ISSN: 0974-8571 Vol.14 No. 1 June, 2022

International Journal of Computational Intelligence in Control

Offline Signature Verification Based on RFDL

Salma Bibi[1], Muhammad Ijaz Khan[1], Muhammad Farhan[1], Muhammad Iqbal[1], Maria Zuraiz[2], Asia Zaman[1], Shahid Salim[1]

salmameerani@yahoo.com
ijaz171@gmail.com
muhammmadfarhan01@gmail.com
malikiqbalprince1@gmail.com
zuraizm@gmail.com
aasiazaman123@gmail.com
Shahidsalim9@gmail.com

1. Institute of Computing and Information Technology, Gomal University. Pakistan.
2. Department of Computer Science, sub-campus Gomal University Tank. Pakistan.

***Abstract*—Signature is a type of behavioral biometric which is widely used for personal verification. So, it is essential to verify authenticity of signature itself. It is difficult to find true differences between a Signature and a Forgery. Also less accuracy exists in finding of differences between a genuine signature and a high quality skilled forgery. This study constructs a new signature verification scheme Reduced Features with Deep Learning (RFDL). This scheme reduces the volume of features vector of signature image by reducing the dimensionality of extracted features through Principle Component Analysis. Deep Neural Network is used as a classifier for signature verification. DNN is trained on training data set to classify genuine signatures and forgeries. The experimental results of RFDL showed that False Rejection Ratio is reduced highly. FRR 0.6 % and accuracy 99.4 % is observed.**

***Keywords*—Neural Networks, GLCM, Deep Neural Network, FRR, Principle Component Analysis, PNN.**

I. INTRODUCTION

Behavioral biometric is a source of authentication of an individual. Signatures are used as a high source for authentication in official documentations, financial transactions and business. Handwritten stylized name or nick name of someone is termed as signature. A signature is a mark which a person writes on his documents for identification proof. It is required to have methods of automatic signature verification so that authenticity may be verified and guaranteed successfully on a regular basis. Specially, there is a high need of an efficient way to differentiate between genuine signatures and forgeries.

Different types of forgeries are used in documentation as fluent forgery, copied forgery, self forgery and random forgery. The forger attempts to imitate the movement, and neglect shape of letters, the relative location of letter parts, spacing and directions of movement in the genuine signatures is named as fluent forgery. Copied forgery is based on imitation of the shape design. This forgery includes slow tracing of the genuine signatures. Self forgery is exposed and often can be traced because of person's personal signatures characteristics. While random forgery is called simple forgery. In this type of forgery, person name is written in different styles. This forgery is very easy to find by naked eye. The forgery that is made by experienced persons is named as skilled forgery [11]. Figure 1 shows genuine signatures as well as well as forgery.

Fig.1 Genuine Signature & Forgery

This study proposed a signature verification scheme RFDL which combines Principle Component Analysis and Deep Neural Network. It is an improvement in the results of already used Artificial Neural Networks based techniques for signature verification using with respect to accuracy and efficiency. In this scheme, key features of an offline Signature Image are introduced.

With PCA, Hierarchical version of Artificial Network called Deep Neural Network (DNN) is used for classification. PCA has been used for features reduction of signature image and DNN as a classifier.

II. RELATED WORK

In 1989, Mighell proposed a signature verification technique based on Neural Network Back Propagation to identify signature forgeries. An EER of 2% is achieved for random forgeries in this work [1].

Another technique was also developed by Quek, C., & Zhou, R. W. (2002) which combines the results of Euclidean distance obtained after using three feature sets and Neural Networks. In this model, first stage classifier gives input to NN structure. Data set taken was of large volume. An average of 3% FRR and 9.8 % FAR is achieved in signature verification.

For skilled forgery detection, an investigation was made by Quek *et al.* in 2002 and global features of signature image were used for signature verification. Image was converted into binary form and then histogram of the vertical and horizontal of binary image, slant features, pressure features were detected by getting the neighbors of each pixel. The average 22.4% ERR was achieved for skilled forgeries [2].

Oliveira, L. S., Justino, E., & Sabourin, R. in 2007 proposed a writer independent model to reduce the pattern recognition problem into 2-class problem. System performance was improved by using Receiver Operating characteristics. Then classification was made by SVM [3].

Abuhaiba investigated and presented a signature verification method. It is easy method that does not use complex features set. It considers binary pixels intensities. In this method, signature verification is just like graph matching problem. This method is tested on data set containing signatures of five persons. The result achieved is 26.7 % EER for skilled forgeries [4].

Prathiba, M. K., & Basavaraj, L., 2014 investigated that Dynamic features extraction is also a better way of static (off line) signatures verification. Here four speed strokes are considered. Intensity is considered proportional to stroke speed. In this technique, FRR of 14.5 % achieved [6].

A technique based on combination of Back propagation Neural Network and probablistic model is also proposed by Alhaddad, M. J., Mohamad, D., Ahsan, A. M., 2012 to eliminate single model draw backs. BPNN classified local features of signature images while the probablistic model is used to classify global features of image. Final result is obtained by combining both using fusion “ÄND” . Well known data set SVC2004 is used in the study to implement the proposed technique and 0.3 % FRR , 0.5% FAR is obtained . The proposed technique produced encouraging results[7].

Rapanjot Kaur, G. S. (2014) presented a hybrid method which combines Support Vector Machine and Neural networks introduced for offline signature verification. In this method, a signature is represented in image format. By using image processing techniques, Parameters are extracted and on their basis signatures are verified [8].

Tian and Lv (2012) proposed an offline signature verification Method based on registration of genuine signatures and forgeries. Genuine signatures and forgeries points are considered as complex number. A polynomial with coefficients is computed from point sets. Difference between the points is taken to obtain verification function for detection of Signatures and forgeries.

Algorithm based on two steps is implemented. First step is converting affine registration problem to rigid registration problem. Second step is computing coefficients of polynomials. Result of this system is achieved as 13.08 % DER [18].

Alpaydın, E., Cheplygina, V., Loog, M., Tax, D. M. (2015) investigated that each entity can be represented by set of instances in multiple instance classification. This entity set is named by a bag which carries the label. This type of learning is used in various applications. From label information point of view, multiple instance classification is reviewed to find when it is preferable to cast a problem in multiple instance frame work. A set of artificial multiple instance tasks is defined to level the various multiple instance approaches. In the study instance level classification and bag-level classification is compared. Results obtained by this study indicated that instance level and bag level techniques may be suitable. A bag level multiple instance approach is suitable in the case bag gives balanced information. If the bag information contains no valuable information then instance level single instance classifier works well and some time works better. Principle component analysis is also used for reduction of features vector and then PNN is used [10].

TABLE.1
PERFORMANCE OF PNN BASED TECHNIQUES [10]

	FAR (%)	FRR (%)	EER (%)
Random Forgery	1.50	1.52	1.51
Casual Forgery	3.22	3.24	3.23
Skilled Forgery	12.98	13.16	13.07

Umar, P., Singh, S., Garg, A., & Prabhat, N. (2013) detected that the motive to use the Neural Networks for signature verification is that it is powerful and easy tool for pattern recognition. If detailed features of signature image are extracted and Neural Network is then applied, classifier can learn and understand relationship between genuine signatures and forge [12].

M. Raghu Ram Red, C. S. R. K. (2009) introduced that Artificial Neural Network is formed by the interconnection of artificial neurons. A perceptron classifier is a binary classifier. It maps input to an output. It produce target vector. Its biases and weights are trained to produce target vector. The weights are trained by learning mechanism. In this study, Artificial Neural Network is used for online signature verification and distinguish results are obtained [13].

Guru, D. S. and Prakash, H. N. (2009) introduced the feature-dependent threshold concept in signature verification and achieved significant reduction in equal error rate [14].

Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005) proved that if only global features of a signature image are considered, significant results of signature identification can be obtained. On the dataset of 924 signatures of 22 subjects, the system achieved EER 18%. Only, global features are considered, satisfactory results are obtained. Using a database of 924 signatures from 22 writers, our system achieves an equal error rate (EER) of 18 % for high-quality forgeries (skilled forgeries) and an EER of 4.5% for identification of casual forgeries [15].

III. METHODOLOGY

This study introduces a novel signature verification method named as “RFDL” method for offline signature verification” which is based on Deep Neural Network with more than one hidden layers already introduced in machine learning field of Computer Sciences called Deep Neural Network (DNN) and Principle Component Analysis (PCA).

Principal component analysis (PCA) is a statistical procedure. It converts a set of correlated variables into a set of values of linear uncorrelated variables called principle components.

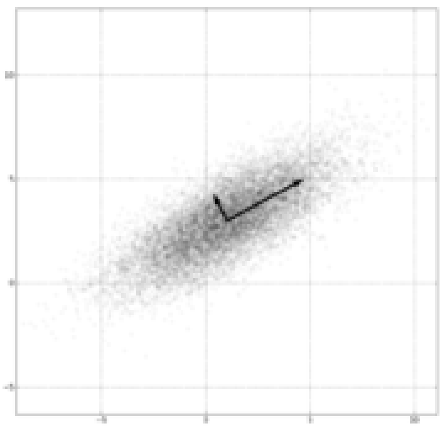

Fig.2 PCA Dimensional Reduction [19]

DEEP Neural Networks has a great worth in the area of Artificial Intelligence. It is an important hierarchical form of neural network which maximizes the efficiency and accuracy of the network. Genuine and forgeries signature verification is a hard task. In offline signature verification, use of DNN minimizes the misclassification rate. Motivation to use the DNN in offline signature verification is its extreme efficiency and accuracy. The specific classifier is trained with signatures from different individuals. More accuracy is expected and achieved from specific classifier.

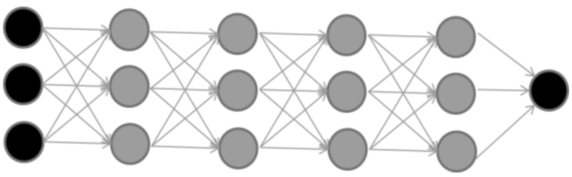

Fig. 3 Deep Neural Network Structure

The implementation flow of RFDL is given in Figure 3.

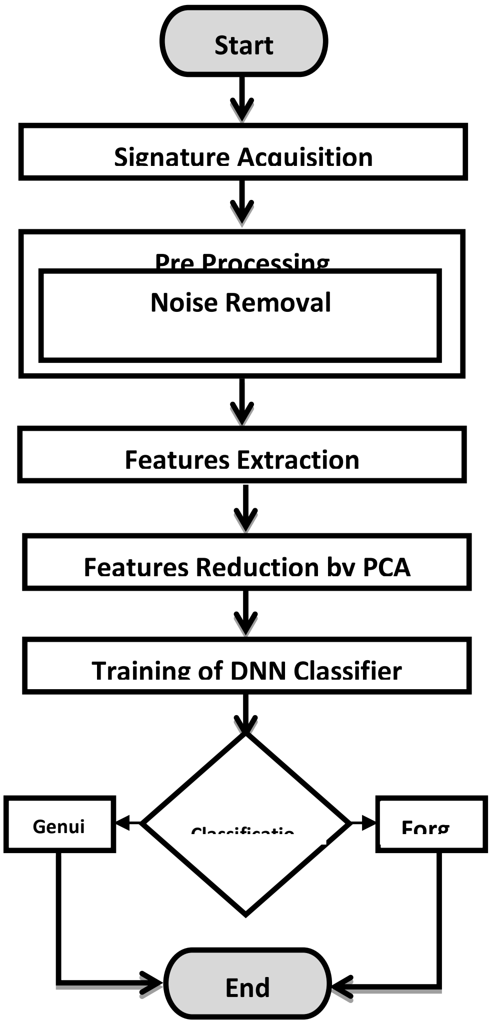

Fig. 4 Proposed Method (RFDL)

The proposed signature verification method Reduced Features with Deep Learning (RFDL) combines the Principle Components Analysis and Deep Neural Network.

The main goal of RFDL is signature authentication by considering signature image features. The RFDL Methodology is taking scanned images of signatures, Preprocessing, Features extraction, Features reduction and Classification.

MATLAB and WEKA are used to implement the proposed methodology of signature verification.

- ***Signature Acquisition***

In this study, signatures considered are offline signatures in nature which means signatures are in the form of hard copy as signatures written on any document. This is the first step of methodology in which signatures of signatory are taken on the plain paper. Each input image is consisting of signatory single signature. So, the signatures of each signatory taken on plain paper are scanned by using HP Laser jet scanner. The default scanning interface of the said scanner is used for signature scanning. These scanned signatures images are considered as input for the proposed signature verification methodology, RFDL.

- ***Data Set***

Data set taken in this study is consisting of 13 scanned signature images of each 36 objects. Similarly, data set for training of the classifier is consisting of 13 scanned signature images of each 36 objects. Signature images are saved in .PNG format.

In this study, SMOTING is applied on the scanned signature data set to increase number of samples of each signatory. It increased data set volume for the purpose to enhance FRDL model accuracy more for signature verification because increase in number of samples of a signatory cause identification of signature easily.

- ***Preprocessing***

Preprocessing is important in signature verification system in the sense that signatures can be some dissimilar because of writing thickness, scale etc. Some preprocesses are applied on signature data set because it is not essential that all captured signatures are always same. The principal objective of preprocessing is to obtain a transformed image with enhanced quality. Preprocessing stage mainly included in the study is Noise removal of the signature image.

Noise is arbitrary disparity of intensity or shade information in signature images. A sort of roughness in an image often exists because of scanner low quality or distortion of document containing signature image. It can be created by the feeler and circuitry of a scanner. Image noise can also initiate in film crumb. So, an image noise is an unwanted result of image capturing that adds forged and inappropriate information in the image. The unusual meaning of noise is always given as not needed signal.

Median Filter is applied to remove noise from image as salt and pepper noise and random noise. This is the intermediate process which prepares the object for feature extraction step.

- ***Features Extraction***

Features extraction and recognition of patterns both are necessary works of signature authentication system. Image features are actually important characteristics of image. Each feature of an image has a particular value. In hierarchy of Image features, two classes of features are defined Parameter features and function features. Parameter features are further classified as local features and global features. Local features are such type of features which are related to each point of signature image. Global features are such type of features which are related to the whole image of signature.

Wavelet Transform, GLCM and Histogram Moments features of data set of noise removed signature images are proposed and extracted in the study.

GLCM are Grey level Co occurrence matrix features. These features include Correlation, Inverse Difference Moment, Entropy, and Angular Second Moment. These features are extracted commonly in pattern recognition. GLCM features are stored in a matrix of j x k x l where l is the number of GLCM.

Textural analysis of a digital image use Wavelet transforms features. With the help of these features, it is possible to analyze an image at different resolution levels. Signal transformation is another way of signal representation. The discrete wavelet transforms works on a data vector. The length of that data vector is power of two. Its work is separation of data into components of various frequencies. It is used for multi scale analysis of signals. The wavelet features are reconstructing exact features. Kociołek *et. al*, (2001) says a vector of Wavelet Transform feature of the signature image is enough for texture analysis and classification of that image. Wavelet Toolbox is available in MATLAB for producing the wavelet transform features of an image. The discrete Wavelet Transformation gives a non-redundant image representation of image signals. In this way comparatively, better localization as spectral and spatial is obtained than other multi scale representations as Gaussian etc. Wavelet transform features gives the representation of time-frequency of the signal. Histogram provides concise and useful information of intensity level in gray scale image. A useful way for image analysis is the histogram of image. This is an approach in which, the statistical moments are taken from grey level histogram of signature image. First order statistics are retrieved directly from signature image. Histogram of an image is the actually graphical plot of intestines. It represents the frequency of occurrence of signature image intensity. The second order moment of histogram provided the variance σ2 (u). Second order moment is an important descriptor to measure the gray level of image. This feature is extracted to identify the contrast, relative smoothness in signature image.

$$m_n(k,l) = E[\mathrm{u}(k,l)^n] = \frac{1}{N_W} \sum_{(i,j)\in W} [I(i-k, j-l)]^n$$

Equation 1 Moments of Order n [20]

So, Moments of Grey-Level Histogram Features of signature image are recommended to extract. MATLAB code is used to extract features.

- ***Features Reduction***

Vector dimensionality reduction is minimization of number of vector dimensions by selecting only important features of the image having maximum information regarding image. The benefit of feature vector dimensionality is to minimize the complexity and cost of algorithm computation.

- ***Training of Classifier: Deep Neural Network (DNN)***

DNN is trained on the training data set consist of 1730 samples of genuine signatures of 36 subjects scanned handwritten offline signature images by giving reduced feature vector of size 14 ranked strongest features as input which was obtained through PCA. DNN with 100-540 hidden layers is taken by considering the fact that the more hidden layers in the deep neural network cause more learning of network. It is adopted that network must be trained with all provided signatures in training data set in a well standard form.

IV. IMPLEMENTATION AND RESULTS

In this Offline signature verification scheme, the data set was divided in two slices training data set and testing data set. 12 samples of each signature are used for training and testing of RFDL. Collectively, 1730 attributes for 36 objects are used. Noise of hand written scanned image is removed by applying median filter.

Fig.5 Noised Signature Image

Fig.6 Noise Removed Signature Image

In MATLAB, Medfilt command is used to apply median filter on the signature images. Wavelet transform, Histogram momentum Features of test data set are extracted. As a whole 90 features are extracted.

Feature vectors are actually the feature points. A feature vector is an n-dimensional vector containing numerical features of an object. A feature vector consists of GLCM, Moments of gray level Histogram and Wavelet Transform features of a signature image are formed which represent signature image.

Features vector size = 1x90

The scaling of features is done before reducing the vector dimensionality.

Then obtained feature vector of signature images of training data set is reduced by Principle Component Analysis up to 17 features. Image features reduction by PCA is shown in Figure 7.

If obtained signature image features are scaled, then after applying PCA, size of features vector is reduced up to 14 features and 1x 14 features are obtained. Experiment is made on original features vector size containing 90 features and also on feature vectors of size 17 and 14.

Reduced features vector size= 1x14

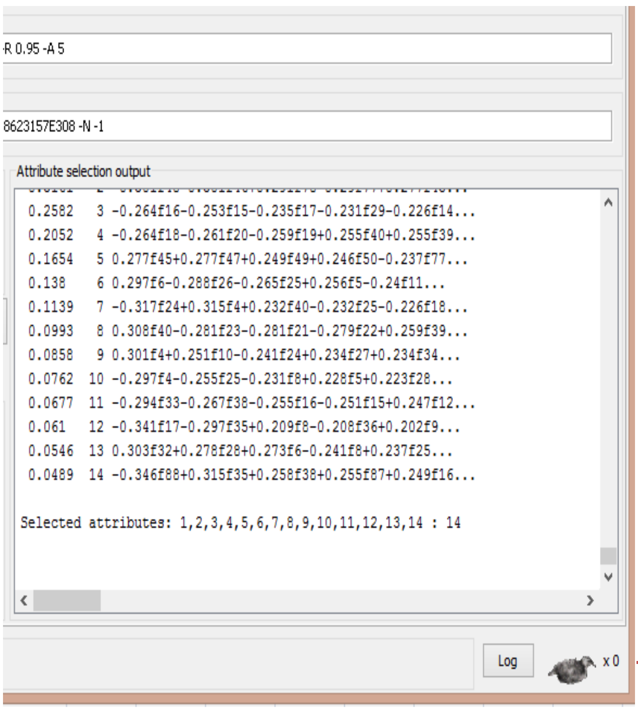

Fig. 7 PCA Reduced Features

The Deep Neural Network with 540 hidden layers is trained on reduced feature vector with most essential 14 features of each signature image.

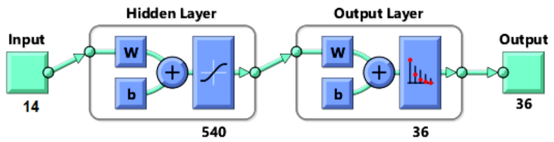

Fig. 8 DNN architecture of RFDL

The trained classifier is tested on images of test data set consist of genuine signatures and forgeries including random and skilled forgeries of each individual.

- ***Verification Accuracy***

The training and testing process is repeated 10 times on the data set. The system is tested on genuine signatures and forgeries queries. While the deep neural network is tested with training signature images samples.

In obtained results, type of error mainly considered related to characteristics of the signature authentication problem is False Rejection Rate, when a genuine signature is rejected. When the random, skilled and other forgeries image samples are presented in test data set for verification the accuracy observed is FAR 0.6%, Accuracy is 99.4 %.

FRR calculated as:

Signature rejected=197

Signatures tested= 1730

FRR = 197/ 1730*100= 11.4 %

The performance evaluation metric is also evaluated by confusion matrix with TP (True Positive), TN (True Negative), FN (False Negative) and FP (False Positive).

TABLE 2

PERFORMANCE OF RFDL

	Accuracy %Age
Without Features Reduction	88.624
With Features Reduction	99.4

For performance comparison PNN classifier are also trained and tested on the same dataset and accuracy observed is described in Table 3.

TABLE 3

RESULTS COMPARISON OF PNN & RFDL

	Accuracy %Age
PNN	99.3
RFDL	99.4

TABLE 8

AVERAGE TIME COMPARISON OF PNN & RFDL

Classification Techniques	Average Time (In Seconds)
PNN	62.9
RFDL	56.6

V. CONCLUSION

In this study, effort is made to create an efficient signature authentication system RFDL by combing Principle Component Analysis and Deep Neural Networks. The scheme is implemented in MATLAB.

Many systems for offline signature verification have developed by using different techniques as simple data base comparisons, use of Artificial Neural Networks, SVM etc but still there is a need to design a system which may provide more accuracy in case of highly skilled forges in efficient way. When large multivariate datasets are analyzed, it is often desirable to reduce their dimensionality.

Principal component analysis is one technique which is used for this purpose. It replaces the p original variables by a smaller number, q, of derived variables, the principal components, which are linear combinations of the original variables. PCA extracts the important information from the data table.

Neural Networks and Deep Learning currently provide the best solutions to many problems in image recognition, speech recognition, and natural language processing. Deep Neural Networks *(DNNs)* have recently shown outstanding performance on image classification tasks compare to conventional Neural Network. DNN can reduce the error to a given level by using many neurons and samples in shallow network. Deep networks: adding a layer can reduce the number of neurons required in the previous layer exponentially.

In this study, Principle component analysis is made for reduction of signature image features. PCA is the simplest multivariate analyses based on Eigen vector. PCA is mostly used commonly for data analysis and PCA can be done by using Eigen value and decomposition of data. The data matrix of signature image is maintained for each attribute. PCA results are described in component scores, also called factor scores. Principal component analysis (PCA) is a statistical procedure. It converts a set of correlated variables into a set of values of linear uncorrelated variables called Principle Components.

VI. RECOMMENDATIONS

The study presented offline signature verification system based on Principle Component Analysis and Deep Neural Network. There is ever chance to bring improvement in every research study. This is recommended that if the back propagation technique is applied on the results obtained in this study (by applying PCA and DNN), the learning of algorithm can be improved and most accurate results regarding offline signature verification can be obtained. Moreover, the work is required regarding that how much number of hidden layers can produce most accurate output of signature verification. The future work will make broad study in this work. Complexity analysis of the offline signature verification by PCA and DNN can also guide the researchers how much is feasibility to implement this studied scheme in real way.

REFERENCES

[1] Xiong, Y. J., Lu, Y., & Wang, P. S. (2017). Off-line text-independent writer recognition: A survey. International Journal of Pattern Recognition and Artificial Intelligence, 31(05), 1756008.

[2] Shabbir, S., Malik, M. I., & Siddiqi, I. (2021). Offline signature verification using feature learning and one-class classification. In Mediterranean Conference on Pattern Recognition and Artificial Intelligence (pp. 242-254). Springer, Cham.

[3] Chandra, S., & Kumar, V. (2022). A novel approach to validate online signature using dynamic features based on locally weighted learning. Multimedia Tools and Applications, 1-18.

[4] Abuhaiba, I. S. (2007). Offline signature verification using graph matching. Turkish Journal of Electrical Engineering and Computer Sciences, 15(1), 89-104.

[5] Jena, D., Majhi, B., Panigrahy, S. K., & Jena, S. K. (2008, August), Improved offline signature verification scheme using feature point extraction method. In *Cognitive Informatics, 2008. ICCI 2008. 7th IEEE International Conference on* (pp. 475-480). IEEE.

[6] Prathiba, M. K., & Basavaraj, L. (2014). Online handwritten signature verification system: A Review. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *3*(2).

[7] Alhaddad, M. J., Mohamad, D., Ahsan, A. M. (2012). *Online signature verification using probablistic modeling and neural network.* Paper presented at the Engineering and Technology (S-CET), 2012 Spring Congress on.

[8] Rapanjot Kaur, G. S. (2014). Enhanced Offline Signature Recognition Using Neural Network and SVM *International Journal of Computer Science and Information Technologies, 5 (3)* 3648-3652.

[9] Dash, T., Nayak, T., & Chattopadhyay, S. (2012). Offline Verification of Hand Written Signature Using Adaptive Resonance Theory Net (Type-1). In *Proc: IEEE Int. Conf. Electronics Computer Technology (ICECT)* (Vol. 2, pp. 205-210).

[10] Alpaydın, E., Cheplygina, V., Loog, M., Tax, D. M. (2015). Single-vs. multiple-instance classification. *Pattern Recognition, 48*(9), 2831-2838.

[11] Bibi, K., Naz, S., & Rehman, A. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79(1), 289-340.

[12] umar, P., Singh, S., Garg, A., & Prabhat, N. (2013). Hand written signature recognition & verification using neural network. *International journal of advanced research in computer science and software engineering*, *3*(3).

[13] Alsuhimat, F. M., & Mohamad, F. S. (2023). Offline signature verification using long short-term memory and histogram orientation gradient. Bulletin of Electrical Engineering and Informatics, 12(1), 283-292.

[14] Guru, D. S., & Prakash, H. N. (2009). Online signature verification and recognition: An approach based on symbolic representation. *IEEE transactions on pattern analysis and machine intelligence*, *31*(6), 1059-1073.

[15] Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE transactions on pattern analysis and machine intelligence*, *27*(6), 993-997.

[16] ahu, N., Rathy, R., Kashyap, I. (2012). Survey and Analysis of Devnagari Character Recognition Techniques using Neural Networks. *International Journal of Computer Applications (0975–888), 47*(15).

[17] Shekar, B., Bharathi, R. (2014). Off-Line Signature Verification Based on Principal Component Analysis and Multi-Layer Perceptrons *Recent Advances in Intelligent Informatics* (pp. 101-109).

[18] Tian, W., & Lv, J. (2012, June). A new affine registration algorithm applied to off-line signature verification. In *Information and Automation (ICIA), 2012 International Conference on* (pp. 806-810).

[19] Er. Mandeep Kaur Randhawa, K., Haryana, Signature verification entailing principal component analysis as a feature extractor. *International Journal of Advanced Technology Engineering Research.*

[20] Tao, Y., & Dong, Z. (2023). An UNet-CRF network with structural similarity for SAR image classification. In Advances in Geology and Resources Exploration (pp. 43-48). CRC Press.