off line signature verification (SV),
Particle Swarm Optimization (PSO),
Neural Networks (NN), Chi square test, PSO-NN

M.T. DAŞ[**], L.C. DULGER and H.E. DULGER[**]

A STATISTICAL APPROACH FOR OFF-LINE SIGNATURE VERIFICATION (SV)

This paper includes off line Signature Verification (SV) process with test results using the proposed algorithm Particle Swarm Optimization-Neural Network (PSO-NN) together with statistical analysis, Chi-square test. The verification process is performed in four steps. Signature images are scanned (data acquisition) and image processing is applied to make images suitable for extracting features (pre-processing). Each pre-processed image is then used to extract relevant geometric parameters (feature extraction) that can distinguish signatures of different volunteers. Finally, the proposed verification algorithm is tested on the database that includes 1350 skilled and genuine signatures taken from 25 volunteers. The Chi-square test is applied to see how the signature data fits with probability test function.

1. INTRODUCTION

Signature is a behavioural biometric and is important for personal verification. There is no doubt about its acceptability in legal documents worldwide. Signature always appears on letters, cheques and all legal documents. Each writer produces a particular pattern during signing. Variations occur in size, connections and alignment. An individual's signature may change overtime depending on many reasons such as age, time, psychological or mental state [9, 13, 15]. A forgery may be prepared in several ways and mainly known as "*random forgery*" and "*unskilled forgery*". The hardest verification problem is "*skilled forgery*". The rejection rates of the random and unskilled forgeries are higher than skilled one. The most important characteristics of the signatures are crossings, upstrokes, enclosed areas, curves and loops. Characteristic of a signature can be seen in Figure 1. Studies on SV are continuously improving. The verification rates are not accepted as sufficient enough in studies. No system is available that can verify signatures with 100% accuracy at present applications. Researchers address the issues important on signature verification nearly 25 years of time [12]. A literature on off-line SV is already performed based on verification algorithms, pre-processing techniques, and extraction processes in use. The most appealing approaches are taken as as Neural Networks (NNs), Hidden Markov Models (HMM) and the other approaches. Many reference studies (80) are included in [3]. Das has presented a Ph.D study on design and implementation of biometric recognition using off line signature analysis [4]. Previously an introductory study has been presented [5] on off-line SV with a small signature data base. The study is then extended with a package for document analysis and SV, Image Processing for Questioned Documents (IMPQD) has been introduced in the same study [5].

The problem of off-line signature verification addressed here. A SV system has been performed using PSO-NN algorithm. A SV toolbox is developed in the study; data acquisition, pre processing, feature extraction, comparison process and performance evaluation for the verification process are performed. Two different data sets are prepared; one for '*Forgery*' and the other one for '*Genuine*' signatures. Finally a decision is made to accept or reject the signature based on FAR (False Acceptance Rate) and FRR (False Rejection Rate) measures to give performance of biometric system. The verification results are presented with histogram plots and probability measures by looking at distributions available.

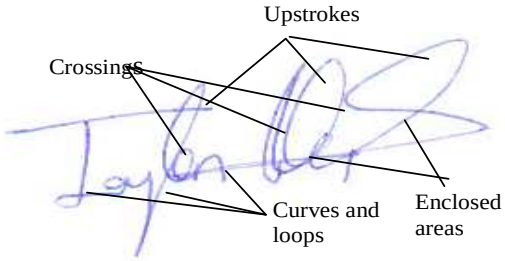


Fig. 1. Characteristic of the signature

2. IMAGE PROCESSING SOFTWARE

Image Processing of Questioned Document (IMPQD) is developed by using C++ Builder 6.0. [5] At Gaziantep University, Dept. of Mech. Eng. Menu options of the package can be seen in Figure 2. It includes all image processing features. In addition to classical menu toolbox, image processing applications, SV toolbox, a camera control and a position

* Roketsan Company[*],Elmadağ-Ankara/TURKEY, Gaziantep University, Faculty of Engineering, Mechanical Eng. Dept. Gaziantep University, Faculty of Medicine, Forensic Science[**], Gaziantep/TURKEY tdas@roketsan.com.tr, dulger@gantep.edu.tr, edulger@gantep.edu.tr

control of a table can be performed with IMPQD. Details of default of IMPQD can be seen in Table 1. Camera controller is embedded into the software which is connected to PC with IEEE 1394 protocol. The execution of software can be used in any traditional Pentium 4 PC without any additional software. The verification process only requires C compiler. Basic and advanced image processing algorithms have been adapted on IMPQD software in this paper. IMPQD supports the data file formats which are *.JPEG (Joint photographic experts group), *.PNG(Portable network graphics) *.TIFF(Tagged image file format), *.GIF(Graphical Interchange Format), *.BMP(Bit-mapped format).

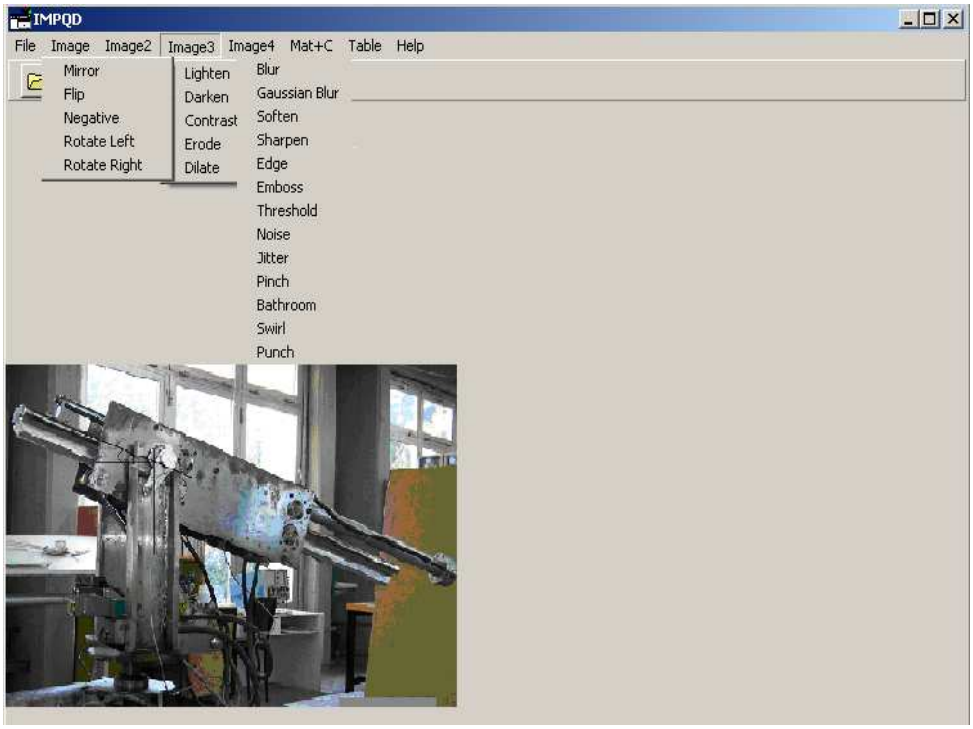


Fig. 2. IMPQD with Image Processing Units (8 Dialogue boxes) [5]

Table 1. The default of IMPQD

File	**New, Open, Save, Save As, Print, Send, Exit**
Image	Mirror, Flip, Negative, Rotate Left, Rotate Right, Skew, Resample
Image 2	Gray Scale, Negative, Dither
Image 3	Lighten, Darken, Contrast, Erode, Dilate
Image 4	Blur, Gaussian, Median, Soften, Sharpen, Edge, Emboss, Threshold, Noise, Jitter, Pinch, Bathroom, Swirl, Punch
Mat + C	Neural Network (NN) and Signature Verification (SV) Toolbox
Table Control	X-Y table and Camera controller
Help	About

3. SIGNATURE VERIFICATION (SV)

A verification approach based on PSO-NN is developed to recognize the genuine signatures from forgeries with reliable accuracy. Parameters of the proposed method are adjusted which are number of particles (variable), dimension which is constant for each application for example dimension is 608 for 18 input, and 32 nodes for the hidden layer, the number of parameters and the constants for NN and PSO (λ, c_1,c_2,etc…) in training process. After training, weights of the network are obtained in data file that is used in testing of the algorithm. Finally, the program is run for the testing part of the signatures. "Grupo de Procesado Digital de Senales"(GPDS) database [6] and also new signatures are collected from Mechanical Engineering Department, Gaziantep University. Scanner views with 300dpi and 8 bit are used for collecting signatures. GPDS consists of 160 sets of signatures; and for each set, 24 samples of genuine and 30 samples of forgeries were available. Genuine and skilled forgeries taken from the data base are shown in Figure 3. In this paper, 25 new sets of signatures have been used. The user needs to specify a local region of most interest. A cropping tool is provided so that the user can scissor-out a region of interest (ROI) from the original document.

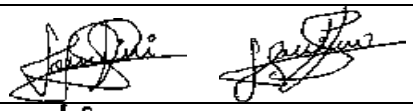
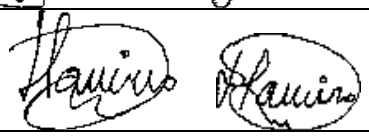
Genuine	Skilled Forgeries
	
	

Fig. 3. Signature samples from the database [6]

Two types of image division can be obtained on the signatures in SV toolbox successively; "*the vertical equal size distribution*" and "*equal size distribution*". In the first approach, signature is divided in equal size box vertically or horizontally. The division direction can be chosen by the user for both horizontal and vertical directions. Dimension of the boxes can be chosen from SV toolbox. In the second approach; signature is divided as the same dimension pixel size for the each column and row which is available application in the literature. After division process, extraction is applied automatically on to the image. Width and height ratio, position of centre of gravity in each part is calculated. Normal angle with respect to centre of gravity of signature is extracted. Figures 4.(a) and (b) illustrate the general interface of software and the extracted signatures. In the program, many parameters can be adjusted by the user. To obtain better performance of the algorithm, the different numbers of division applications are also applied on to the signatures.

4. APPLICATION RESULTS

Implementation of the algorithm to SV is a not an easy task. One signature does not describe the signature distribution of any writer. In the study, having performed image processing and feature extraction, the extracted data are divided into two parts (training and testing) which are then normalized. Normalization is performed between '0' to '1' for each signature. Near to '1' represents 'the genuine signature' and '0' represents 'the forged signature for output values. During application, 25 sets of 54 different signatures have been used while verification. Numbers of 24 genuine and 30 forgery signatures have been performed for each set. Genuine 15 signatures and 16 forgery signatures are trained for NN training. PSO-NN algorithm has 40 particles and 5000 iteration.

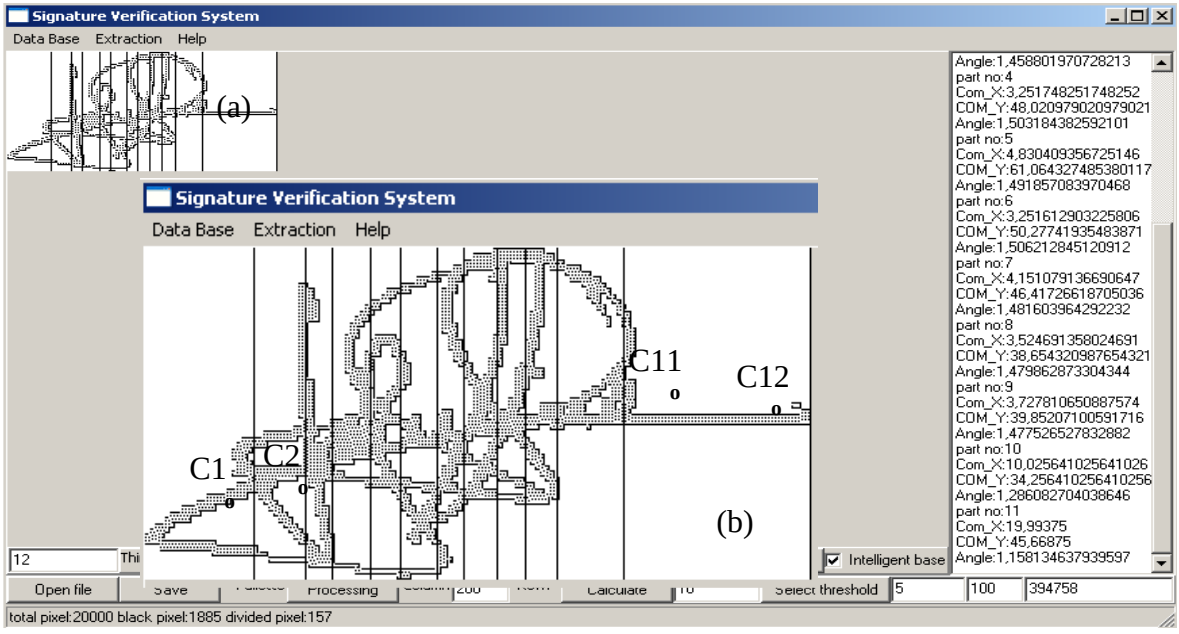


Fig. 4. (a) SV toolbox used in verification (b) Sample Signature used in extraction, C1, C2,…C11 and C12 are the centres of gravity for the divided parts

Input nodes (18) are adapted for each input set and hidden layer (32) nodes adapted system with trials in the training section. Parameters of the network have been used with 0.8 learning rate and λ is 1. Results have been tested with rest of the signatures. Trials have been executed on a P4 2800 MHz CPU, 512 MB PC.

4.1. THE FALSE REJECTION RATE(FRR) AND THE FALSE ACCEPTANCE RATE (FAR)

The false rejection rate (FRR) and the false acceptance rate (FAR) for a biometric device are defined as; the distribution of FAR and FRR is shown in Figure 5. FRR is defined as number of failed attempts at authentication by authorized users divided to number of attempts at authentication by authorized users. FAR is defined as number of successful authentications by impostors divided to number of attempts at authentication by impostors. Both FRR and FAR measure the percent of invalid matches respectively. Both FAR and FRR are dependent on the adjustable adopted threshold. A higher threshold is caused to increase FAR while FRR will decrease. When the value of threshold is decreased, the proportion FAR will decrease, while FRR increases [7, 16]. Equal Error Rate (EER) is the intersection point of FAR and FRR on the coordinate system as shown in Figure 5. Verification results on signatures can then be seen in Table 2.

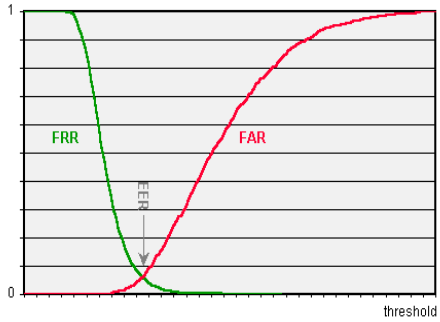


Fig. 5. FAR - FRR Diagram

According to the results, the verification system has 26.85% FAR. This means that 94 skilled forgeries are accepted incorrectly from 350 forgeries. On the other hand, the verification system has given 17.33% FRR which tells 39 genuine samples are rejected in 225 signatures by mistake. Thus the experiments on data base have shown comparable performance. Table 3 illustrates the results of system for 25 samples.

Table 2. Verification Results of Signature Database [5]

	Tested	**Accepted**	**Rejected**	**Results in %**
Skilled	350	94	256	26.85 FAR
Genuine	225	186	39	17.33 FRR

Table 3. Verification Results for 25 samples [5]

	Genuine		***Skilled Forgery***	
No of samples	**Accepted**	**Rejected**	**Accepted**	**Rejected**
1	8	*1*	3	*11*
2	7	*2*	5	*9*
3	8	*1*	4	*10*
4	8	*1*	3	*11*
5	6	*3*	6	*8*
6	8	*1*	3	*11*
7	8	*1*	4	*10*
8	7	*2*	3	*11*
9	8	*1*	4	*10*
10	7	*2*	3	*11*
11	7	*2*	3	*11*
12	6	*3*	5	*9*
13	8	*1*	3	*11*
14	8	*1*	3	*11*
15	8	*1*	4	*10*
16	7	*2*	5	*9*
17	8	*1*	3	*11*
18	6	*3*	4	*10*
19	8	*1*	4	*10*
20	7	*2*	5	*9*
21	7	*2*	4	*10*
22	8	*1*	3	*11*
23	7	*2*	4	*10*
24	8	*1*	3	*11*
25	8	*1*	3	*11*
Total	186	*39*	94	*256*

5. COMPARISON OF VERIFICATION ACCURACIES

Some of the successful verification rates seen in literature are compared with PSO-NN method applied. Comparisons can be made with the error rates obtained, or verification rates seen or conducting hypothesis testing in general. By observing the results obtained in Table 3, some of the studies are chosen to be a base for our SV paper given here. Verification efficiency of PSO-NN is compared with the Resilient Back Propagation (RBP) Neural Network and the Radial Basis Function (RBF) network [1]. Armand et al. have been studied off-line SV using an enhanced modified direction feature (MDF) with NN approaches. MDF is defined as combination of direction feature and transition feature which are described in reference [11]. Addition to MDF, centroid feature(C), tri surface feature (T), length feature (L), six fold-surface feature (S) and the best-fit features (F) have been used with different applications. GPDS database (44 samples), 135 input values from each signature have been used for verification process. The genuine set, 20 samples of each signature have been used for training, 4 samples for testing. For the forged signatures, 25 samples of each signature have been used for training, 5 samples are applied for testing. Number of hidden layer (40) and number of iteration (10000) have been chosen during experimentation. Verification rate for RBP is 88.64% with 1.16% error rate using a single NN. The second one is the RBF which is 89.77% verification rate and 1.22% error rate. Due to the differences in experimental methodology and database size chosen, the comparisons between studies are not accurate. The other system performance which is used in skilled forgery verification has been seen as 23.18 FAR %, and 20.62 FRR% [10]. Kalera et al. [10] have been used Bayes and k-nearest classifier in the off-line SV. Overall accuracy of system is given 78.1% means. The average error rate for verification is given 21.9%. The general result will be based on probability of the verification rates.

6. STATISTICAL ANALYSIS

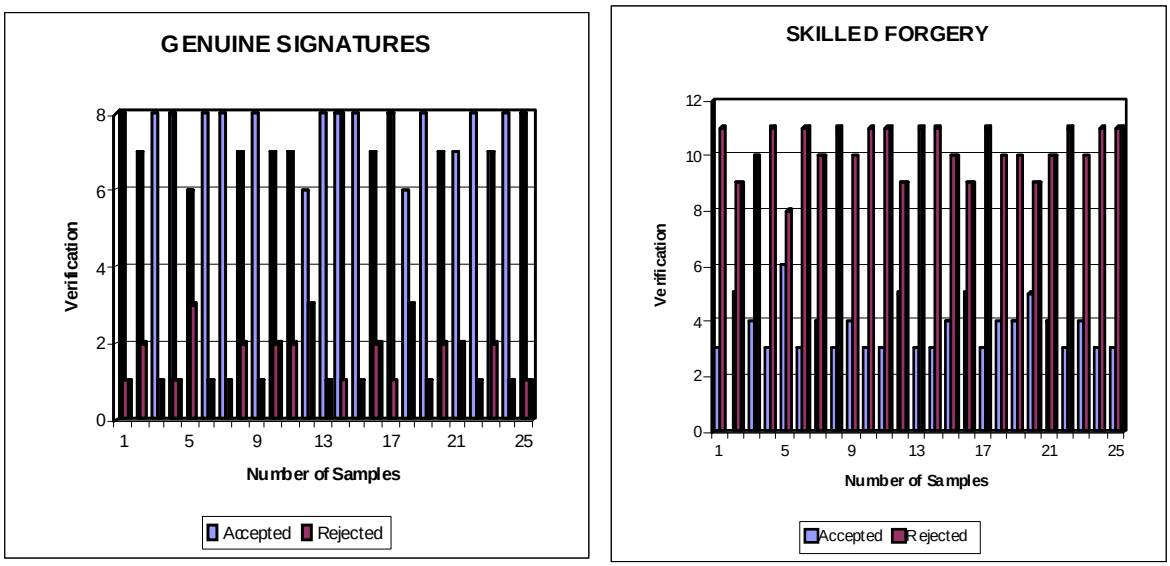
Initially a histogram plot is presented where each sample is studied with equal bins. Here '*population*' refers the entire collection of objects, measurements, observations. GPDS data base is *population* referred in this paper. Similarly, a sample is a subset of population on which the method is applied, 25 sample set are performed. The data given in Table 3 can be visualized better by plotting them in the form of bar graph, called *histogram.* The histogram shows the data much more clearly than the tabular method given in Table 3. Figures 6 (a) and (b) show histogram plot of genuine and skilled forgery rows obtained. There are also many possible methods to compare the distributions. Srinivasan et al. [14] have addressed SV using Kolmogorov-Smirnov (KS) test [17] and its performance results were presented with figures. The Chi-Square test is an alternative to Anderson-Dawning (AD) and KS, goodness of fit tests. The KS and AD tests are restricted to be used in continuous distributions. The Chi-square is applied to a discrete distribution here.

6.1. THE CHI –SQUARE (X^2) TEST

The Chi-square (χ^2), Goodness of fit test is considered to see how well the signature data set "fits" or "agrees" with the probability distribution function. A data set is believed to be matched by a completely specified finite discrete probability distribution in this test. Since signature is a behavioural biometrics, change in age and health condition is a factor in the signature produced. In this test, the hypothesis to be tested is called '*the null hypotheses'* and a counter corruption is called '*the alternative hypothesis*' [2, 8]. The Chi-square test is based on a calculation of the quantity defined by;

$$\chi^2 = \sum_{i=1}^{n} \frac{[(observedvalue)_i - (\exp ectedvalue)_i]^2}{(\exp ectedvalue)_i} \qquad (1)$$

Where '*n'* is the number of cells or groups of observations. In this study, calculations have been made to see how the actual calculation results match the expected one. The probability is defined by *'P'*. It is calculated using X^2 and F [8]. In the table, F refers to degree of freedom in the measurement, or observation as $F=n-k$ where '*k'* is the number of imposed condition on the expected distribution. This test is sensitive to the choice of *k*.



(a) (b)

Fig. 6. Histogram plots for genuine and skilled forgery samples

6.2. THE CHI-SQUARE TEST ON SIGNATURE DATABASE

Having applied PSO-NN method, verification results are presented in Table 2 for '*genuine signature'* and '*skilled forgery*'. The Chi-square test is applied for both signatures. Initially, '*genuine signature*' data are taken; the values of interest are given in tabulated manner. Total 225 genuine signatures are taken; the Chi-square is computed according to equation (3), X^2 and using Table 3 with degrees of freedom found, F. It is then consulted for the probability, P [8]. The test can be found in any statistics textbook with related probability table.

Table 2 shows the verification results for 25 samples, where in each samples, genuine signatures are taken '9' and skilled forgeries are taken '14' signatures during the test. The Chi-square is also applied to Table 3 to see how this information is conveyed in 25 samples. In each, a check is initially performed such that a certain number of samples for statistics to apply. For this test, the accepted minimum number of each cell is 5; therefore by consulting Table 3, same samples are to be redefined. When the hypothesis is accepted, the statistics follows the normal distribution, when the statistics are significant, the hypothesis are rejected (Significance levels of 0.10, 0.05 or 0.01) [2, 8]. *Hypothesis*: From the data taken, would you conclude that 'signatures are genuine'? Two observations; accepted and rejected results can be seen, $n = 2$, $k = 1$ *and* $F=1$. $P<0.005$, a decision can be made that, the signatures are '*genuine*'. Similarly, additional data is used for testing '*skilled forgery*', using Table 3. Total 350 signatures are applied here. Two observations are taken as '*accepted*' and '*rejected'*. Where $n=2$, $k=1$, $F=1$. *Hypothesis*: From the data taken, would you conclude that '*signatures are forgery*'? $P<0.005$, a decision is made as the signatures are forgery. There is no absolute check in this method. A confidence level must be applied at the beginning, and then the final acceptance or rejection will be left to the judgement or expert. A misplaced data point can also be eliminated to improve the data of evidence. By eliminating the misplaced data, rate of success can be changed for both *genuine* and *skilled forgery*. If *random forgery* has been applied, the obvious point was that the rate of success would be significantly different.

7. CONCLUSIONS

Artificial Intelligence (AI) techniques NN, in particular, an Evolutionary Algorithm (EA) based on Swarm Intelligence (SI); PSO is used for SV system in this paper. Overall accuracy of the system is nearly seen as 78 % (22 % mismatches). Series of results are subjected to the Chi-square test to check the validity of the assumed function. Quality of uncertainty is studied using previous marks in biometric studies. Levels of uncertainty can be classified as; low, medium, high, and very high uncertainty level. Table 4 shows levels of uncertainty which is defined by [15] in biometric studies. Strength of evidence changes depending on level of uncertainties. So in the Table, the verification rate found here is included in '*ideal conditions*'. Thus this biometric system based on SV works.

Table 4. Levels of Uncertainty [15]

Ideal Condition	Low level of uncertainty (< 30 %)	Biometric system works.
Medium Condition	Medium level of uncertainty (about 50 %)	Decision is not certain. (not conclusive)
Hard Condition	High level of uncertainty (about 70 %)	Biometric system is unreliable.
Very Hard Condition	Very high level of uncertainty (about 90 %)	Biometric system fails to make a decision.

ACKNOWLEDGEMENT

This study is supported by Gaziantep University Research Unit under the project number of MF.06.04. Project name is 'Design and Implementation of a Mechatronic Questioned Document Device'.

BIBLIOGRAPHY

[1] ARMAND S, BLUMENSTEIN M., and MUTHUKKUMARASAMY V "Off-line Signature verification Using an Enhanced Modified Direction Feature with Single and Multi- Classifier Approaches", IEEE Comp. Int. Magazine, pp.18-25, 2007.

[2] BERNES J. W., "*Statistical Analysis for Engineers and Scientists"*, McGraw Hill, 7th Edition, 1994.

[3] DAŞ M.T, DÜLGER L.C.,' Off-line signature verification with PSO-NN algorithm', 22nd Int. Symposium on Computer and Information Sciences- IEEE, Ankara-TURKEY, 2007.

[4] DAŞ M.T, DÜLGER L.C.,' Design and Implementation of a Questioned document Device and Automatic Signature Verification Toolbox', 5th Summer School for Advanced Studies on Biometrics for Secure Authentication: Algero-Italy, June 2008.

[5] DAŞ M.T,, 'Design and Implementation of Biometric Recognition using off-line signature analysis, Ph.D.Thesis, Gaziantep University, November- 2008.

[6] FERRER M.A, ALANSO J.B., TRAVESO M,'Off line geometric parameters for automatic signature verification using fixed point arithmetic', IEEE Trans on Pattern An. and Mach. Int., Vol. 27, No.6, pp.993-997,2005.

[7] HITCHCOCK D.C, 'Evaluation and combination of Biometric Authentication Systems', M.Sc.Thesis, University of Florida,2003.

[8] HOLMAN J. P., "*Experimental Methods for Engineers*", McGraw Hill, 2001.

[9] JAIN A.K., PANKANTI S., PRAPHAKAR S., HONG L., ROSS A., WAYMAN J.L.,'Biometrics: A Grand Challenge', Pr. of Int. Conf. on Pattern Recognition, 2004.

[10] KALERA M.K., SRIHARI S., XU A., 'Off-line signature verification and identification using distance statistics', Int. J. of Pattern Recognition and Artificial Intelligence, Vol.18, No.7, pp.1339-1360,2004.

[11] LIU X.Y and BLUMENSTEIN M., "Experimental Analysis of the Modified Direction Feature for Cursive Character Recognition", Int. Workshop on the frontiers of Hand Writing Recognition, pp. 353-358, 2004.

[12] MADASU V.K., 'Automatic Bank Check Processing and Authentication using Signature Verification', Ph.D.Thesis, Queensland University, Australia, 2006.

[13] PLAMONDON R., BRAULT J.J., 'A complexity measure of handwritten curves: Modelling of Dynamic Signature Forgery', IEEE Trans. On Systems, Man and Cybernetics, Vol.23, No.2, pp.400-413,1993.

[14] SRIVINASAN H., SRIHARI S.N., BEAL M. J., "Signature Verification using Kolmogorov Smirnov Statistics", Proc. Int. Graphonomics Society Conference Salerno, pp. 152-156,2005.

[15] YANUSHKEVICH N., STOICA A., SRIHARI S.N., SHMERKO V.P., GAVRILOVA M.L., 'Simulation of Biometric Information: The New Generation of Biometric systems', Int. Workshop on Biometric Technologies, University of Calgary,-Alberta-Canada, p.1-12, 2004.

[16] http://www.bromba.com/faq/biofage.htm#Messgroessen

[17] www.physics.csbsju.edu/stats/KS-test.html