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

Enhanced Approach on Online Handwritten Signature Verification through Multi rate SVM with Wavelet Transformation

Prathibha MK [1], Basavaraj L [2]

[1,2] Dept. of Electronics and communication Engineering, ATME college of Engineering, VTU, Mysore, India

[*]Corresponding Author: mailtoprathiba@gmail.com, Tel.: +91-944100-54321

Available online at: www.ijcseonline.org

Accepted: 14/Jul/2018, Published: 31/July/2018

Abstract— Online Handwritten Signature verification plays a significant role in the field of administrative, banking, business sector, etc. Therefore, an accurate signature verification system is required in order to provide an identification of an individual. A new Online Handwritten Signature verification is proposed based on a Multirate Support Vector Machine (MSVM) and for verification the SUSIG database is used. The input database is obtained from the pressure sensitive tablet, removal of noise and resizing is done through fourth order wavelet and discrete cosine transform. Further, the functional feature such as standard deviation, skewness etc. are extracted and processed to MSVM for generation of threshold value between genuine and sample signature. The obtained result is more sensitive, specific and accurate. The Equal Error rate (EER) of 0.33 is obtained, so that the proposed system shows competitive performance with the other existing approaches.

Keywords— Online Handwritten Signature Verification,(OHSV), Multirate Support Vector Model (MSVM), Discrete, Wavelet Transform (DWT), Discrete Cosine Transformation (DCT), Feature Extraction, Forgery, Threshold value.

I. INTRODUCTION

Signature verification is defined as the biometric [1] behavior used for demonstrating the authenticity of a person. The processing and verification of large number of signatures can be easily done through electronic signature verification. It is chosen to be popular and world-wide accepted technique compared to other biometrics. It is widely accepted in various credential systems such as E-banking, business sector, and smart card etc., traditionally offline signature verification [2]is used their main limitation is security and authenticity during verification and transmission of data. In order to solve this issue, an efficient automatic system such as Dynamic Time Wrapping (DTW) [3], Hidden Markov Model (HMM) [4], Support Vector Machine (SVM) [5] and Neural Networks (NN) has been used to authenticate the person's signature on the basis of individual claimed identity [6].

The applications of electronic signature mainly depend on biometrics since it is the only way to guarantee the presence of owner [7]. Biometrics is a technique used to verify authentication of a person and authorize the transaction by employing physical, biological and behavioral characteristics of an individual person [8]. The authentication is carried out by enrolling set of biometric samples such has Handwritten signatures of the user into the system. During verification, the threshold value is obtained amongst claimed sampled signature and reference signature of an individual, if the similarities found is below the threshold, the signature is said to be authenticated or else signature is rejected. Biometric signature verification has been categorized into two types, offline verification and online verification [9]. Offline process is carried out by considering image format of signature, which is stored in the form of static images and performing recognition through artificial intelligence techniques [10]. Online process is done by considering the dynamic and spatial information of the signature using digitalized tablet. The difference between the input and reference signature is captured through string matching [11]. In perspective, online verification has proved to be robust, reliable and accurate in nature [12].

The Online Handwritten Signature verification consists of a set of strokes in which each stroke comprises with an array of points [13]. Verification process determines whether the input signature is from a genuine user or a forgery [14]. Forgery has been further classified into random, simple and skilled forgery. Random forgery comprises irrelevant sampled signature compared to genuine signature parameters, simple forgery consists only the name of the signer and skilled forgery comprises a signature similar to that of the original signature. Different algorithms have been used to obtain authenticity of Online Handwritten Signature verification. Dynamic Time Wrapping (DTW) is broadly used algorithm, the distance amongst two signals is calculated through optimal nonlinear path and then it is aligned by constructing n-m matrix called as wrapping matrix [15]. Hidden Markov Model (HMM) consists of a set of signature class, each class is modeled using single HMM; training and testing of HMM model is done by employing set of sample signature of the user [16]. Support Vector Machine (SVM) is a supervised machine learning model comprising different learning algorithms and analyzes the information used for classification and regression analysis. In Neural Networks (NN) technique [17], function of the probability density is used as global shape factor and discriminating power was enhanced by reducing its cardinality via filtering.

This paper has been divided into five sections; first section comprises the introduction to Online Handwritten Signature verification system and briefed about the various techniques used for Online Handwritten Signature verification. The different online handwritten signature verification algorithm proposed by different authors and their reviews on different algorithms has been showcased in section two. Section three comprises with the proposed design methodology and the algorithm used. It consists of block diagram and flow chart of the proposed algorithm. Simulation results and comparison of the proposed algorithm has been featured in section four. Section five comprises with the conclusion and future work.

II. RELATED WORK

There is a wide range of literature obtained in the field of Online Handwritten Signature Verification (OHSV). The different methods and techniques used by different authors has been briefly explained as follows,

The paper [18] introduced fast dynamic time wrapping technique, upgraded version of DTW. Multilevel approach has been used solve the issues of quadratic time and space complexity [19]. Theoretical and practical calculations have been conducted and shown that proposed algorithm shows better accuracy compared to other existing algorithms. Further, DTW is implemented using embedded systems such as low-cost FPGA [20]. The system comprises genetic VFPU, which is capable of performing multiple tasks at one time. The performance of the proposed technique improves the computation speed and reduces the size of the program memory. Two stage normalization techniques are proposed [21] to detect various forgeries. In the first step, simple forgeries have been detected and skilled forgeries in the second step. By using this technique, performance can be improved especially in MCYT and SUSIG visual sub corpus. The paper [22] proposes a new model for implementing dynamic signature verification. Two efficient approaches have been used to extract regional and global features of the signature. The results calculated shows that better accuracy can be obtained by combining two or more techniques. In order to reduce the ratio of error, probabilistic dynamic time wrapping technique [23] is introduced. The distance between the signatures is calculated using dynamic wrapping [24] and robustness is obtained through multi-threshold and multi-segments. High robustness is obtained and changes in certain parts of the signature can be easily recognized through this method.

The paper [25] implemented new ANN based technique for feature selection in verification and recognition called Principal Component Analysis (PCA). In this technique, PCA is used for 50 prominent feature extractions on handwritten signatures. Further, multilayer perceptron is used authenticate the signature, whether it is forged or genuine. The experimental results show's that 93.1% accuracy is obtained comprising both genuine and skill-forged signatures. Single Reference Signature System (SRSS) technique has been developed for Online Handwritten Signature verification [26]. SRSS develops an intrapersonal variability through synthetic generation to differentiate forged signature from one signature. By making use of two methods, SW distortion and TW distortion, human like forged signatures has been developed and experimentally validated with the genuine one. The results show's that duplicate samples are indistinguishable as it is developed through visual turning test and performance analysis in terms of skilled forgery is slightly better compared to other existing technique. The paper [27] comprises a new technique based on dependency of writer both at feature and classifier level. The efficiency of OHSV is calculated by comparing the proposed model with six different classifiers of OHSV. The experimental results showcased that an error rate of 1.92 is observed in skilled forgery and it is the least value compared to other existing model in terms of set of test samples. In another study, a new approach for secure authentication is implemented using mouse gesture of an individual [28]. In this technique, the gesture is drawn by making use of mouse, and these gestures are evaluated using Markov model classifier. Observations show that there is advancement in terms of precision and authentication compared to conventional systems.

The paper [29] comprises new SVM based technique for implementing OHSV using reference feature vector. The authentication is obtained by representing the signature set in the form of 0 and 1 using reference feature vectors and it is allowed to flow through a two class SVM classifier which concludes whether the test signature is genuine or forgery. Results shows that an accuracy of 95.36% is obtained compared to other technique thereby successfully discriminates genuine signatures from forgery signature. In another study, novel study based OHSV has been proposed based on shadow sensing [30]. The author mainly concentrated on the drawbacks of size, affordability in designing hardware and intelligent software routine to complement the simplicity of hardware. The results show's that an accuracy of 96.2% is observed compared to other existing techniques. The study on hybrid technology of OHSV has been proposed in the paper [31]. It comprises templates of quad tree histogram and SVM based artificial immune system. The results showcase's that proposed algorithm is high efficient and provides high accuracy compared to other techniques. Simple, low cost SVM based approach and software used has been proposed in the paper [32]. The local binary pattern features such as stroke end and stroke edge were successfully employed in SVM classifier in order to distinguish between the genuine and forgery.

III. METHODOLOGY

In this paper, Multiclass SVM based Online Handwritten Signature verification has been proposed for implementation of high authentic and security-based systems. The framework for proposed system is shown in Figure 1.

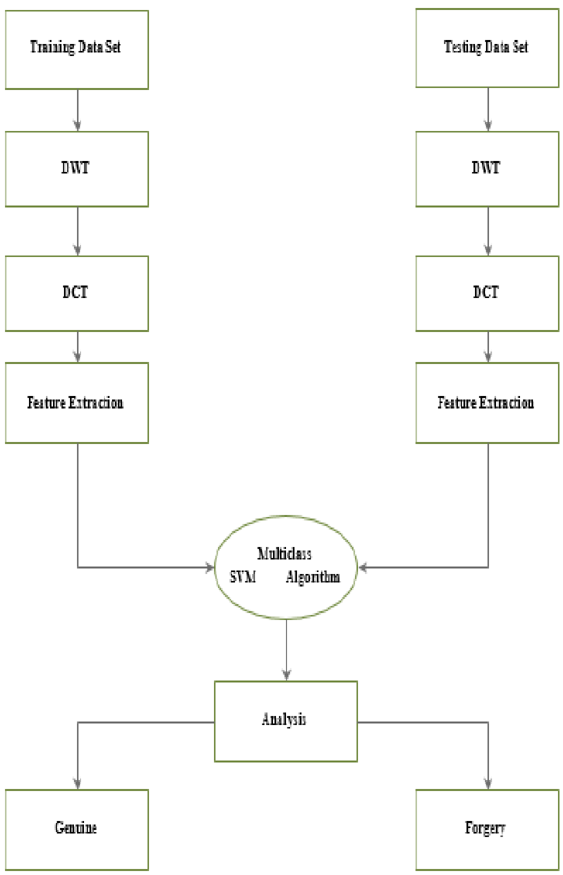

Figure 1. Flow Chart of the Proposed Algorithm

The proposed methodology of Online Handwritten Signature verification has been divided into four stages, in first stage, the training and testing signature data is obtained through input device and it is represented in 2D signal domain. In second stage, the obtained signal is digitalized and sampled with respect to size and frequency domain by using DCT and DWT technique and in third stage, the feature set such as skewness, kurtosis etc., has been extracted. Fourth stage comprises with working of MSVM algorithm and analysis part to showcase whether the test signature is genuine or forgery.

A. *Training and Testing Data Set*

SUSIG is a new online signature database which is available for use in developing or testing signature verification systems. The SUSIG database consists of two parts collected using different pressure sensitive tablets (one with and one without LCD display). A total of 100 people contributed to each part, resulting in a database of more than 3000 genuine and 2000 skilled forgery signatures.

The pen position of the signature is plotted on the basis of x-y coordinates and represented in the form of time domain signal and it is trained using 256 forged signatures set of the genuine user. Simultaneously, signature for testing purpose is stored in the testing data set and these signals are sampled and digitalized in the form of time sequence and presented in IxJ matrix, which is represented as shown in "(1)".

$$S(n) = [x(i\ j)\ y(i\ j)\ a(i\ j)\ b(i,j)]^T \quad (1)$$

Where, n=number of digitalized samples.
x(n), y(n)= represents coordinate points of signature trajectory
a(n), b(n)=specifies pen pressure and time stamp at sample point n

B. *Discrete Wavelet Transform (DWT)*

The processing of signature signals is done in discrete wavelet transform (DWT), where the signals are converted to frequency domain plane and data size is scaled and converted into frequency components. These frequency components are called as mother function. Daubechies D4 Wavelet Transform is used for scaling and it is shown in Table 1.

Table 1. Co-efficient of scaling factor with respect to Wavelet

Wavelet	**H_0**	**H_1**	**H_2**	**H_3**
Scaling Function Co-efficient	$\frac{1+\sqrt{3}}{4\sqrt{2}}$	$\frac{3+\sqrt{3}}{4\sqrt{2}}$	$\frac{3-\sqrt{3}}{4\sqrt{2}}$	$\frac{1-\sqrt{3}}{4\sqrt{2}}$

The scaling functions are calculated by considering the inner product of the functions with respect to four data values. The equation for calculation is shown in "(2)",

$$a_{i(i,j)} = h_0 s_{2i(i,j)} + h_1 s_{2i(i,j)+1} + h_2 s_{2i(i,j)+2} + h_3 s_{2i(i,j)+3} \quad (2)$$

Where h0, h1, h2, h3 represents wavelet function co efficient
i = number of iterations
S2i= Number of samples.

The Daubechies fourth order wavelet acts as a low pass filter and approximation coefficients of the first level decomposition is extracted in order to reduce the noise of the signal. The computation speed of DWT is found faster compared to other wavelet transform, easier to implement and less computational time. The output signal obtained from DWT is later analyzed with discrete cut-off frequencies at different scale and it is sent to DCT stage. The Daubechies fourth order wavelet as shown in "(3)".

$$\begin{bmatrix} h_0 & h_1 & h_2 & h_3 & h_4 & 0 & & & & \\ g_0 & g_1 & g_2 & g_3 & 0 & 0 & & & & \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & & & & \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & & & & \\ 0 & 0 & 0 & 0 & h_0 & h_1 & h_2 & h_3 & & \\ 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & & \\ 0 & 0 & 0 & 0 & 0 & 0 & h_0 & h_1 & h_2 & h_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{bmatrix} X \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} \quad (3)$$

C. *Discrete Cosine Transformation (DCT)*

It is found that DCT is more efficient in reducing dimensionality of the system compared to other techniques. Decorrelation and energy compaction are two important properties thus by providing a compromise amongst capability of data packing and computational complexity, dimensionality of the system can be reduced. The dynamic characters are showcased in transformation patterns as shown in "(4)".

$$x(i,j) = \sum_{k=0}^{N-1} a(k).X(k)\cos\left[\frac{\pi(2k+1)i,j}{2N}\right] \quad (4)$$

The output obtained from DCT is passed to feature extraction stage where the signature has been divided based on different features.

D. *Feature Extraction*

Feature extraction is the process representing the data in the form of different sets, which is used for solving computational task for the given applications. Each person signature is unique and comprises different features. When an unauthorized or fake user tries to reproduce genuine signature, he can come up with the similar type of signature, but some features of the genuine cannot be replaced. The features considered while designing this algorithm are differentiated based on different size and dimension and they are as follows,

Standard Deviation (σ)

The standard deviation is defined as the mean square difference of the grey pixel value to its mean deviation defined in "(5)".

$$\sigma = \sqrt{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-\mu)^2} \quad (5)$$

Where μ=mean

M= Number of rows

N= number of columns

X(i,j)= Pixel value at point i,j

MxN = Image size in terms of rows and columns

Skewness

It represents the angle of asymmetry in the distribution of pixel across the fixed image size. It can be quantified as the deviation in the size compared to the genuine signature across the specific boundary defined in "(6)".

$$S = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{x(i,j)-\mu}{\sigma}\right)^3 \quad (6)$$

Kurtosis

It is defined as the level of flatness or a peak value of distribution with respect to the normal distribution defined in "(7)".

$$K = \left\{\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\frac{x(i,j)-\mu}{\sigma}\right]^4\right\} - 3 \quad (7)$$

RMS Value

The Root Means Square (RMS) value defines the MS of the input matrix comprising vector dimensions of entire input defined in "(8)".

$$Y = \sqrt{\frac{\sum_{i=1}^{M}|x_{i,j}|^2}{M}} \quad (8)$$

Variance

It is defined as the squared deviation of the random variable amongst mean defined in "(9)".

$$V = \sqrt{SD} \quad (9)$$

E. *Multirate Support Vector Machines (SVM)*

SVM is generally designed for classification of binary variables, which predicts multivariate and structured outputs. It comprises discriminative classifier which shows efficient performance for classifying between two data sets in terms of accuracy and robustness. The equation for implementing SVM over other training set are given by,

Different approaches have been used to implement SVM technique, they are as follows,

1. By constructing and combining several binary classifiers
2. By considering all data in one optimization formulation

In this paper, we have considered a method by comprising all the data set for optimization formulation. The main features of the proposed algorithm are as follows,

1. The selection of the working set depends on the steepest feasible descent.
2. The fastest optimization algorithm for solving regression problems for multivariate and structure outputs.
3. It efficiently computes the error rate, Standard deviation, Precision etc.
4. It can handle several signatures of test sample and genuine simultaneously.

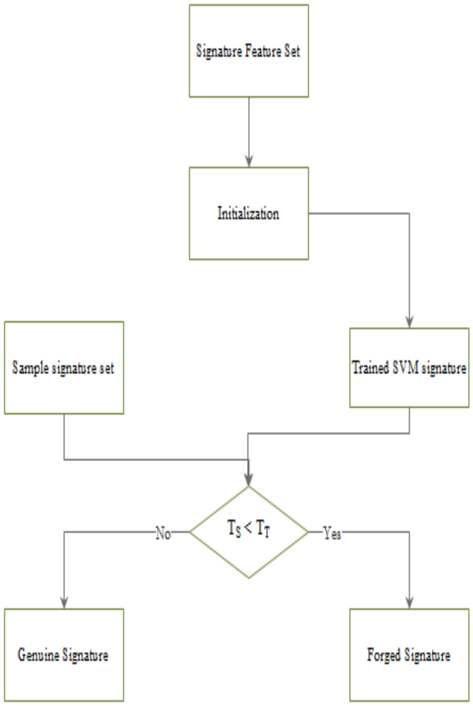

Figure 2. Flow chart of MSVM

The flowchart of Multirate SVM is shown in Figure 2. The features of the signature obtained from the feature extraction stage are processed to MSVM block. During initialization, the features of the genuine signature are extracted and it is trained with 256 high skilled forged signatures set and it is optimized. The sample signature feature set is compared with trained signature in terms of threshold value. The threshold value obtained from comparison of test and genuine signature is checked. If the threshold value is lesser then that of the genuine signature, then it is stated as genuine one and authentication is approved or else the signature is termed to fake one and it is cancelled.

IV. Results and Discussion

The input database is obtained through the SUGSIG data base. The features of the database are obtained and genuine signature is trained with 256 high forged signatures and 20 signature samples are used for testing purpose. The proposed method has been implemented using MATLAB R2014a software and minimum values of False Acceptance Rate (FAR) and False Rejection Rate (FRR) obtained for 10 sample set of signatures is shown in Table 2.

Table 2. FAR and FRR values for different sample signature

Samples Number	FAR_{Min}	FAR_{Max}	FRR_{Min}	FRR_{Max}
1	0.00237966	0.00657812	0.91982158	0.99128953
2	0.00573113	0.01155043	0.91982158	0.99128953
3	0.0002416	0.00261694	0.91982158	0.99128953
4	0.00152669	0.00192873	0.91982158	0.99128953
5	0.00162669	0.0053279	0.91982158	0.99128953
6	0.00012012	0.00157517	0.91982158	0.99128953
7	0.00313106	0.00775773	0.91982158	0.99128953
8	0.00658002	0.0127279	0.91982158	0.99128953
9	0.00114707	0.00447639	0.91982158	0.99128953
10	0.00085848	0.00169095	0.91982158	0.99128953

Table 3. Prediction of sample signature with respect to user

User Prediction	Multirate SVM Algorithm Prediction	Conclusion
Genuine	Genuine	T_P
Genuine	Forgery	F_N
Forgery	Genuine	T_N
Forgery	Forgery	F_P

The proposed algorithm is verified to the user prediction of signature and it is showcased in Table 3. If the user prediction is a genuine signature and algorithm result is genuine, then it is stated as true positive (TP), If user prediction is genuine but algorithm states it is forged signature, then it is said to be a false negative (FN). Similarly, true negative (TN) and false positive (Fp) parameters are predicted and calculated as follows,

$$Tp = Sum\ ((idx) == Predicte(idx)) = 93$$

$$Tn = (Ac(\sim idx) == Predicted(\sim idx)) = 12$$

$$Fp = n - Tn = 4$$

$$Fn = p - Tp = 0$$

From the above equations, Accuracy is calculated which is given by,

Accuracy = (Tp + Tn)/N = (93+12)/103 = 0.956

Sensitivity = Tp/p = 0.88

Specificity = Tn/n = 0.85

The performance parameter of the proposed model is calculated on the basis of False Acceptance Ratio (FAR) to False Rejection Ratio (FRR). The probability of negatively accepted forged signature samples is called FAR and probability of rejecting genuine signature samples is shown by the FRR.

The graph shown in Figure 3 shows comprises that both FAR and FRR value will be approximately same and error ratio will be constant throughout until completion of the process.

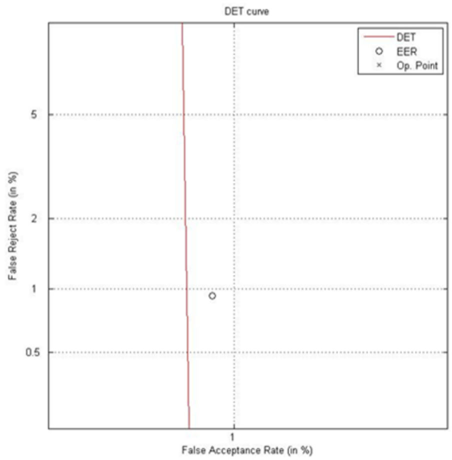

Figure 3. DET curve

The performance analysis is depicted based on Equal Error Rate (EER), FAR and FRR. From Table 4 is shown that both FAR are 0.008957 and FRR is 0.9552, which is less compared to other existing techniques.

Table 4. Performance analysis of existing and the proposed technique

Method	EER	FAR	FRR
PDF Classifier[33]	-	-	5
Neural Network and SVM[34]	-	3.5	21.5
DTW[35]	-	4.13	5.5
SVM LCSS[36]	6.84	-	-
Multirate SVM Model	0.33	0.008957	0.9552

The proposed model has been evaluated based on the performance of ROC. If the input sample signature is positive and output obtained from the proposed model is positive, i.e. genuine, then it is said to be genuine attempts accepted. If the sample signature is a forgery and the output obtained also a forgery, then it is called imposter attempts accepted. Figure 4 depicts the ROC curve between general attempts accepted to imposter attempts accepted and it is shown that curve obtained is in a straight line with less variation, which predicts the system is efficient and accurate.

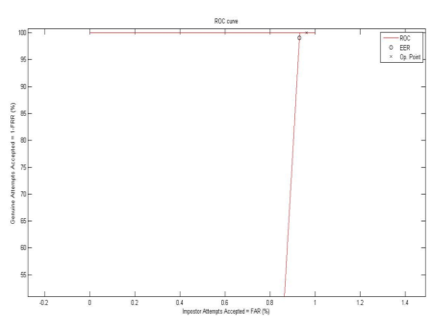

Figure 4. Region of Convergence (ROC) curve

The accuracy and efficiency of the system can also be evaluated using FAR vs FRR curve for error rate calculation.

A unique threshold value should be selected to differentiate between the genuine and forgery signature. The unique threshold value is obtained as shown in Figure5.

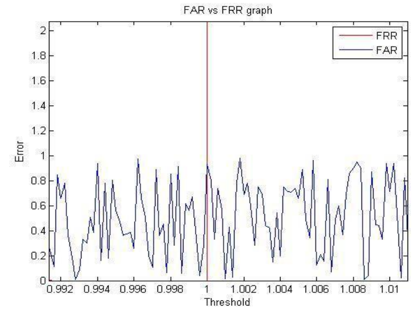

Figure 5. FAR vs FRR curve with respect to threshold

The Figure 5 shows that the two curves will intersect at threshold value of 1 and approximate error rate is around 0.9, which shows that the threshold value below 1 is proven to be genuine signature and above is stated as forged signature.

V. CONCLUSION AND FUTURE SCOPE

In this paper, multirate support vector machines has been proposed and implemented for Online Handwritten Signature verification. The approaches of optimization and feature extraction of signature has been demonstrated by different set of sample and genuine signature. DWT and DCT techniques are used for optimization and sampling of input signature and the output obtained is processed for feature extraction. The features such standard deviation and Kurtosis etc. has been extracted and compared using multirate SVM algorithm. SVM algorithm is implemented using MATLAB tool and the performance analysis is calculated through graph. The results show's that proposed model has accuracy of 0.956 and sensitivity of 0.88, which is more efficient, compared to other existing techniques. Further study on the proposed technique, feature selection and size reduction can increase the efficiency and error rate can be minimized.

REFERENCES

[1] Nitin Tiwari, "An Overview and Analysis Based on Biometric Framework Technique and Fingerprint Biometric Technology", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.6, pp.69-74, 2017

[2] Abughfa, A.B. Elmadani, "Offline Signature Verification Based on Image Processing and Hu Moment", International Journal of Scientific Research in Network Security and Communication, Vol.4, Issue.5, pp.1-7, 2016.

[3] EdigaLingappa, Geetavani.B, JambulaHareesha , "Online Signature Verification using Dynamic Properties", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.6, pp.33-38, 2017.

[4] Kashi R, Hu J, Nelson W L and Turin W "Hidden Markov Model Approach to On-Line Handwritten Signature Verification", Conf. Document Analysis and Recognition 4: pp.253-257, 1997.
[5] Alister K and Yanikoglu B, identity Authentication Using Improved On-Line Signature Verification Method. Pattern Recognition Letters 26: pp. 2400-2408,2005.
[6] Fierrez, J, Garcia J O, Ramos D and Rodriguez J G "HMM based on-line signature verification: Feature extraction and signature modelling
',. Pattern Recognition Letters. 28: pp.2325–2334 2007.
[7] Kholmatov A and Yanikoglu B "Identity authentication using improved Online Handwritten Signature verification method", Pattern Recognition. Letter 26: pp. 2400–2408, 2005.
[8] Kour J, Hanmandlu, M and Ansar, A Q "Online Handwritten Signature verification using GA-SVM", International Conference on Image Information Processing (ICIIP 2011), pp. 1 – 4, 2011.
[9] Durrani M Y, Khan S and Khalid S, "VerSig: a new approach for Online Signature verification", Cluster Computing, pp. 1-11, 2017
[10 Ibrahim M T, Kyan M and Guan L "On-line signature verification using global features", Canadian conference on Electrical and Computer Engineering, (CCECE'09), pp. 682-685, 2009.
[11] Song X, Xia X. and Luan F "Online Handwritten Signature verification based on stable features extracted dynamically", IEEE Transactions on Systems, Man and Cybernetics: Systems 47: pp.2663-2676, 2017.
[12] Guru D S and Prakash H N "Online Handwritten Signature verification and recognition: An approach based on symbolic representation", IEEE transactions on pattern analysis and machine intelligence 31: pp.1059 – 1073, 2009.
[13] Jain A K, Griess F D and Connell S D "On-line signature verification", Pattern Recognition 35: pp. 2963– 2972, 2002.
[14] Zalasiński M "New algorithm for on-line signature verification using characteristic global features", In: Information Systems Architecture and Technology: Proceedings of 36th International Conference, pp. 137- 146, 2016.
[15] Khalil M I, Moustafa, M and Abbas H M "Enhanced DTW based on-line signature verification", In: Conf. Image Processing (ICIP) 16: pp. 2713-2716,2009.
[16] Vaseghi B, and Hashemi, S "Online Handwritten Signature Verification Using Vector Quantization and Hidden Markov Model", IOSR Journal of Electronics and Communication Engineering (IOSR- JECE)10: pp.48-53,2015.
[17] Draouhard J P, Sabourin R and Godbout M "A neural network approach to Off-line Signature verification using directional PDF", Pattern Recognition 29: pp.415-424, 1996.
[18] Salvador and Chan P "Toward accurate dynamic time warping in linear time and space", Intelligent Data Analysis 11: pp. 61-71,2007.
[19] Liu Y, Yang, Z, and Yang, L "Online Handwritten Signature verification based on DCT and sparse representation", IEEE transactions on cybernetics 45: pp.2498-2511,2015.
[20] García M L, Lara R R, Hurtado O M, Navarro E C "Embedded system for biometric Online Handwritten Signature verification", IEEE Transactions on industrial informatics 10: pp.491- 501,2014.
[21] Fischer A, Diaz M, Plamondon R.,and Ferrer M A "Robust score normalization for DTW-based on- line signature verification". Int. conf. Document Analysis and Recognition (ICDAR), pp.241-245,2015.
[22] Zalasiński M, Cpałka K and Andersson E R. "An idea of the dynamic signature verification based on a hybrid approach", In: International Conference on Artificial Intelligence and Soft Computing, pp.232-246, 2016.
[23] Aguilar J F, Krawczyk S, Garcia J O and Jain A K, "Fusion of local and regional approaches for on- line signature verification", In: Proc. Int. Conf. Adv. Biometric Recognition Syst. (IWBRS), pp. 188–196, 2005.
[24] Rehman, A U, Rehman S, Babar Z H, Qadeer M K and Seelro F A "Offline Signature Recognition and Verification System Using Artificial Neural Network", University of Sindh Journal of Information and Communication Technology 2: pp.73-80, 2018.
[25] Iranmanesh, V, Ahmad S M S, Adnan W A W, Yussof S, Arigbabu O A, and Malallah, F L, "Online Handwritten signature verification using neural network classifier based on principal component analysis", The Scientific World Journal, pp.1-8, 2014.
[26] Diaz M, Fischer A, Ferrer M A, and Plamondon R. "Dynamic signature verification system based on one-real signature", IEEE transactions on cybernetics 48: pp.228-239,2018.
[27] Manjunatha K S, Manjunath S, Guru D S, and Somashekara M T "Online Signature verification based on writer dependent features and classifiers", Pattern Recognition Letters 80: pp.129-136, 2016.
[28] Baraki P and Ramaswamy V "Biometric Authentication of a Person Using Mouse Gesture Dynamics: An Innovative Approach", In: International Proceedings on Advances in Soft Computing, Intelligent Systems and Application 7: pp. 331-344,2018.
[29] Rohilla S and Sharma A "SVM Based Online Signature Verification Technique Using Reference Feature Vector", Proceedings of the National Academy of Sciences, India Section A: Physical Sciences 87: pp.125-136,2017.
[30] Roy D, Chowdhury A, Sihnaray A and Ghose A "Novel Handwritten signature verification system based on shadow sensing", In: IEEE SENSORS, pp. 1-3,2017.
[31] Serdouk Y, Nemmour H and Chibani Y "Handwritten signature verification using the quad-tree histogram of templates and a Support Vector-based artificial immune classification", Image and Vision Computing 66: pp. 26-35,2017.
[32] Tran V Q, Chew M T, Demidenko S, Kuang Y C, and Ooi M "Simple signature verification sub- system for identity recognition", In: IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), pp. 94-98,2017.
[33] Kiran G V, Kunte R S R and Samuel S "On-line signature verification system using probabilistic feature modelling", In: Sixth International Symposium on Signal Processing and its Applications, pp.355- 358,2001.
[34] Khalid M, Mokayed H, Yuso, R, and Ono O 2009 Online Handwritten Signature verification with neural networks classifier and fuzzy inference. In:Third Asia International Conference Modelling & Simulation (AMS'09), pp. 236-241.
[35] Reza A G, Lim H and Alam M J "An Efficient Online Handwritten Signature Verification Scheme Using Dynamic Programming of String Matching", In: International Conference on Hybrid Information Technology 6935: pp. 590–597,2011.
[36] Gruber C, Gruber T, Krinninger S and Sick B "Online Handwritten Signature verification with support vector machines based on LCSS kernel function", IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 40: pp. 1088-1100,2010.

Authors Profile

Prathiba M K received her Bachelor of Engineering Degree in Electronics and Communication Engineering from Mysore University in 1996. She did her Master of Technology in Industrial Electronics from Visvesvaraya Technological University, Belgaum in 2008. Presently she is pursuing Ph.D. in the area of Biometric Application under the guidance of Dr. L. Basavaraj. Her area of interest is Signal processing and Image processing.

E-mail: mailtoprathiba@gmail.com

Basavaraj L received his M.E degree in Digital Electronics from Karnatak University in 1994, and Ph.D. in Electronics from University of Mysore in 2010. His researches interests include VLSI Implementation of signal Processing Applications, Biomedical Signal Processing, Offline, and on-line handwritten signature recognition.

E-mail : basavaraj.atme@gmail.com