A Fusion Approach for Signature Recognition

M. Mani Roja and Sudhir Sawarkar

***Abstract*—A new approach for the personal authentication using signatures is presented. This paper attempts to improve the performance of signature based authentication system by integrating multiple algorithms. The signatures are acquired using digital pen tablet and then features are extracted. These features are then examined for their combined performances. Our experimental results on the image data set from 30 users confirm the advantages of our fusion technique using simple image acquisition.**

***Index Terms*—Image processing, discrete cosine Transform, singular value decomposition**

I. Introduction

Reliability in the personal authentication is key to the security in the networked society. Many physiological characters of human are typically time invariant, easy to acquire and unique for every individual. Biometric features such as face, iris, finger print, signature etc have been suggested for the security in access control. Most of the current research in biometrics is based on finger print and face. The reliability of personal authentication using face is currently low as the researchers today continue to grapple with problem of pose, lighting, orientation and gesture. Finger print identification is widely used in personal identification, as it works well in most cases. However it is difficult to acquire finger print features i.e. minutiae for some class of persons as manual labourers, elderly people etc. As a result, other biometric characteristics are receiving increasing attention [1].

Signature verification by computers has received extensive research interest in the field of pattern recognition.

As ones signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public makes it more suitable for lower authentication needs. Use of signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction on his or her authentication method.

Signature verification system can be generally divided into two categories: a static method (called as Offline) that extracts shape related information and dynamic method (called as Online) with time related information [1]. In the former method, the input is a two dimensional signature image captured by a scanner or other imaging device. Since Offline signature verification system extracts shape related information which can be imitated therefore it is generally used for lower authentication needs and it is useful in automatic verification of signatures found on bank cheque and documents. In the latter case, a digital pen tablet together with an instructed pen is used to obtain the online information of pencil tip. Online signature verification system extracts dynamic features such as speed, pressure, time information which can not be imitated. Therefore it is used for higher authentication like protection of personal devices and authentication of individuals for access to buildings and so on.

A. Types of Forgery

The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability [2]. There are three different types of forgeries to take into account. The first, known as random forgery, is usually represented by a signature sample which belongs to a different writer of the signature model. The second, called simple forgery, is represented by a signature sample which has the same shape as the genuine writer's name. The last type is so-called skilled forgery, represented by a suitable imitation of the genuine signature model.

Each type of forgery requires a different verification approach. Methods based on the static approach are generally used to identify random and simple forgeries. The reason for this is that these methods have proven to be more suitable for describing characteristics related to the signature shape. A skilled forgery has practically the same shape as the genuine signature. Therefore, methods based on dynamic (online) or pseudo dynamic approaches have been shown to be more robust for identifying this kind of forgery.

For many years the problem of signature verification has generally been solved by some authorities or clerical employee, however with the invention of computers and scanning devices the trend has been towards automation of the whole process. The accuracy of offline signature verification system depends upon the robustness of feature vector. As a consequence, more and more researchers have looked into the feature extraction methodology of signature recognition and verification. This methodology can be based on one of the following.

- Global features
- Statistical features
- Geometrical and topological features

The classifier modules are like neural network [3], [4],

Manuscript received June 10, 2012; revised July 27, 2012.

M. Mani Roja is a Research Scholar from Sant Gadge Baba Amravati University and Associate Professor in the Electronics and Telecommunication Engineering Department, Thadomal Shahani Engineering College, 400050, India (e-mail: maniroja@yahoo.com).

Sudhir Sawarkar is the Principal of Data Meghe College of Engineering, Airoli Navi Mumbai, Maharashtra 400708, India (e-mail: sudhir_sawarkar@yahoo.com).

Hidden Markov model (HMM) [5], [6], and Euclidean distance classifier [7], [8] support vector machine [9] and many more are used as classifiers in signature recognition system. This paper focuses on semi online signature verification using fusion approach for low level online authentication and offline applications. This paper is organized as follows. Section II describes the proposed system. Section III discusses the algorithms used. Sections IV provide the information about the fusion. Section V discusses the experimental procedure and results. Section VI draws the conclusion and future scope of this work.

II. Proposed System

The block diagram of the proposed method for signature authentication is shown in Fig.1. The signature from every user is acquired using the pen tablet. After pre processing, the number of pixels in each row and column are extracted .Statistical parameters, decomposed singular values (SVD) and discrete cosine transform (DCT) coefficients are calculated as feature vectors. These parameters are matched with the parameters corresponding to their respective signature images from the data base. In decision level fusion, individual decisions are taken and final decision is based on the logical operation between these decisions. In match score level fusion, matching scores from these classifiers are combined and a combined matching score is obtained which is used to take a final decision.

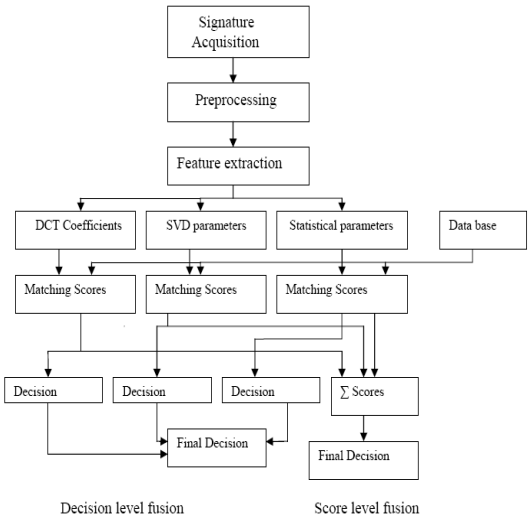

Fig. 1. Block Diagram of signature recognition system

A. Image Acquisition and Pre-processing

Our image acquisition is inherently simple and does not employ any special illumination. The WACOM bamboo digital pen tablet as shown in Fig 2 was used to acquire the signatures. Ten signature samples from 30 users have been collected. Hence our data base consists of 300 signature samples. These images have different dimensions therefore images are scaled to a dimension of 128×256. After scaling, the next step is colour normalization and binarization. After this, image becomes ready for feature extraction phase. Since image has 128 rows and 256 columns, counting the number of pixels in each column gives a row vector of size 128 and counting the number of pixels in each column gives a column vector of size 256.

Fig. 2. Wacom digital pen tablet

B. Information Fusion and Matching Criteria

In the context of biometrics, three levels of fusion schemes have been suggested [8].

1) Fusion at Feature level: Each individual biometric process outputs a collection of features. The fusion process fuses these collections into a single feature set or vector.
2) Fusion at score level: Each individual biometric process outputs a match score. The fusion process fuses these into a single score, which is then compared to the system acceptable threshold.
3) Fusion at decision level: Each individual biometric process outputs its own Boolean result. The fusion process fuses them together by a combination algorithm such as AND, OR etc.

C. Score Normalization

A normalization step is necessary before the raw scores originating from different matchers can be combined in the fusion stage. For example, if one matcher yields scores in the range [100, 1000] and another matcher in the range [0, 1], fusing the scores without normalization effectively eliminates the contribution of second matcher. We have used TanH normalization technique. It maps the score to [0, 1] range .We denote the raw match score as S and the corresponding normalized score as S'. Using TanH approach, S' is calculated as

$$s' = \frac{1}{2}\left[\tanh 0.01\left(\frac{s - mean(s)}{std(s)}\right) + 1\right] \quad \text{nn} \quad (1)$$

where mean and std denotes the mean and standard deviation.

D. Fusion

The normalized outputs of the two matching modules are combined using fusion at the matching score level. The fusion is expressed by means of the total similarity measure TSM [10].

$$TSM = w_1 s_1 + w_2 s_2 + w_3 s_3 \quad (2)$$

where w_1, w_2 and w_2 are weight factors and the weights are set proportional to their unimodal recognition result.

III. Implementation

A. Statistical Method

After finding row and column vectors, we calculate mean, standard deviation and moment of these vectors using

following formulae: Given a vector r_i where i = 1, 2, 3...n

Mean

$$M1 = \frac{\sum_{i=1}^{n} r_i}{n} \quad (3)$$

Variance

$$\sigma^2 = \frac{\sum_{i=1}^{n} (r_i - M_1)^2}{n} \quad (4)$$

The variance value is not directly taken as a feature, since it is a squared value it can dominate other features so we take square root of variance which is also called as Standard deviation. Therefore the next feature is:-

$$V_1 = \sqrt{\sigma^2} \quad (5)$$

The third moment also, is not taken directly as the feature vector because since it is a cube value, it can dominate the other values in the feature vector while finding the Euclidean distance. Therefore cube root of the third moment is taken as a feature. Sometimes it is possible that the value of moment may come negative. In this case, we first make the value of moment positive, then take the cube root and after that again the negative sign is assigned to the value. So the next feature is cube root of the third moment which is given as below:

$$\text{Third moment} = M_3 = \frac{\sum_{i=1}^{n} (r_i - M_1)^3}{n} \quad (6)$$

If the moment is positive then

$$M_{o1} = \sqrt[3]{M_3} \quad (7)$$

If the moment is negative then

$$X = -M_3 \quad (8)$$

and

$$M_{o1} = -\sqrt[3]{X} \quad (9)$$

Feature vector = $[M_1, V_1, M_{o1}, M_2, V_2, M_{o2}]$

B. Singular Value Decomposition Method

The singular value decomposition of image A is a decomposition of the form [11]

$$A = UDV^T \quad (10)$$

where A is m x n matrix, U and V are orthogonal matrices. D is a diagonal matrix of singular values,

The singular values $\sigma_1 \geq \sigma_2 \geq \sigma_3 ..... \sigma_n \geq 0$ appear in descending order along the main diagonal of D. The singular values are obtained by taking the square root the of Eigan values of AA^T and A^TA.Hence the image A can be represented as

$$A = [U_1, U_2, ...U_N] \begin{bmatrix} \sigma_1 & 0 & ... & 0 \\ 0 & \sigma_2 & ... & 0 \\ & & ..... & \\ 0 & 0 & .... & \sigma_N \end{bmatrix} \begin{bmatrix} V_1^T \\ V_2^T \\ . \\ . \\ V_N^T \end{bmatrix} \quad (11)$$

The U and V vector are calculated as the Eigen vectors of AA^T and A^TA respectively. The square roots of the Eigen values are the singular values along the diagonal of the matrix D. Since our signature is resized to 128 x 256, we get a total of 128 singular values, out of which we consider the first 64 values as feature vectors.

C. Discrete Cosine Transform

DCT is [12] a well-known signal analysis tool used in compression due to its compact representation power. It's known that Karhunen-Loeve transform (KLT) is the optimal transform in terms of information packing, however, its data dependent nature makes it infeasible to implement in some practical tasks. Moreover, DCT closely approximates the compact representation ability of the KLT, which makes it a very useful tool for signal representation both in terms of information packing and in terms of computational complexity due to its data independent nature.

DCT helps in separating the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to Discrete Fourier transform (DFT): it transforms a signal or image from the spatial domain to the frequency domain. The general equation for a 1D (*N* data items) DCT is defined by the following equation:

$$F(u) = \sqrt{\left(\frac{2}{N}\right)} \sum_{i=0}^{N-1} A(i) * \cos\left(\frac{u(2i+1)\pi}{2N}\right) * f(i) \quad (12)$$

where, $A(i) = \frac{1}{\sqrt{2}}$ for u = 0

= 1 otherwise

and $f(i)$ is the input sequence.

Using equation 12, the DCT coefficients are calculated for the row and column vectors. Hence we get a total of 384 DCT coefficients. Since DCT is having very good energy compaction, we have considered only 36 DCT coefficients as feature vectors.

IV. Experiments and Results

A. Testing for Accuracy

In global system, 5 genuine signatures are selected for each subject. Signatures not involves in training process are used for system performance evaluation. In testing phase, when the test signature is entered, the feature vector corresponding to this signature is calculated and it is compared with the feature vector of each of the 150 signatures. For comparison, we use Euclidean distance model which calculates the

Euclidean distance between feature vector of the test signature and feature vectors of the database signatures [13]. The formula for Euclidean distance is given as follows:

Let A (a_1, a_2 ... a_n) and B (b_1, b_2 …bn) are two vectors of size n. We can calculate distance by equation 13 as

$$d = \sqrt{\sum_{i=1}^{n} (a_i - b_i)^2} \quad (13)$$

As we are comparing the feature vector of test signature with all 150 feature vectors in the database, we have total 150 Euclidean distances which are then sorted in the ascending order and stored in an array. The first element of this array indicates smallest Euclidean distance that means the signature corresponding to this Euclidean distance matches the most with the test signature. While testing the performance of the system we calculate true acceptation rate (TAR) which indicates number of correctly accepted signatures. Equation 14 gives formula for TAR.

$$\text{TAR} = \frac{\text{Number of genuine signatures matched}}{\text{Total number of signatures in block (150)}} \times 100 \quad (14)$$

B. Procedure for Authentication

Our system is designed for offline applications and low level online authentication applications. The person who wants to authenticated is provided with the digital tablet for the purpose of collecting test signature sample. The feature vectors from this test signature are extracted and compared with the feature vectors of database signatures. Match cores are generated using Euclidean distance classifier. If there is a match, authentication is granted otherwise, the person is denied from access.

V. Result

The results of unimodal signature recognition with three algorithms are listed in Table I.We got a recognition rate of 62% using statistical parameters, 61% with singular values and 79% with DCT coefficients.

TABLE I: Results of Unimodal Techniques

Technique	TAR in %	Training period In seconds
Statistical	62.3	20
SVD	61	40
DCT	79.3	17

For the uni modal techniques, we have got a very low level recognition rate. Hence to improve the rate, we have considered two types of fusion techniques: score level fusion and decision level fusion. The results for match score level fusion is given in Table II.

TABLE II: Results of Match Score Level Fusion

Technique	TAR in %	Training period In seconds
Statistical +SVD	71	55
DCT+SVD	80	56
Statistical +DCT	82	32
Statistical +SVD+DCT	85	71

The results of decision level fusion are given in Table III. We have considered AND logic and OR logic as the fusion techniques. AND logic can be used for high level authentication like security applications and OR logic can be used for low level authentication like giving attendance.

TABLE III: Results of Decision Level Fusion

Technique	TAR in % AND	TAR in % OR
Statistical +SVD	36	76
DCT+SVD	48	87
Statistical +DCT	46	87.3
Statistical +SVD+DCT	31	93

Using decision level fusion with logical OR, we have false acceptation ratio of 7%, with respect to the Euclidean distance for random forgeries and the true acceptation rate is 93%. We have also tested the algorithm separately for random forgeries and simple forgeries. Random forgeries are taken from database itself and simple forgeries are collected from different persons. But our system is not giving satisfactory results with AND logic.

VI. Conclusion

The objective of this work was to investigate the fusion approach for signature recognition to achieve higher performance that may not be possible with single biometric indicator alone. The achieved results are significant since the three biometric matching scores are derived from the same image unlike other biomedical biometric system which requires three different sensor/images. Our results show that decision level fusion using OR logic scheme with Tanh normalization score achieves better performance than those for fusion at the score level. Our system gives a TAR of 93% in case of low level online authentication. Currently we are trying to improve the TAR by incorporating additional algorithms for signature authentication.

References

[1] D. Kalenova, "Personal Authentication Using Signature Recognition," *department of Information technolo*gy, Lappeenranta University of technology.

[2] E. J. R. Justino, F. Bortolozzi, and R. Sabourin, "The Interpersonal and Intrapersonal Variability Influences on Off-line signature Verification Using HMM," in *Proceedings of 15th Brazilian symposium on computer graphics and image processing*, pp. 197-202, 2002

[3] T. Kaewkongka, K. Chamnongthai, and B. Thipakorn, " Off-Line Signature Recognition using parameterized Hough Transform," *5th International Symposium on Signal Processing and its Applications*, vol. 1, August 1999, pp. 451-454.

[4] S. Armand, M. Blumenstein, and V. Muthukkumarasamy, "Off-Line Signature Verification based on the Modified Direction Feature," *18th International conference on pattern recognition*, vol. 4, pp. 509-512, 2006.

[5] J. Coetzer, B. M.Herbst, J. A. D. Preez, " Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model," *EURASIP Journal on Aplplied Signal Processing*, 2004, vol. 4, pp 559-571.

[6] E. J. R. Justino, A. E. Yacoubi, F. Bortolozzi, and R. Sabourin, "An Off-line Signature Verification System Using HMM and Graphometric Features," 2002.

[7] M. A. Ferrer, J. B. Alonso, and C. M. Travieso, "Offline Geometric Parameter For Automatic signature Verification Using Fixed- Point Arithmetic," *IEEE Transaction On Pattern Analysis and Machine Intelligence*, vol. 27, no .6, pp. 993- 997, June 2005.

[8] T. Ko, "Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition," in *Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05)*, 2005.
[9] M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. K. Jain, "Multimodal biometric authentication methods: A COTS approach," in *Proc. of Workshop on Multimodal User Authentication*, (Santa Barbara, CA), pp. 99–106, Dec 2003.
[10] R. Ivan, "A Biometric Identification System Based on Eigen palm and Eigen finger Features," *IEEE Trans. on Patt. Anal. and Mach. Intel*, vol. 16, Nov, 2005
[11] S. Sayeed, N. S. Kamel, and R. Besar, "A Sensor-Based Approach for Dynamic Signature Verification using Data Glove," *Signal Processing: An International Journal*, vol. 2, no. 1.
[12] B. Majhi, Y. S. Reddy, and D. P. Babu, "Novel Features for Off-line Signature Verification," *International Journal of computers, communication and contr*ol, vol. 1, no. 1, pp. 17-24, 2006.
[13] I. A. Ismail, M. A. Ramadan, T. S. E. Danaf, and A. H. Samak, "An Efficient Off-line Signature Identification Method Based On Fourier Descriptor and Chain Codes," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 5, May 2010, pp. 29-35.

M. Mani Roja was born in Tirunelveli (T.N.) in India on June 19, 1969. She has received B.E. in Electronics & Communication Engineering from GCE Tirunelveli, Madurai Kamraj University in 1990, and M.E. in Electronics from Mumbai University in 2002. Her employment experience includes 21 years as an educationist at Thadomal Shahani Engineering College (TSEC), Mumbai University. She holds the post of an Associate Professor in TSEC. Her special fields of interest include Image Processing and Data Encryption. Currently, she is persuing her PhD from Sant Gadge Baba Amravati University. She has over 20 papers in National / International Conferences and Journals to her credit. Ms. M.Mani Roja is a member of IETE, ISTE, IACSIT and ACM.

Sudhir Sawarkar was born in Amravati, Maharashtra in India on October, 1966. He received his BE (Electronics) and ME (Electronics) from Sant Gadge Baba Amravati University, India in 1988 and 1995 respectively. He received his PhD degree in 2007 from Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra India.

He is currently working as a Principal of Datta Meghe college of Engineering, Navi Mumbai. His employment experience includes 24 years in teaching. He has published more than 25 research papers in national / international journals /conferences. He has guided many M Tech and ME dissertations. He is a recognized PhD supervisor in Amravati University nd many other universities.