.D.E.). Among these approaches we considered first two methods for computing exponential of a feature space. The result analysis of SVD and Sparse SVD for feature extraction process and also authentication/verification process of the proposed system in terms of performance measures as Mean square error rates will be presented.

KEYWORDS

Biometrics; Biometric fusion; Face; Fingerprint; Context-Sensitive Exponent Associative Memory Model (CSEAM); Kronecker Product; Exponential Kronecker Product (eKP); Multimodal Authentication; Singular Value Decomposition (SVD); Sprase SVD (SSVD);

1. INTRODUCTION

Modelling is the bread and butter for many working researchers and naturally is being applied to address issues in Biometric security. Many of the speculative queries, researchers and decision-makers have about security issues in Biometrics can be more practically and efficiently tested in computer models as opposed to actual physical experiments.

Traditional methods of authentication and identification make use of identification (ID) cards or personal identification numbers (PINs), but such identifiers can be lost, stolen, or forgotten. In addition, these models fail to differentiate between an authorized person and an impostor who fraudulently acquires knowledge or "token" of the authorized person. Security breaches have led to losses in terms of cost for the sectors like banks and telecommunication systems that depend on token-based security systems.

DOI : 10.5121/ijnsa.2013.5406

The connectionist models or Artificial Neural Networks (ANN) [2, 18], due to the resemblance of processing with the form of processing of the human nervous system, they are essential parts of an emerging field of knowledge known as Computational Intelligence. The use of connectionist models has provided a solid step forward in solving some of the more complex problems in Artificial Intelligence (AI), including such areas as machine vision, pattern recognition, biometric data analysis and recognition. The research in this field has focused on the evaluation of new neural networks for pattern recognition, training algorithms using real biometric data, and whether parallel architectures of neural networks can be designed to perform effectively the work required for complex algorithms for the recognition of biometric patterns.

1.1 Biometrics

Passwords and ID cards used to restrict access to secure systems. When a password or ID card is available to an unauthorized user, security can be easily breached in these systems. The flaws in traditional verification methods can be addressed in the biometric authentication systems.

Current biometric systems [8, 10 and 12] make use of face, fingerprints, iris, hand geometry, retina, signature, palm print, voiceprint and so on to establish a person's identity. Though there are limitations in biometric systems, they have some advantages over the conventional security methods. In this regard the biometric patterns cannot be easily stolen or shared. Biometric systems also enhance user friendliness by alleviating the need to design and remember passwords.

Biometric systems [7, 10 and 12] can operate in one of two modes 1) the identification mode, in which the identity of an unknown user is determined, and 2) the verification mode, in which a claimed identity is either accepted or rejected. Biometric systems are being deployed in various applications including User logins, ATM PINs, Marts, Adhar cards and any other identity cards. The successful installation of biometric systems in these applications does not imply that the biometrics is a not complete solution.

1.2 Multibiometric Systems

By use of multiple biometric modalities (multibiometric systems), the limitations of unimodal biometric systems can be overcome. The modalities of multibiometric systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. These systems are also able to meet the performance requirements imposed by various applications.

Multibiometric systems [10, 11 and 13] address the problem of non-universality. Due to anti-spoofing measures available in multibiometric systems, it is difficult for an intruder to spoof the multiple biometric traits of a user. Multibiometric systems facilitate the challenge-response type of authentication. A variety of factors to be considered include: 1) the choice and number of biometric traits, 2) the level in the biometric system that provides the multiple traits to be integrated, 3) the methodology adopted to integrate the information and 4) the cost versus matching performance trade-off. A commercial multibiometric system called AdharID integrates the face, iris, palm and fingerprint of an individual. The information presented by multiple traits may be consolidated at various levels.

The proposed system can be categorized into three levels, according to the level within which the authentication/verification is performed. Three possible levels of evaluation: (1) fusion at feature level, (2) computation level using CSEAM[2], and (3) decision level. Figure 1 illustrates these different stages of biometric system.

1. Feature Level: the biometric fusion comprises the construction of a new feature vector of higher order dimensionality. This vector is composed of selection feature elements of

various feature vectors generated using Sparse SVD(SSVD)[1]/SVD. The new vector is more discriminative than the individual ones.

2. Computation Level: at this level, fusion matching scores are returned by individual subsystem and the obtained scores are combined. The normalized scores can be combined using CSEAM model as neural system so that the fusion of normalized scores leads to a more accurate overall system.
3. Decision Level: The final decision (in general accept/ reject) is to be performed to make the decision in this level through performance metrics. Various final decisions of independent subsystems can be processed by applying a majority voting in order to increase the accuracy or convenience of the entire system.

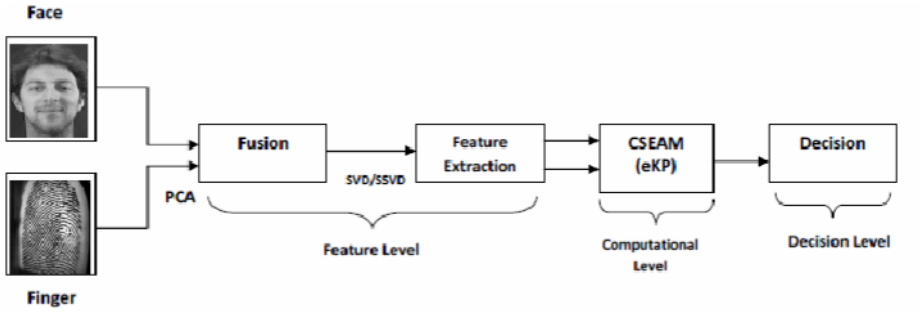

Figure 1: Block Diagram of Proposed System

At the feature extraction level, a new feature set is generated from the integration of multiple modalities of the feature sets. The new feature set is then used in the matching and decision-making modules of the biometric system. At the computation level, the matching output by multiple matchers is integrated. At the decision level, the final decisions will be made by the individual systems consolidated by employing techniques such as majority voting. *All these three levels of process can be applied in three stages of the proposed model.*

In most cases, the integration at the feature level usually performs better, but it is not always feasible for multiple reasons. First, Most of the commercial systems do not provide access to information at this level. Second, the feature spaces of different biometric traits may not be compatible. Third, even if the feature sets were compatible, concatenation might result in a feature vector with a very large dimensionality leading to the "curse of dimensionality" problem. This problem can be solved using vector logic in the cognitive domain. Here, we proposed a novel approach for computing the large dimensionality of the feature vector space using Exponential kronecker Product (eKP) as a part of CSEAM Model, that creates an associative memory for holding the combined feature patterns of fusion biometric data for authentication/verification in multimodal authentication process.

1.3 Multi-biometric recognition

Whenever biometric verification systems based on single biometric indicators have to deal with noisy sensor acquisition, restricted degrees-of-freedom, or non-universality, impractical performance rates are yielded. These drawbacks are common scenarios when operating biometric recognition systems that raise the need for multi-biometric recognition or other approaches to increase the accuracy of recognition. A fusion of multiple biometric indicators shows that improve the accuracy and reliability of biometric systems.

In this paper we describe a connectionist approach often called CSEAM [2, 4] model to authenticate the multimodal biometrics, in which the first step is to fusion the face and fingerprint

biometric patterns through PCA[9] followed by SVD/Sparse SVD[1] decomposition for extracting the feature spaces as keys for security and then apply the CSEAM model using ***exponential kronecker product***(eKP)[2, 17] to encode the feature patterns. In the second step the verification process can be done using the same model.

2. FEATURE EXTRACTION USING SPARSE SVD[1]

The singular value decomposition, or SVD, is a very powerful and useful matrix decomposition, particularly in the context of data analysis, dimension reducing transformations of images, satellite data etc, and is the method of choice for solving most linear least–squares problems.
The singular value decomposition (SVD) of X can be written as

$$X=UDV^T=\sum_{k=1}^{r} s_k\, u_k v_k^T \quad (1)$$

The proposed SSVD [1] seeks a low-rank matrix approximation to X as that in (2), but with the requirement that the vectors u_k and v_k are sparse, that is, they have many zero entries. We obtain sparsity by adding sparsity-inducing penalties to the minimization objective in (3). The sparsity property implies that, the rank-one matrix $s_k u_k v_k^T$, now referred to as an SSVD layer. Specifically, for the k^{th} SSVD layer, those rows (or samples) with nonzero u_{ik} s are naturally clustered together, as well as those columns (or variables) with nonzero v_{jk} s. Hence the k^{th} layer simultaneously links sets of samples and sets of variables together to reveal some desirable sample-variable association.

If we consider the first $K \le r$ rank-one matrices in the summation in (1), we obtain the following rank-K approximation to X:

$$X \approx X^{(k)} = \sum_{k=1}^{r} s_k\, u_k v_k^T \quad (2)$$

In fact, $X^{(K)}$ gives the closest rank-K matrix approximation to X in the sense that $X^{(K)}$ minimizes the squared Frobenius norm, i.e.,

$$X^{(K)} = \underset{X^* \in A_K}{argmin} \|X - X^*\|_F^2 = \underset{X^* \in A_K}{argmin} tr\{(X - X^*)(X - X^*)^T\} \quad (3)$$

The process of SSVD algorithm[1] is computed as :

Algorithm:

1.Apply the standard SVD to X. Let $\{S_{old}, U_{old}, V_{old}\}$ denote the first SVD triple.
2.Update:

a) Set $\tilde{v}_j = \sin\{(X^T U_{old})_j\}(|(X^T U_{old})_j| - \lambda_v w_{2,j}/2)_+$, j=1…d, where λ_v is the minimize of BIC(λ_v).Let $\tilde{v}=(\tilde{v}_{1,\ldots,} \tilde{v}_d)^T$, s=$\|\tilde{v}\|$, and $v_{new}=\tilde{v}/s$.

b) Set $\tilde{u}_i = \sin\{(X\, u_{new})_i\}\}(|(X\, u_{new})_i| - \lambda_u w_{2,i}/2)_+$, i=1…n, where λ_u is the minimizer of BIC(λ_u).Let $\tilde{u}=(\tilde{u}_{1,\ldots,} \tilde{u}_n)^T$, s=$\|\tilde{u}\|$, and $u_{new}=\tilde{u}/s$.

c)Set $u_{old}=u_{new}$ and repeat Steps2(a) and 2(b) until convergence.

3. Set u= u_{old} , v=v_{new}, s=$u_{new}^T X\, v_{new}$ at convergence

Where u and v are the degree of sparsity of the sparse singular vectors, λ_u and λ_v are the penalty parameters for the singular vectors u and v.

Bayesian information criterion (BIC) can be used for the process of selecting the degrees of sparsity by making use of the connection of SSVD to penalized regression.

$$\text{BIC}(\lambda_v)=\frac{\|Y-\hat{Y}\|^2}{nd.\hat{\sigma}^2}+\frac{\log(nd)}{nd}\hat{df}(\lambda_v) \quad (4)$$

$$\text{BIC}(\lambda_v)=\frac{\|Z-\hat{Z}\|^2}{nd.\hat{\sigma}^2}+\frac{\log(nd)}{nd}\hat{df}(\lambda_u) \quad (5)$$

Where $\hat{df}(\lambda_v)$ [6]is the degree of sparcity of v with λ_v as the penalty parameter and $\hat{\sigma}^2$ is the Ordinary Least Square(OLS) estimate error. $\hat{df}(\lambda_u)$ [6]is the degree of sparcity of u with λ_u as the penalty parameter and $\hat{\sigma}^2$ is the Ordinary Least Square(OLS) estimate error.

$$\text{df}(\hat{\mu})=\sum_{i=1}^{n} cov(\hat{\mu}_i y_i)/\sigma^2 \quad (6)$$

3. Computation of Matrix Exponential:

The exponential of a matrix [17, 23] A is computed 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 approach of computing the exponential of a matrix is first to diagonalize the matrix and then to compute the exponential of each diagonal element of the matrix. The exponential of a diagonal matrix can be computed using *Pade Approximation* [17, 22]. Let A be a diagonal matrix as:

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

Then the exponential of a diagonal matrix is as:

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

Also to compute the matrix exponential in various ways using Ordinary differential equation methods discussed in [17, 23].

3.1 Properties of Matrix Exponential:

The matrix exponential has several properties [17,19 and 23], in which some of the properties are listed below.

1. $e^0 = I_n$
2. If A *and* B commute,i.e. $AB=BA$, then $e^{A+B}=e^A e^B$
3. For any matrix A, e^A is invertible and $(e^A)^{-1}=e^{-A}$
4. $e^{aX}e^{bX}=e^{(a+b)X}$

5. $e^X e^{-X} = I$
6. If $XY = YX$ then $e^X e^Y = e^Y e^X = e^{(X+Y)}$
7. If Y is invertible then $e^{YXY^{-1}} = Ye^X Y^{-1}$
8. $e^{X^T} = (e^X)^T$, where X^{T} denotes the transpose of X

3.2 Exponential Kronecker Product (*eKP*):

The exponential function [19, 20] possesses some specific properties in connection with tensor operations. Let A and B be the two matrices, then the exponential kronecker product is described as:

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

The eKP [19, 20, 21] has nice properties to imply the concept of vector logic theory. The properties are as:

- $e^A \otimes e^B = \left(e^{A^T} \otimes e^{B^T}\right)^T$
- $e^A \otimes e^B = e^{A \oplus B}$, which is a special property in the kronecker calculus.
- $e^{(A \otimes B)} = e^A \otimes e^B$

In this paper, we have chosen *exponential kronecker product* as *associative memory model* [2, 16 and 18] in the connectionist models often called Context-sensitive Exponent Associative Memory Model (CSEAM).

4. BIOMETRIC FUSION

In this task, the system works as follows: We start with the biometric sample of face and fingerprint data for training from the user. Once acquired from the user, the fusion of face and fingerprint image patterns using Principal Component Analysis (PCA) [7, 9, 13] and in parallel face pattern can be pre-processed to extract the features of face and also from the fusion pattern. In this case, a feature vector that holds the information of fusion samples are normalized onto values between [0, 1], transformed into a matrix *R* (Figure 2), and then compressed into; $G \in F(I \times J)$.

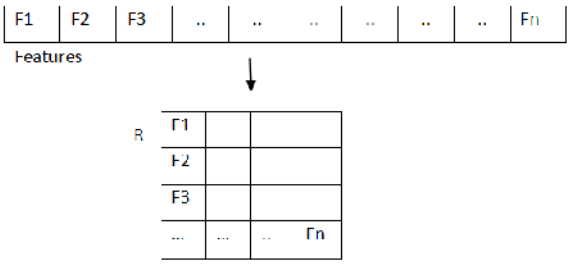

Figure 2. Feature vector normalized and transformed into Matrix *R*

In the next stage, we apply the Sparse SVD[1]/SVD factorization on matrix *R*, to obtain the feature space from these two patterns individually with various sizes *n*xn for recognition as well as for verification of samples which are collected from the user. Initially we trained the user data with two samples at the time of registration which is in the form of associative memory M, that can be stored in the network.

Once the keys are extracted from the fusion data with various sizes, the generated keys can be supplied to the *connectionist model or ANN model: Context-sensitive Exponent Associative Memory model (CSEAM)* [2,3] for encoding and verification process. In this model, memory is acted as *exponential kronecker product (eKP)* [18, 20 and 21], which is powerful concept in the field of advanced matrices. In the matrix theory, kronecker product can be applied to rectangular matrices as well as square matrices with different sizes of matrices. Suppose *mxn* and *pxq* and then produce *mpxnq* resultant matrix. One of the primary advancing concepts in the matrix theory is to apply exponential to the matrices; this can be done with various approaches, generally, the experts used to follow the Taylor series and other approaches discussed in [17].

In the proposed model, the feature vectors will be extracted from fusion and face patterns that can be passed to CSAM model for computing exponential kronecker product and the result will be stored in the smart cards as Associative Memory (CSAM) for verification.

5. CONTEXT-SENSITIVE EXPONENT ASSOCIATIVE MEMORY MODEL (CSEAM)

In the cognitive domain, information stored in the brain is extensively used by the cognitive functions and the task of searching for the relevant information for solving a problem is a very complex. Human cognition uses biological search engines. Cognitive functions need to understand the way these search engines work. The approach is to study multi modular network models that are able to solve particular problems involving information searching. The building blocks of these multi modular networks are the context-dependent memory models. These models work by associating an output to the Kronecker product of an input and a context. Input, context and output are cognitive variables in the form of vectors.

Vector logic [2, 3] is a mathematical model of logic in which the truth values are mapped on to elements of a vector space. The binary logical functions are performed by rectangular matrices operating on the Kronecker product of their vectorial arguments. The binary operators acting on vectors representing ambiguous (fuzzy) truth values generate many-valued logics. [3 and 16] showed that, within the formalism of vector logic, it becomes possible to obtain truth-functional definitions of the modalities “possibility” and “necessity”. These definitions are based on the matrix operators that represent disjunction and conjunction respectively, and each modality emerges by means of an iterative process. The mathematical representations of logic have opened illuminating perspectives for the understanding of the logical constructions created by the humans.

Memory plays a major role in Artificial Neural Networks [4, 15and 16]. Without memory, Neural Network cannot be learned by itself. In neural networks, one of the primary concepts of memory is associative neural memories. It accesses the memory by its contents, not by where it is stored in the neural pathways of the brain. Memory capacity and Content-addressability are traditional measures of associative memory performance. The maximum number of associated pattern pairs that can be stored and correctly retrieved is often referred to as Memory Capacity. The content-addressability is the ability of the neural network to retrieve the correct stored patterns. Associative neural memories are concerned with associative learning and retrieval of information in the form of vector patterns in the networks.

Associative memories [2, 4] can be implemented either in feed forward or recurrent neural networks. Such networks are used to associate one set of patterns with another set of patterns as input and output vectors. The purpose of an associative memory is to produce the associated output vector whenever one of the input vectors is applied to the neural network. The input vector

may be applied to the network either as input or as initial state and the output vector is observed at the outputs of some neurons constituting the network. Context-sensitive associative memories are models that allow the retrieval of different vectorial responses given the same vectorial stimulus, depending on the context presented to the memory. The contextualization is obtained by the Kronecker product between two vectorial entries to the associative memory: the key stimulus and the context. These memories are able to display a wide variety of behaviours that range from all the basic operations of the logical calculus (including fuzzy logics) to the selective extraction of features from complex vectorial patterns.

By providing a rich knowledge representation capable of representing highly complex knowledge that supports the features required for the context sensitive search, the experience store provides a task independent basis for context-sensitive search.

Context-Sensitive Exponent Associative Memory model (CSEAM) [2, 3 and 16] is a novel model for information access, which is general, scalable, operates in parallel with the reasoning, controls the cost of the retrieval and exploits contextual information that improves the performance. A CSEAM is built upon an associative based retrieval manager that can be implemented with vector logic, a context-sensitive search process and a content addressable store.

Here, CSEAM model [2, 3 and 16] is described using the concept of vector logic, which is one of the prime logic mechanisms to store and retrieve the associated patterns using the Context-sensitive search model with the support of content addressability. The associative memory model accesses the memory patterns as cue by its contents and not exactly where it is stored in the neural pathways of the model. The performance of associative memory is its memory capacity and content addressability.

Associative memories are connected to associative learning and retrieval of vector patterns in the semantic nets. Associative nets are used to associate one set of patterns with another set of patterns and produce output patterns. In CSEAM model, the associative memory is represented as an exponential kronecker product (eKP) that associates two sets of input patterns to frame memory model often called exponent associative memory model (M). Mathematically, this model is represented as:

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

The two input patterns A and B are represented as vectors or matrices using vector logic, then apply exponential to such vector patterns and then apply kronecker product these exponential matrices. Finally, this model gives an associative memory which is of exponential. We suggested the name for this model as exponent associative memory with the use of kronecker product based on the context-sensitive search and content addressability. It is conceived that the model is often called as context-sensitive Associative memory (CSEAM) model

6. PROPOSED MODEL

In this paper, we proposed this model for recognition and authentication of biometric data [5, 7 and 11]. Two kinds of biometrics such as face and fingerprint are considered as inputs of this network for making an association between these two patterns by applying the chosen model to create a memory model (M). The proposed model is presented as in Figure 1 that represents the recognition of the biometrics to train and test the network using CSEAM model. The resultant memory is stored in the trained network. 2(b) represents the authentication or verification of the system based on the user provided samples, these samples are supplied as inputs to the same

model to create memory M^T and then the created memory M^T is compared with the existing memory M in the trained network. The Memory model M^T is computed as:

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

Where A and B are the keys, which are generated from the user for verification. If matched, the provided samples are verified; otherwise authentication failed.

The processing of a proposed system is described in different stages. In stage 1, the system acquires the biometric patterns face and fingerprint either for registration or for verification. Once acquired, those two patterns can be pre-processed and then extracted features as vectors, then these features will be represented in matrix form. After acquiring the features, the keys are generated by applying the SVD/SSVD factorization methods. Then, the generated keys are transformed to the proposed model CSEAM for registration to represent as Associative Memory M. The resultant memory is stored in the trained network for verification whenever the user wants to verify the registered data for his/her usage of the system. Similarly, the same process is continued in the verification mode, there the computed memory M^T is compared with the memory M that is available in the trained network. The difference will be computed through some performance metrics such as mean square error (MSE). In this model, we fix the threshold of MSE for SVD based model, *d*= 0.001 and for SSVD, *d=0.01* based on the normalized errors for both proposed models, which is minimum of the tested samples. Based on the threshold errors, the user provided data will be verified by using the proposed model

7. EXPERIMENTAL ANALYSIS

In the experiments conducted on this model, we test the verification performance on the standard databases from [25, 26 and 27], and also on the realistic data collected through webcam for training and testing. In the evaluation of verification performance, we computed the Mean Square Error (MSE) [24] based on the error which is the difference between training and testing memories M and M^T respectively. The error is computed as: $\xi = M - M^T$, then the MSE will be computed with the following equation.

$$MSE = \frac{1}{K}\sum_{i=1}^{k} \xi . \xi^T$$

The experimental results on the chosen databases [25,26,27] are given in tables 1, 2, 3 and 4 with different sizes such as 8x8,16x16,....,64x64 on similar and dissimilar face and fingerprint patterns.

7.1 False Match Rate (FMR) and False Non-Match Rate (FNMR)

To characterize a biometric system, FNMR and FMR parameters have been considered for authentication/verification process. Supposing that there are no errors in the acquisition, the FAR/FMR and FRR/FNMR pairs are equivalent.

False match rate (FMR)[24] is the probability of the system matching incorrectly the input data to a non-matching template in the database, i.e. the percentage of imposters incorrectly matched to a valid user's biometric. It measures the percent of invalid inputs which are incorrectly accepted.
FMR is obtained by matching face and fingerprint of different people. The FMR parameter is computed as the percentage of matching whose error value is equal or less than the threshold *d*: $MSE \leq d$, where the threshold *d* is the set of possible values of the global error.

False non-match rate (FNMR) [24] is the probability of the system not matching the input data to a matching template in the database, i.e. the percentage of incorrectly rejected valid users. It measures the percent of valid inputs which are incorrectly rejected. FNMR is obtained by matching biometric data of the same people. The FNMR is computed as the percentage of matching whose error is greater than the threshold *d*: *MSE>d.*

		MSE	
S.NO	Key Size	Similar	Dissimilar
1	8x8	1.982	1.2935
2	16x16	0.0211	0.2257
3	24x24	2.42E-02	0.1153
4	32x32	2.86E-02	0.0863
5	40x40	1.66E-02	0.0642
6	48x48	1.26E-02	0.0543
7	56x56	1.07E-02	0.0447
8	64x64	8.50E-03	0.0393

Table 1: MSE of various key sizes for Fusion based CSEAM with SSVD using Taylor Series

		MSE	
S.NO	Key Size	Similar	Dissimilar
1	8x8	1.982	1.2935
2	16x16	0.0211	0.2257
3	24x24	2.42E-02	0.1153
4	32x32	2.86E-02	0.0863
5	40x40	1.66E-02	0.0642
6	48x48	1.26E-02	0.0543
7	56x56	1.07E-02	0.0447
8	64x64	8.50E-03	0.0393

Table 2: MSE of various key sizes for Fusion based CSEAM with SSVD using Pade Approximation

S.NO	Key Size	MSE	
		Similar	Dissimilar
1	8x8	0.0162	0.0488
2	16x16	0.0011	0.0074
3	24x24	4.50E-04	0.0067
4	32x32	4.44E-04	0.0033
5	40x40	3.92E-04	0.0027
6	48x48	2.71E-04	0.0018
7	56x56	2.08E-04	0.0015
8	64x64	1.82E-04	0.0013

Table 3: MSE of various key sizes for Fusion based CSEAM with SVD using Taylor Series

		MSE	
S.NO	Key Size	Similar	Dissimilar
1	8x8	0.0012	0.0232
2	16x16	0.0025	0.0034

3	24x24	1.40E-03	0.003
4	32x32	6.81E-04	0.0015
5	40x40	4.64E-04	0.0012
6	48x48	3.71E-04	8.06E-04
7	56x56	3.24E-04	6.72E-04
8	64x64	2.78E-04	5.83E-04

Table 4: MSE of various key sizes for Fusion based CSEAM with SVD using Pade Approximation

By the observation of the experimental results, The proposed model works with Sparse SVD and SVD algorithms for feature/ key extraction process for authentication and also the Computation model (CSEAM) works with two approaches 1) Taylor Series and 2) Pade Approximation. From these combinations, it is notified that the Sparse SVD based approach for both computation models (CSEAM using Taylor series/Pade Approximation) gets the same results and the key sizes 8x8 and 16x16, have been encountered in rejecting rate when provided similar biometric data patterns (FMR). Whereas SVD based computation models (CSEAM using Taylor series/Pade Approximation) differs the results for similar and dissimilar based data. The key sizes 8x8 and 16x16, have been encountered in rejecting rate when provided similar biometric data patterns (FMR) for both computation models, but in process of dissimilar data patterns the key sizes 48x48 onwards have been accepted when we are using Pade approximation based CSEAM model with SVD. The results are discussed in the table 1,2,3 and 4 for all approaches.

7. CONCLUSIONS

In this paper, we proposed a novel model in the cognitive logic often referred as CSEAM model (Taylor / Pade Approximation) through Sparse SVD/SVD based feature extraction for authentication/ verification of the biometrics data in multimodal authentication. The Sparse SVD based CSEAM model using Taylor series gives better results from the chosen databases when compared with other approaches and provides more complex security in terms of time and space, which uses exponential kronecker product in the vector logic that can be computed using Taylor series. From the observation of experimental results, the key sizes should be more than 16x16, since while extracting the feature and applying the PCA, some of the features might be lost. In such scenarios, the biometric data will be refused by the model. For the rest of the cases the proposed model gives better results.

REFERENCES

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

[2] 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.

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

[4] Neil A. Thacker, Joh E. Mayhew, Designing a Layered Network for Context-Sensitive Pattern Classification, Neural Networks, Vol. 3, No. 3, 291-299, 1990.

[5] L. Wiskott, J.-M. Fellous, N. Krueuger, C. von der Malsburg, Face Recognition by Elastic Bunch Graph Matching, Intelligent Biometric Techniques in Fingerprint and Face Recognition, eds. L.C. Jain et al., CRC Press, 1999, pp. 355-396.

[6] By Hui Zou, Trevor Hastie and Robert Tibshirani, ON THE “DEGREES OF FREEDOM” OF THE LASSO, The Annals of Statistics, 2007, Vol. 35, No. 5, 2173–2192,DOI: 10.1214/009053607000000127,c Institute of Mathematical Statistics, 2007.

[7] 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.
[8] Samir Nanavati, Michael Thieme, and Raj Nanavati, Biometrics Indentity verification in the network World, Weily Tech Brief, 2002.
[9] H. Moon, P.J. Phillips, Computational and Performance aspects of PCA-based Face Recognition Algorithms, Perception, Vol. 30, 2001, pp. 303-321
[10] 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
[11] Arun Ross and Anil K. Jain, Multimodel Biometrics: an Overview, 12th European Signal Processing Conference, 1221-1224,2004.
[12] Jain, A.K.; Ross, A., Prabhakar, S. An Introduction to Biometric Recognition. IEEE Trans. Circuits Syst. Video Technol., 14, 4-20, 2004.
[13] Tejas, J.; Sommath, D. Multimodal Biometrics: State of the art in Fusion Techniques. Int. J. Biometrics, 4, 393-417, 2009.
[14] Kyungnam Kim, Face Recognition using PCA,Vision and AI Research group, 2001.
[15] Wayne A. Wickelgren, Context-sensitive coding, Associative Memory and serial order in Speech Behaviour, Psychological Review., Vol. 76, No. 1, 1-15, 1969,
[16] 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.
[17] 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
[18] 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.
[19] H. V. Henderson, F. Pukelsheim and S. R. Searle. On the history of the Kronecker product. Linear and Multilinear Algebra. 14:113-120, 1983.
[20] Lester Lipsky and Appie van deLiefvoort, Transformations of the Kronecker Product of Identical Servers to Reduced Product Space, 1995.
[21] John W. Brewer, Kronecker Products and Matrix Calculus in System Analysis, IEEE Transactions on Circuits and Systems, Vol. 25, No. 9, 1978
[22] Wolfgang Hackbusch, Boris N. Khoromskij, Hierarchical Tensor-Product Approximations.
[23] Lubomír Brančík, Matlab Programs for Matrix Exponential Function Derivative Evaluation
[24] 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.
[25] Face databases – AT&T databases, www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
[26] Face FERET Databases - http://www.face-rec.org/databases/
[27] Fingerprint Databases - http://www.advancedsourcecode.com/fingerprintdatabase.asp