FUSION BASED MULTIMODAL AUTHENTICATION IN BIOMETRICS USING CONTEXT-SENSITIVE EXPONENT ASSOCIATIVE MEMORY MODEL : A NOVEL APPROACH

P. E. S. N. Krishna Prasad[1], Pavan Kumar K[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]surya125@gmail.com, [2]pavanpvpsit@gmail.com,
[3]krishna1959@gmail.com and
[4]bdcnprasad@gmail.com

ABSTRACT

Biometrics is one of the primary key concepts of real application domains such as aadhar card, passport, pan card, etc. In such applications user can provide two to three biometrics patterns like face, finger, palm, signature, iris data, and so on. We considered face and finger patterns for encoding and then also for 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 patterns. In stage 1, face and finger patterns can be fusion through Principal Component Analysis (PCA), in stage 2 by applying SVD decomposition to generate keys from the fusion data and pre-processed face pattern and then in stage 3, using CSEAM model the generated keys can be encoded. The final key will be stored in the smart cards. In CSEAM model, exponential kronecker product plays a critical role for encoding and also for verification to verify the chosen samples from the users. This paper discusses by considering realistic biometric data in terms of time and space.

KEYWORDS

Biometrics; Biometric fusion; Face; Finger; Context-Sensitive Exponent Associative Memory Model (CSEAM); Kronecker Product; Exponential Kronecker Product (eKP); Multimodal Authentication;

1. INTRODUCTION

People are far better at perceiving objects in natural scenes and noting their relations, understanding language and retrieving contextually appropriate information from memory, making plans and carrying out contextually appropriate actions, and wide range of other natural cognitive tasks. People are also far better at learning to do these things more accurately and fluently through processing experience.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 81–90, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3608

Artificial Intelligence (AI) is a tool that has the right program which might be able to capture the fluidity and adaptability of human information processing. There have been great breakthroughs in understanding of cognition as a result of the development of powerful algorithms.

The connectionist models or Artificial Neural Networks (ANN) [1, 16], due to the resemblance its processing has 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.

Biometrics [10, 11] are used for measuring and analyzing a person's unique characteristics. There are two types of biometrics: behavioural and physical. The behavioural characteristics are voice, handwritten signature, keyboard strokes, and more. The physiological ones are fingerprint, iris, face, hand geometry, finger geometry, retina, vein structure, ear, and more. Behavioural biometrics are generally used for verification while physical biometrics can be used for either identification or verification.

The physiological characteristic systems are generally more reliable than the ones based on behavioural characteristics. The most commonly used biometrics are fingerprint, face, voice, iris, handwritten signature and hand geometry.

Biometrics [6] plays an important role in public security and information security domains. Using various physiological characteristics of the human, biometrics accurately identifies each individual and distinguishes one from another. The recognition of people is of great importance, since it allows us to have a greater control when a person has access to certain information, area, or simply to identify if the person is the one who claims to be. The achieved results indicate that biometric techniques are much more precise and accurate than the traditional techniques.

Basically a biometric system may operate in verification mode also known as authentication, or identification mode also known as recognition. In identification mode, the system recognizes by searching the templates of all the users in the database for a match. In verification mode, the system validates a person’s identity by comparing the captured biometric data with his / her own biometric.

Multimodal biometric [11] technology uses more than one biometric identifier to compare the identity of the person. Multimodal biometry is based on using different biometric characteristics to improve the recognition rate and reliability of the final result of recognition. For this reason, in this paper, two biometric characteristics such as face and fingerprint of a person are used to achieve a good verification rate of human beings.

In this paper we describe a connectionist approach often called CSEAM [1,3] model to authenticate the multimodal biometrics , in which the first step is to obtain the keys through PCA followed by SVD decomposition and then apply the CSEAM model using ***exponential kronecker product*** [2, 17] to encode the key patterns. In the second step the verification process can be done using the same model.

2. PRELIMINARIES

The Kronecker Product (KP) is the fundamental operation in the Context-Sensitive Exponent Associative memory Model (CSEAM). The operation defined by the symbol ⊗ was first used by Johann Georg Zehfuss in 1858 [17, 19]. It has since been called by various names, including the

Zehfuss product, the Product transformation, the conjunction, the tensor product, the direct product and the Kronecker product. In the end, the Kronecker product stuck as the name for the symbol and operation⊗.

The Kronecker Product of $A_{m\times n} \in \Re\, and\ B_{p\times q} \in \Re$ written $A\otimes B$, is the tensor algebraic operation as

$$A\otimes B = \begin{bmatrix} a_{11}B & a_{12}B \dots\dots\dots & a_{1n}B \\ a_{21}B & a_{22}B \dots\dots\dots & a_{2n}B \\ \vdots & \dots & \vdots \\ a_{m1}B & \dots\dots\dots & a_{mn}B \end{bmatrix}$$

Each $a_{ij}B$ is a block of size $p \times q$. $A\otimes B$ is of size $mp \times nq$.

One advantage of Kronecker product [18] is their compact representation. We assume, the linear system $Cx = d$ in which C can be written as the Kronecker product of two much smaller matrices, A and B. The system $(A\otimes B)x = d$ can be solved quickly without ever forming the full matrix $C = A\otimes B$ only the smaller matrices A and B need to be stored. Suppose $C_{10000x10000}$ can be expressed as the Kronecker product of $A_{100x100}$ and $B_{100x100}$. The linear system $Cx = d$ only requires the storage of two 100x100 matrices. Storage savings and the linear matrix equation problem are just a few of the benefits and applications of the Kronecker product.

2.1 Properties of Kronecker Product:

The elementary properties of the Kronecker Product [17,19, 20]:

- $(A\otimes B)(C\otimes D) = AC\otimes BD$
- $(A\otimes B)^T = A^T\otimes B^T$
- $(A\otimes B)^{-1} = A^{-1}\otimes B^{-1}$
- $tr(A\otimes B) = tr(A)tr(B) = tr(B\otimes A)$
- $||A\otimes B|| = ||A||\,||B||$
- $rank(A\otimes B) = rank(A)rank(B)$
- If A and B are square then $(A\otimes B)^n = A^n\otimes B^n$
- ***Eigen values and Eigen vectors:*** For A and B square, let λ be a member of the spectrum of A. i.e λ ∈ σ(A). Let$x_A$be a corresponding eigenvector of λ and let μ∈ $\sigma(B)$ and x_B be a corresponding eigenvector. Then $\lambda\mu \in \sigma(A\otimes B) and\ x_A\otimes x_B$ is the corresponding eigenvector of $A\otimes B$. That is, every eigenvalue of $A\otimes B$ arises as a product of eigenvalues of A and B.

2.2 Factorizations:

The matrices can be factorized into various ways with the use of Kronecker Product [18, 19] .

a. ***LU:*** Let A be a square nonsingular matrix of order m_A with LU factorization $A = P_A^T L_A U_A$and B be a square nonsingular matrix of order m_B with LU factorization $B = P_B^T L_B U_B$. Then
$$A\otimes B = (P_A^T L_A U_A)\otimes(P_B^T L_B U_B)= (P_A^T\otimes P_B^T)(L_A\otimes L_B)(U_A\otimes U_B)$$

b. ***QR:*** let A be am mxn matrix with linearly independent columns and QR factorization $A = Q_A R_A$, where Q is an mxn matrix with orthonormal columns and R is nxn upper triangular matrix. B is similarly defines with $B = Q_B R_B$ as its QR factorization. Then the QR factorization of A⊗B is
$$A\otimes B = (Q_A R_A)\otimes(Q_B R_B) = (Q_A\otimes Q_B)(R_A\otimes R_B)$$

c. ***Single value Decomposition (SVD)***: Let A be an mxn matrix with singular value decomposition $A = U_A \Sigma_A V_A^T$ and B be an pxq matrix with singular value decomposition $B = U_B\Sigma_B V_B^T$. Let $rank(A) = r_A$ and $rank(B) = r_B$. Then A⊗B has rank $r_A r_B$ and singular value decomposition

$$A\otimes B = \left(U_A\Sigma_A V_A^T\right)\otimes\left(U_B\Sigma_B V_B^T\right) = \left(U_A\otimes U_B\right)(\Sigma_A\otimes\Sigma_B)\left(V_A\otimes V_B\right)$$

Similarly, we can define other factorization approaches such as Schur decomposition, Cholesky decomposition using kronecker Product.

2.3 Exponential of a matrix:

The exponential of a matrix [15,19] A is defined as:

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

Thus, a common method 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. To obtain the exponential of a diagonal matrix, you can compute the exponential of each diagonal element of the matrix A using Pade Approximation. Let A be a diagonal matrix 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 the exponential of a diagonal matrix is as:

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

Similarly, we can compute the exponential of a matrix in different ways discussed in [15, 21] and also to compute natural logarithm of the matrix.

2.4 Properties of Matrix Exponential:

The matrix exponential has several properties [17,19 and 21], 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

2.5 Exponential Kronecker Product (*eKP*):

The exponential function [19] 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 chosen *exponential kronecker product* as *associative memory model* [1, 14 and 16] in the connectionist models often called Context-sensitive Exponent Associative Memory Model (CSEAM).

3. Feature Extraction

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, face and fingerprint image patterns can be fusion using Principal Component Analysis (PCA) [6, 7, 8, 11] 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 an face and fusion sample is also normalized onto values between [0; 1], transformed into a matrix *R* (Figure 1), and then compressed into; *G ∈ F(I × J)*

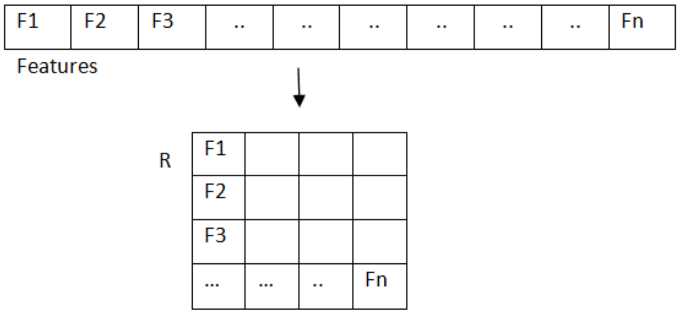

Fig. 1. Feature vector normalized and transformed into Matrix *R*

In the next stage, we apply the SVD factorization on matrix *R*, to obtain the keys 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 and face data with various sizes, the generated keys can supplied to the *connectionist model or ANN model* which chosen here is *Context-sensitive Exponent Associative Memory model (CSEAM)* [1,2] for encoding and verification process. In this model, memory is acted as *exponential kronecker product (eKP)* [16,19], 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 *mp*x*nq* 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 [6].

In the proposed model, the generated keys from fusion and face patterns can be passed to CSAM model for computing exponential kronecker product and the result will be stored in the smart cards for verification.

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

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) [1, 2, 14] 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.

Associative Memory Retrieval (AMR) [3, 13 and 16] is another novel model for memory retrieval that simultaneously enables context based retrieval and spontaneous responses while supporting the revision of retrieval specifications or the inputs of contextual information. The AMR process accepts memory retrieval requests, process them incrementally and accepts revised specifications when provided and provides conclusions on demand.

Context-sensitive memory search [1, 3 and 13] is an innovative model of memory search, working hand to hand within an associative memory that improves the precision of memory search. This model uses cues beyond the questions to guide search, focusing the search effort on the portion of the knowledge base that yields useful answers. This approach enables the priming effort of human memory retrieval as in the cognitive architectures that can be applied to general intelligent systems.

Another important element of CSEAM is a Content Addressable (CA) [2, 14 and 16] store implemented with the experience based knowledge representation. The experience store enables the CSEAM model to apply in a variety of tasks.

Content Addressability (CA) is the one very prominent feature of human memory. It seems fairly clear that can access information in memory based on nearly any attribute of the representation that are trying to retrieve. It is possible to implement some kind of content addressability of memory on a standard computer in a variety of different ways. A more efficient scheme involves some form of indexing, keeping a list, for each content a memory might have, of which memories have that content. Such an indexing scheme can be made to work with error-free probes, but it will break down if there is an error in the specification of the retrieval cue. There are possible ways of recovering from such errors, but they lead to the kind of combinatorial explosions which plague this kind of computer implementation. One way is to search the patterns as cue by examining each memory in the system to find the memory or the set of memories which has the particular content specified in the cue.

Each memory is represented by a unit which has mutually excitatory interactions with units standing for each of its properties. Then, whenever any property of the memory became active, the memory would tend to be activated, and whenever the memory was activated, all of its contents would tend to become activated. Such a scheme would automatically produce content addressability

Here, CSEAM model [1, 2 and 14] described using the concept of vector logic, which is one of the prime logic mechanisms to store and retrieval of 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 not by where it is stored in the neural pathways of the brain.

The performance of associative memory is its memory capacity and content addressability. The capacity of memory refers to the maximum number of associated pattern pairs that can be stored and correctly retrieved based on the content addressability, is the ability of the network to retrieve the correct stored patterns.

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

5. Proposed Model

In this paper, we proposed this model for recognition and authentication of biometric data [4, 5, 9]. 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 2(a) and 2(b). 2(a) represents the recognition of the biometrics to train the network using CSEAM model and generate a memory. 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.

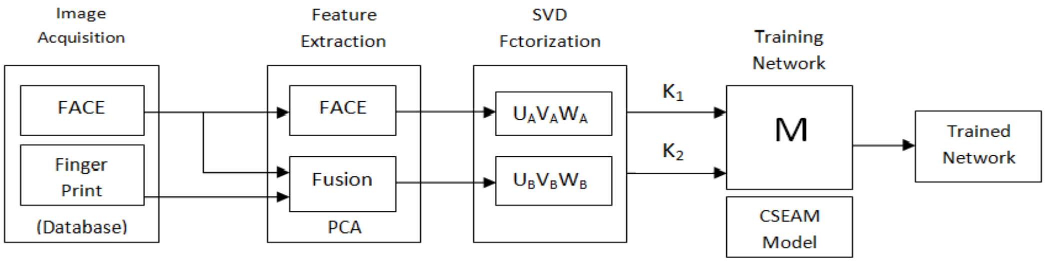

Fig: 2(a): Recognition of Biometric system using CSEAM Model

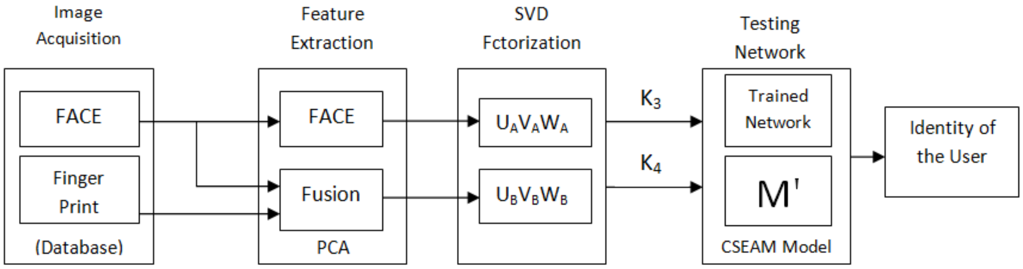

Fig: 2(a): Verification of Biometric system using CSEAM Model

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 factorization. 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 the some performance metrics such as mean square error (MSE). In this model, we fix the threshold of MSE with the value of *d*= 0.001 based on the normalized error, which is minimum of the tested samples. Based on this threshold error, the user provided data will be verified by using the proposed model

6. Experiment Analysis

In the experiments conducted on this model, we test the verification performance on the standard databases from [23, 24 and 25], 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) [22] 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 is given in the table1 with different sizes such as 8x8,16x16,....,64x64 on similar and dissimilar face and fingerprint patterns.

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

Based on the methodology to characterize a biometric system, FNMR and FMR parameters have been calculated. It is assumed that there are no errors in the acquisition; therefore FAR/FMR and FRR/FNMR pairs are equivalent.

False match rate (FMR) 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) 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*: $MSE>d$.

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

By the observation of the experimental results, it is notified that the key sizes 8x8 and 16x16, have been encountered in rejecting rate when provided similar biometric data patterns (FMR).

7. CONCLUSIONS

In this paper, we proposed a novel model in the cognitive logic often referred as CSEAM model for authentication/ verification of the biometrics data in multimodal authentication. This model gives better results from the chosen databases and provides more complex security in terms of time and space, since it uses exponential kronecker product in the vector logic. 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] 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.

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

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

[4] 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.

[5] 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.

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

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

[8] 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

[9] Arun Ross and Anil K. Jain, Multimodel Biometrics: an Overview, 12th European Signal Processing Conference, 1221-1224,2004.

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

[11] Tejas, J.; Sommath, D. Multimodal Biometrics: State of the art in Fusion Techniques. Int. J. Biometrics, 4, 393-417, 2009.

[12] Kyungnam Kim, Face Recognition using PCA,Vision and AI Research group, 2001.

[13] Wayne A. Wickelgren, Context-sensitive coding, Associative Memory and serial order in Speech Behaviour, Psychological Review., Vol. 76, No. 1, 1-15, 1969,

[14] 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.

[15] 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

[16] 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.

[17] H. V. Henderson, F. Pukelsheim and S. R. Searle. On the history of the Kronecker product. Linear and Multilinear Algebra. 14:113-120, 1983.

[18] Lester Lipsky and Appie van deLiefvoort, Transformations of the Kronecker Product of Identical Servers to Reduced Product Space, 1995.

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

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

[21] Lubomír Brančík, Matlab Programs for Matrix Exponential Function Derivative Evaluation

[22] 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.

[23] Face databases – AT&T databases, www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[24] Face FERET Databases - http://www.face-rec.org/databases/

[25] Fingerprint Databases - http://www.advancedsourcecode.com/fingerprintdatabase.asp