J. Appl. Environ. Biol. Sci., 6(3S)159-165, 2016

© 2016, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Signature Verification through Chebyshev Polynomials A Novel Method

Mehr Yahya Durrani[2], Jawad Ur Rehman Chughtai[1], Armughan Ali[2], Ali Mustafa[2]
Dr. Shehzad Khalid[1]

[1] Department of Computer Engineering, Bahria University, Islamabad
[2] Department of Computer Science, COMSATS Institute of IT, Attock

Received: January7, 2016
Accepted: March 2, 2016

ABSTRACT

Online Signature Verification (OSV) is an area of research which has attracted attention of researchers since last decade or so. OSV is in extensive use in many domains such as banking industry, security control, law enforcement to name a few. Signature verification is a pattern recognition problem and like other pattern recognition problems it is traditionally solved by employing some classifier which is trained through a training dataset. This classifier is later used to detect authentic and forged signatures. Employing this approach for OSV is a complex task because of the fact that even two signatures of an individual also exhibit differences. In this paper a novel scheme for the OSV is introduced which is based on Chebeyshev polynomial scheme. We have incorporated a well known signature dataset ICDAR 2013 for training the classifier. This dataset provides dynamic information about the signature such as information about X and Y coordinates and Pressure exerted on the device. This information is used to make segments and dynamic information is extracted from these segments. Classifier is trained on the extracted information and a threshold is identified for a given user to accommodate the signature differences of a person. Later, when a signature is presented for verification the same information is used to identify signature as genuine or forged. The proposed scheme provide results which are comparable to other schemes proposed for the same problem.

KEYWORDS: Signature Verification, Classification, Forgery Detection, Authentication, Chebyshev Polynomials

1 INTRODUCTION

Identification of a Person is one of the important mean for any security system. Traditional authentication mechanisms are based on Passwords, PIN Numbers or some type of cards. The drawback of such scheme is that the password and pins can be forgotten and card can be stolen. This in turn has placed focus on biometric means of identification. Apart from other biometric techniques such as finger prints, iris scanning etc. handwritten signature is a behavioral trait and a promising way for user identification. Signatures are the oldest way of personal verification and has wide spread acceptance in the society [1].

Signature verification can be viewed as online or static signature verification & online or dynamic signature verification from data acquisition standpoint. In offline signature verification, signatures are recorded as images on paper which can later on be transformed into computer by means of a scanner and processed using offline verification stages. Offline signature verification is carried out on static features like shape, style variation, distortion, rotation variation, etc. Conversely, Online signature verification makes use of dynamic features e.g. pressure, velocity, stroke length, pen up/down time, etc. along with the shape of the signature [2].One of the key requirement of a verification system i.e. accuracy, can be achieved with greater precision due to the availability of dynamic information in OSV. Also, OSV is accepted far and wide by the communities for verification purposes as it's more secure method than the available ones. It is difficult for imposters to copy all attributes (speed, pressure) along with the shape as it is present in the genuine signature. Due to the increasing popularity of the input capturing devices e.g. tablets, PDA's etc., data acquisition in OSV is now not a major problem. That's also one of the reasons which attracts the researchers to work in this area. The focus of this study is to design a robust system for signature recognition. When a query signature is presented to it, the proposed system will preprocess the signatures, extract the relevant features and classify query signatures as genuine or forged based on extracted features.

* **Corresponding Author:** Dr. Shehzad Khalid, Department of Computer Engineering, Bahria University, Islamabad. Email: shehzad_khalid@hotmail.com

2 RELATED WORK

Online Signature Verification catches the attention of researches from the past few decades and still is an enduring research area. In the today's society, there has been an enormous growth in the number of documents that are being transmitted and stored electronically. Just like paper documents, electronic documents are subject to forgery. This rising reliance on electronic storage and transmission of documents has raised a need for electronically verifying the identity of the sender. The features of an online signature can be represented as time series data. Time series is a series of values which are measured as a function of time. Research in online signature verification can be broadly categorized into following four classes.

Template Matching Approaches Template matching techniques are based on a straightforward comparison between the features of a captured signature and a template stored in a database. Dynamic Time Warping is reported as the most popular & commonly used template matching approach in the prior research [3][4][5][6][7]. In DTW, a distance measure between feature vectors is required. Euclidean distance has been found in past researches [4][8]. Mahalanobis distance can also be found as a replacement of ED to get better performances [9]. Since the classic DTW is computationally expensive, piecewise aggregate approximation (PAA) of time series or data down-sampling has been
successfully used in past [10][11].

Structural Approaches Structural approaches are broadly classified into three main classes string matching, structural description graph (SDG) and tree matching. Various String Matching Approaches have been reported in past for online signature verification[12][13]. The authors in [13] have presented a signature representation that captures the essentials of the signature shape and the way the pen moves during signature writing by using a string representation for the extrema of the x and y profiles of the signature as well as information about the length of time gaps between successive extrema.

Statistical Approaches In a wide range of publications, online signatures are classified by means of Support Vector Machines (SVM) [2][14][15], Hidden Markov Model (HMM) [16][17] and Neural Networks [18][19]. In the Signature Verification Competition 2004 [20], HMM and DTW based systems were shown to be the most competitive approaches and the system based on DTW outperformed the others and took the first place.

Transform Domain Approaches Discrete Wavelet Transform [19] and Discrete Cosine Transform [21] are the most known transform domain approaches for online signature verification reported in past. The use of discrete wavelet transform (DWT) in feature extraction from handwritten signatures that gave higher verification rate than that of a time domain verification system is found in [22]. DWT coefficients of user genuine signatures that are mostly similar are chosen as candidates for signature authentication features in [19]. A simple and effective approach for an on-line signature verification system can be seen in [21]. First, the Discrete Cosine Transform (DCT) is applied on the time signals of the signature, and feature vector is created using DCT coefficients. The advantage of using the DCT is the ability to compactly represent an on-line signature using a fixed number of coefficients, which leads to fast matching algorithms [21].

3 Proposed Online Signature Verification Methodology

Development of an efficient online signature verification system (OSV) is a non trivial task. OSV is an active research area which aims to develop an efficient system to recognize genuine and forged signatures. A typical OSV consist of data acquisition, pre processing, feature extraction and classification phases shown in Figure 1. Brief overview of various components of our OSV is described in the preceding section.

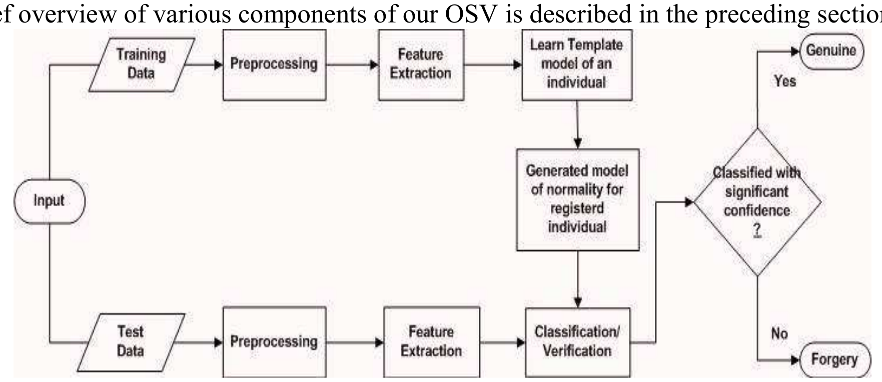

Figure 1: Generic Steps involved in Online Signature Verification System

3.1 Data Acquisition The input to an OSV is a time series data captured through graphic tablet. Different graphic tablets provide different set of information. These range from basic information such as X and Y position coordinates pressure information etc. to derivatives such as velocity and acceleration. Data acquisition is a difficult task as one has to take more than one samples of a person (typically 5-12) due to inters variability of a person's signature. Researchers on the other hand use some well known datasets available on the Internet [20,23]. For this research work we are using dataset of Signature Verification Competition 2013 [24] which consist of online signature information from Japanese signers.

3.2 Preprocessing Since, the training & testing signatures may contain noise & length variability; there is a need to preprocess these signatures before moving to next stages. Since we are using a dataset we have not applied any preprocessing in this research work.

3.3 Feature Extraction & Enhancement Feature extraction is the major task which plays a vital role in effectiveness of an OSV. Feature is an attribute through which we can verify a signature. There are three types of features in an OSV; i.e. global features which consist of whole signature, local features which are extracted from each sample point of a signature and segmental features in which features are extracted from each segment of a signature [25, 26]. Total writing time, number of pen up/down and number of strokes are examples of global features [20, 27, 28] where as speed, pressure and local curvature falls in the category of local features [20, 26, 28]. Areas of high/low pen pressure and high/low speed considered as segmental features [29, 30, 31, 32].

The success of any OSV depends on extraction of certain features which can distinguish between forged and genuine signature. These features represent signature in different classes and it has the capability to stay the same with in a same class. Some external factors also play an important role in creating a system. For example in Banking feature extraction and its optimal matching are of critical importance. On the other hand the system should be robust and efficient to provide result in quick time. In a nutshell following points need to be considered:-

i) Feature set should be simple and efficient to cater the issue of devices which has low computation power such as mobile phones, PDA etc.

ii) Feature selection should be in such a manner that it should have low inter personal similarity in order to differentiate between signatures of different classes. On the contrary signatures which are of same type should have high intra personal similarities.

iii) Feature selection should be in such as way that no one can copy the original signature.

3.3.1 Dynamic Feature Set Dynamic features are group of features which make it difficult to copy someone's signature. These features not only collect information of overall shape of a signature but it also collect information from individual sampling points and other dynamics such as speed etc. More features can also be extracted from these features such as velocity and acceleration etc. which are very useful in OSV against detection of traced signatures etc. Feature selection also plays an important role at later stage i.e. classification stage. In this paper raw data vector is obtained from dataset comprising of three dimensional time series data and is presented in the equations 1-4

$T(S) = [(x_{ts}, y_{ts}, p_{ts})]$ {ts = 0,1,2,……n) Eq. 1

Where x_{ts}, y_{ts} are information of x and y coordinates and p_{ts} are pen up/down information at each sampling point at time t_s. Our feature vector in this research work consist of x,y coordinates and pen up/down time.

We have computed derivatives of the x and y points to calculate speed of each signature sample. Following equation is used for the task.

$$Sp_i = \sum_{s=1,t=1}^{n} \sqrt{(x_s + 1 - x_s)2 + (y_t + 1 - y_t)2\ (i = 1,2,\dots\dots n)} \quad \text{Eq. 2}$$

After this we have calculated mean distance feature (MD_f) by averaging the 2D raw data feature vectors V (S).

$V (S) = [(x_{ts}, y_{ts})]$ {ts = 0,1,2,……n) Eq. 3

This in turn converts our feature vector for signature sample S to

$T (S) = [(MD_f, SP_f, P_f)]$ {S = 1,2,……n) Eq. 4

After these equations we now take care of dimensionality of features before model learning and classification.

3.3.2 Dimensionality Reduction for Feature Vector Representation Since the time series data is in high dimension it is important to reduce its dimensions so that most important and essential information can be preserved within a dataset class. Signature sampling points are in thousands and its direct manipulation will result in many calculations which are practically infeasible. The focus of dimensionality reduction is to use a function F that effectively reduces the dimensionality to a subset of features. Thus further steps such as signature modeling and classification is done on this compact data.

Chebyshev polynomials are well known scheme for approximation of trajectories. The same can be used in signature verification [33]. For each signature spatiotemporal time series up to polynomial m can be calculated through following equation:-.

$$[X|Y|P] = f(t) \approx \sum_{k=0}^{m} b_k c_k \qquad \text{Eq. 5}$$

Where $c_k(t) = \cos(k\cos^{-1}(t))$ and

$$b_0 = \frac{1}{m}\sum_{k=1}^{m} f(t_k),\ b_i = \frac{2}{m}\sum_{k=1}^{m} f(t_k)\, C_i(t_k) \qquad \text{Eq.6}$$

Chebyshev is implemented in various domains and its implementation can be found in [34]. It is possible to approximate time series in the x-y plane by introducing x or y in the equations. In our case we have also used p in the equation.

3.3.3 Signature Classification: Classification is the task to assign a signature to a particular class. Work of Kholmatov [35] and Xu [36] shows that dimensionality reduction can be effectively for feature selection. Through Cehebyshev polynomials a uniform feature based representation of signature sample is provided which is used for learning in our OSV. This in turn will lead to identification of an unseen signature and will assign it to correct class. This is a complex procedure and it is directly related to No. of signatures provided by the enrolled users. In this research work we have shown that our system is capable of learning even with a small training set.

Various classifiers such as Linear classifier, Nearest neighbor and Naïve bayes classifiers are used in signature classification. In this research work we have used SVM classifier which is a well known and popular classifier and is also used in this domain [2], [14], [15]. SVM use a set of data points as input and predicts it to associated output class which makes it a non probabilistic classifier. SVM aims to generate a model by using training data (with labels) and then predicts a class of a query sample on the basis of features supplied to it. Following generic equation is used for separating two classes:-

$$h = \{a|(w,a) + o = 0\} \qquad \text{Eq. 7}$$

where w is the normal vector and o is offset. If the error among the hyperplane and closest sample is 0 then the set of samples are optimally separated with hyperplane. After applying the generic equation some redundancy still persists which can be removed through following equation:-

$$\min_i(w, a_i) + o = 1 \qquad \text{Eq. 8}$$

A graphical representation of SVM is shown in figure 2.

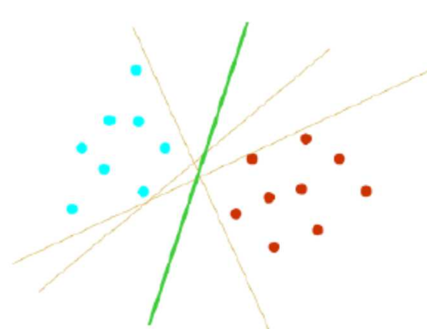

Figure 2: Optimal Separating Hyperplane [37]

4. Experimental Results This research work is using Japanese signature dataset which provides ASCII files which contains the values of X, Y and Z which is the position of X, Y coordinates and pen up/down times respectively. A total of 462 genuine signatures obtained from 11 signers and 396 forged ones are provided for training whereas for testing 42 genuine signatures and 36 forged signatures per author is provided. Evaluation criteria are taken as False Acceptance Rate (FAR) and False Rejection Rate (FRR).

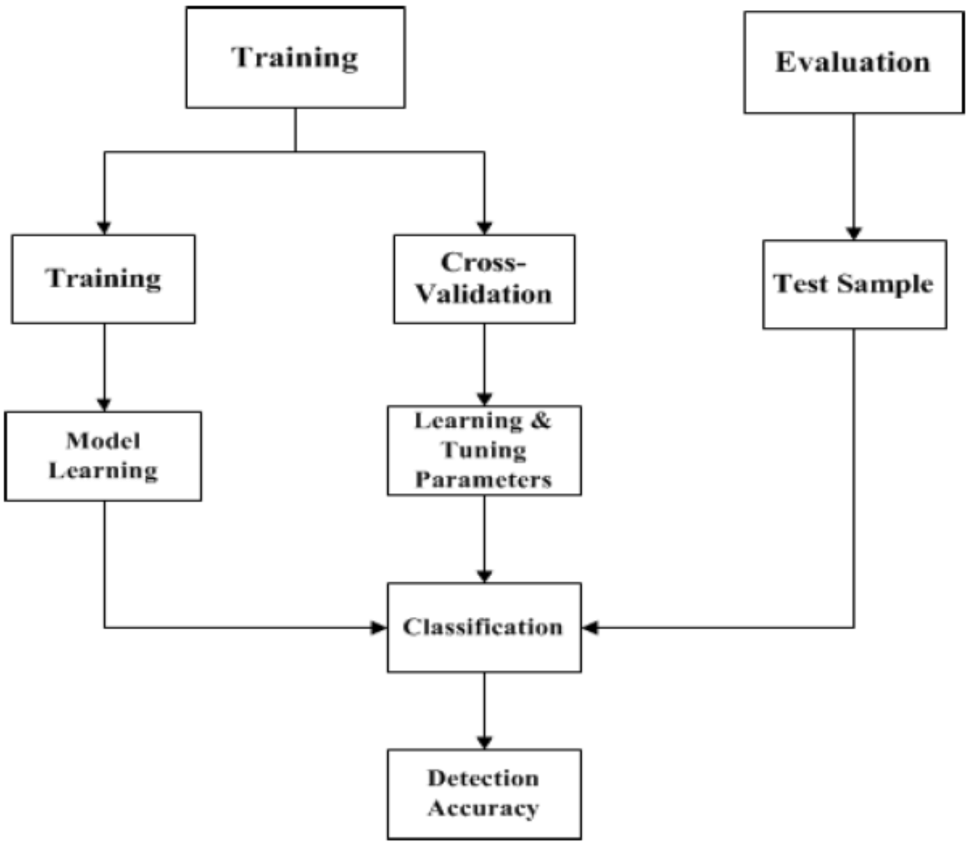

Figure 3: Block Diagram of our study

4.1 Training: The dataset is sub divided in to training and cross validation for model learning and parameter refinement. As explained in signature modeling section the threshold value is calculated which comes as 1055. After threshold identification parameters are tuned to minimize FAR and FRR.

4.2 Evaluation: Signatures in question are compared with the genuine ones and the results of our approach shows promise. The result is given in the Table 1. The equal error rate of our scheme is 19.98% which is better than the one shown in best approach of ICDAR 2013.

Mode	No. of Authors	No. of Total Signature	Detection Accuracy %	FAR %	FRR %
ICDAR 2013	20	1560	72.55	27.36	27.56
Our approach	20	1560	75.12	24.88	24.81

Table 1: Detection Accuracy

4. Conclusion Handwritten signatures' identification is an area of interest which has many applications in the real world. OSV provides better results as compared to offline methods due to the presence of dynamic information available. In this paper a promising scheme is proposed for OSV which is based on well known Chabeyshev polynomials. The proposed approach provides detection accuracy of more than 75% which is better than the one provided by the winner of ICDAR 2013. To cope with the challenges of OSV, a compact feature representation is used which also take in to account speed and pen positions which help in identifying skilled forgery as well.

REFERENCES

[1] Boyer, K. W., Govindaraju, V., & Ratha, N. K. (2007). Introduction to the special issue on recent advances in biometric systems [Guest Editorial].*Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*,*37*(5), 1091-1095.

[2] Bunke, H., Csirik, J., Gingl, Z., & Griechisch, E. (2011). Online signature verification method based on the acceleration signals of handwriting samples. In*Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications* (pp. 499-506). Springer Berlin Heidelberg.

[3] Reza, A. G., Lim, H., & Alam, M. J. (2011). An efficient online signature verification scheme using dynamic programming of string matching. In *Convergence and Hybrid Information Technology* (pp. 590-597). Springer Berlin Heidelberg.

[4] Kholmatov, A., & Yanikoglu, B. (2005). Identity authentication using improved online signature verification method. *Pattern recognition letters*, *26*(15), 2400-2408.

[5] López-García, M., Ramos-Lara, R., Miguel-Hurtado, O., & Canto-Navarro, E. (2014). Embedded System for Biometric Online Signature Verification. *Industrial Informatics, IEEE Transactions on*, *10*(1), 491-501.

[6] Blankers, V. L., Heuvel, C. E. V. D., Franke, K. Y., & Vuurpijl, L. G. (2009, July). Icdar 2009 signature verification competition. In *Document Analysis and Recognition, 2009. ICDAR'09. 10th International Conference on* (pp. 1403-1407). IEEE.

[7] Khalil, M. I., Moustafa, M., & Abbas, H. M. (2009, November). Enhanced DTW based on-line signature verification. In *Image Processing (ICIP), 2009 16th IEEE International Conference on* (pp. 2713-2716). IEEE.

[8] Faundez-Zanuy, M. (2007). On-line signature recognition based on VQ-DTW.*Pattern Recognition*, *40*(3), 981-992.

[9] Qiao, Y., Wang, X., & Xu, C. (2011, June). Learning Mahalanobis distance for DTW based online signature verification. In *Information and Automation (ICIA), 2011 IEEE International Conference on* (pp. 333-338). IEEE.

[10] Salvador, S., & Chan, P. (2007). Toward accurate dynamic time warping in linear time and space. *Intelligent Data Analysis*, *11*(5), 561-580.

[11] Bashir, M., & Kempf, J. (2008). Reduced Dynamic Time Warping for Handwriting Recognition Based on Multidimensional Time Series of a Novel Pen Device. *International Journal of Intelligent Systems and Technologies, WASET*,*3*(4), 194.

[12] Schimke, S., Vielhauer, C., & Dittmann, J. (2004, August). Using adapted levenshtein distance for on-line signature authentication. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on* (Vol. 2, pp. 931-934). IEEE.

[13] Gupta, G. K., & Joyce, R. C. (2007). Using position extrema points to capture shape in on-line handwritten signature verification. *Pattern Recognition*, *40*(10), 2811-2817.

[14] Fauziyah, S., Azlina, O., Mardiana, B., Zahariah, A. M., & Haroon, H. (2009, March). Signature Verification System using Support Vector Machine. In*Mechatronics and its Applications, 2009. ISMA'09. 6th International Symposium on* (pp. 1-4). IEEE.

[15] Kar, B., & Dutta, P. K. (2012). SVM based signature verification by fusing global and functional features. *International Journal of Computer Applications (0975–8887)*, *60*(16), 34-39.

[16] Argones Rua, E., & Alba Castro, J. L. (2012). Online signature verification based on Generative models. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, *42*(4), 1231-1242.

[17] Fierrez, J., Ortega-Garcia, J., Ramos, D., & Gonzalez-Rodriguez, J. (2007). HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recognition Letters*, *28*(16), 2325-2334.

[18] Fallah, A., Jamaati, M., & Soleamani, A. (2011). A new online signature verification system based on combining Mellin transform, MFCC and neural network. *Digital Signal Processing*, *21*(2), 404-416.
[19] Fahmy, M. M. (2010). Online handwritten signature verification system based on DWT features extraction and neural network classification. *Ain Shams Engineering Journal*, *1*(1), 59-70.
[20] Yeung, D. Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., & Rigoll, G. (2004). SVC2004: First international signature verification competition. In *Biometric Authentication* (pp. 16-22). Springer Berlin Heidelberg.
[21] Rashidi, S., Fallah, A., & Towhidkhah, F. (2012). Feature extraction based DCT on dynamic signature verification. *Scientia Iranica*, *19*(6), 1810-1819.
[22] Enqi, Z., Jinxu, G., Jianbin, Z., Chan, M., & Linjuan, W. (2009, May). On-line handwritten signature verification based on two levels back propagation neural network. In *Intelligent Ubiquitous Computing and Education, 2009 International Symposium on* (pp. 202-205). IEEE.
[23] Houmani, N., Mayoue, A., Garcia-Salicetti, S., Dorizzi, B., Khalil, M. I., Moustafa, M. N., ... & Vivaracho-Pascual, C. (2012). BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures. *Pattern Recognition*, *45*(3), 993-1003.
[24] Malik, M. I., Liwicki, M., Alewijnse, L., Ohyama, W., Blumenstein, M., & Found, B. (2013, August). ICDAR 2013 Competitions on Signature Verification and Writer Identification for On-and Offline Skilled Forgeries (SigWiComp 2013). In *Document Analysis and Recognition (ICDAR), 2013 12th International Conference on* (pp. 1477-1483). IEEE.
[25] Zalasiński, M., Cpałka, K., & Er, M. J. (2014, January). New Method for Dynamic Signature Verification Using Hybrid Partitioning. In *Artificial Intelligence and Soft Computing* (pp. 216-230). Springer International Publishing.
[26] Zalasiński, M., Cpałka, K., & Hayashi, Y. (2014, January). New Method for Dynamic Signature Verification Based on Global Features. In *Artificial Intelligence and Soft Computing* (pp. 231-245). Springer International Publishing.
[27] Gruber, C., Gruber, T., Krinninger, S., & Sick, B. (2010). Online signature verification with support vector machines based on LCSS kernel functions.*Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*,*40*(4), 1088-1100.
[28] Kar, B., & Dutta, P. K. (2012). SVM based signature verification by fusing global and functional features. *International Journal of Computer Applications (0975–8887)*, *60*(16), 34-39.
[29] Cpałka, K., & Zalasiński, M. (2014). On-line signature verification using vertical signature partitioning. *Expert Systems with Applications*, *41*(9), 4170-4180.
[30] Wang, K., Wang, Y., & Zhang, Z. (2011, August). On-line signature verification using graph representation. In *Image and Graphics (ICIG), 2011 Sixth International Conference on* (pp. 943-948). IEEE.
[31] Rohilla, S., Sharma, A., & Singla, R. K. (2014). Online Signature Verification at Sub-trajectory Level. In *Advanced Computing, Networking and Informatics-Volume 2* (pp. 369-374). Springer International Publishing.
[32] Cpałka, K., Zalasiński, M., & Rutkowski, L. (2014). New method for the on-line signature verification based on horizontal partitioning. *Pattern Recognition*,*47*(8), 2652-2661.
[33] Naftel, A., & Khalid, S. (2006). Classifying spatiotemporal object trajectories using unsupervised learning in the coefficient feature space. *Multimedia Systems*, *12*(3), 227-238.
[34] Cai, Y., & Ng, R. (2004, June). Indexing spatio-temporal trajectories with Chebyshev polynomials. In *Proceedings of the 2004 ACM SIGMOD international conference on Management of data* (pp. 599-610). ACM.
[35] Yanikoglu, B., & Kholmatov, A. (2009). Online signature verification using fourier descriptors. *EURASIP Journal on Advances in Signal Processing*, *2009*, 12.
[36] Xu, H., Veldhuis, R., Kevenaar, T. A., Akkermans, A. H., & Bazen, A. M. (2008, June). Spectral minutiae: A fixed-length representation of a minutiae set. In*Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on* (pp. 1-6). IEEE.
[37] Gunn, S. R. (1998). Support vector machines for classification and regression.*ISIS technical report*, *14*.