Review on Verification: A Quantitative Report on How Signature Pattern Recognition Scheme Improve Verification's Performance

1Minal D. Shahakar, 2Ayushi S. Tiwari, 3Monica M. Baloji
1Assistant Professor, 2Student, 3Student
Dr.D.Y.Patil Institute of Technology, Pimpri

Abstract - **Human signature is an important bio-metric attribute that can be used to validate person identity. Although signatures are considered as an image and recognized using signature techniques, in which offline signature is challenging task in pattern recognition. In this system, it is proposed and applied offline signature Recognition using Support Vector Machine (SVM) approach and it also presents an off-line signature verification and recognition system using the global, directional and grid features of signatures. Support Vector Machine (SVM) is used to verify and classify the signatures.**

keywords **- Offline signature verification, forgery, genuine signature, Handwritten Signature Verification (HSV), Support Vector Machine (SVM), False Rejection Rate (FRR), False Acceptance Rate (FAR), Average Error Rate (AER), Equal Error Rate (EER).**

I. Introduction

Signatures are composed of special characters and therefore most of the time they can be unreadable. Also intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together. As signatures are the primary mechanism both for authentication and authorization in legal transactions, the need for research in efficient automated solutions for signature recognition and verification has increased in recent years. Recognition is finding the identification of the signature owner. Verification is the decision about whether the signature is genuine or forgery. In this decision phase the forgery images can be classified in three groups:

1. Random: Random forgeries are formed without any knowledge of the signer's name and signature's shape.
2. Simple: Simple forgeries are produced knowing the name of the signer but without having an example of signer's signature.
3. Skilled: Skilled forgeries are produced by people looking at an original instance of the signature, attempting to imitate as closely as possible.

SRVS (Signature Recognition and Verification System) is often categorized in two major classes: on-line SRVS and off-line SRVS. The difference of on-line and off-line lies in how data are obtained. In the on-line SRVS data are obtained using an electronic tablet and other devices. In the off-line SRVS images of the signatures written on a paper are obtained using a scanner or a camera.

Hence off-line signature verification is convenient in various situations like document verification, banking transactions etc. Offline data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation. A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse.

In this system, an off-line SRVS using SVM is proposed. SVMs are universal learners. The system introduced is divided into two major parts:

(i) Training signatures
(ii) Verification or recognition of given signature.

The block diagram of the system is as given below:

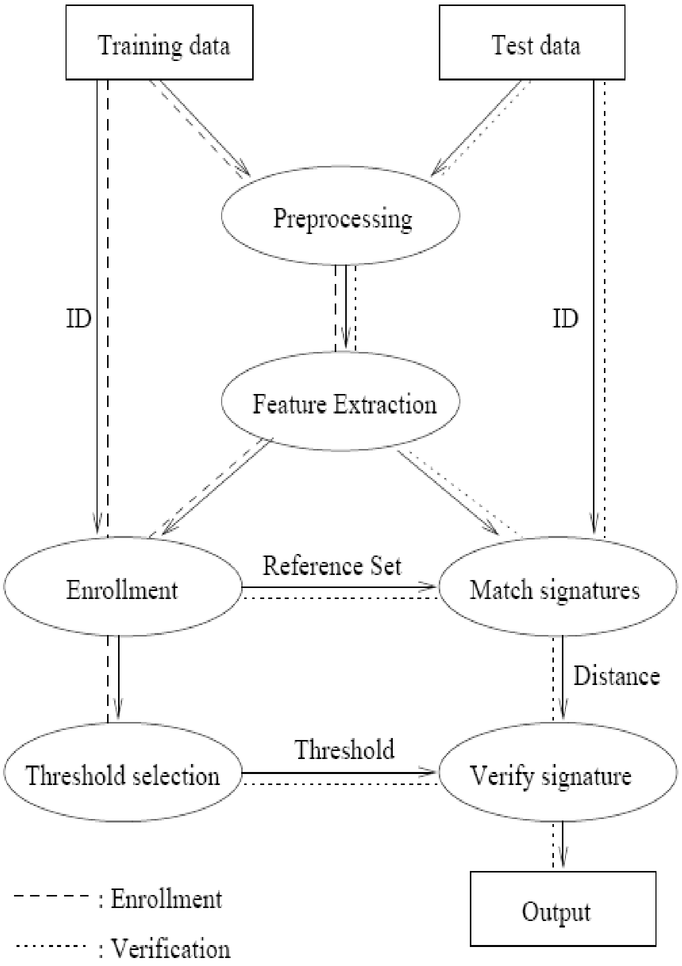


Figure 1: Block Diagram of Signature Verification System

Methodology of Signature Verification System

1. *Pre-Processing:* It is applied in both the training and testing phases. In this phase, signatures are made standard and ready for feature extraction. The preprocessing stage includes four steps: Background Elimination, Noise Reduction, Width Normalization and Thinning.
2. *Feature Extraction:* Extracted features in this phase, which directly affects the verification results, are the input of the training phase. It extracts the global features and grid features after preprocessing, so that a more complete feature vector is formed. It is also applied in both the training and testing phases.
3. *Training, Identification and Evaluation:* In this phase, it trains a proper classifier by using the extracted features. When a new signature is employed, it is matched using the trained classifier which classify it as genuine or forgery. According to the identified results, it evaluates the performance of this system.
4. *Classification:* When a new signature is employed, its features are extracted and matched with those already stores in the database. If the features are matched than it is classified as genuine otherwise forge.

Types of FORGERIES and ERROR RATE

Forgery is an illegal modification or reproduction of any original information. A number of powerful image processing and editing software are available in market due to this it is very easy to manipulate and edit digital images using software it is possible to add or remove important features from a digital image after adding and removing the feature and it gets new image and that image is called as forgery image.

I. TYPES OF FORGERIES

There are eight kinds of forgeries:

a) *Random Forgery:* The signature written by the person who doesn't know the shape of the original signature is the Random Forgery.
b) *Casual Forgery:* The signature written by the person who doesn't know the shape of the original signature is the Casual Forgery.
c) *Skilled Forgery:* The third type called the Skilled Forgery; it is represented by a suitable replication of the genuine signature model.
d) *Simulation Forgery:* The forger has access to a model of the genuine signature from which he practices making copies.
e) *Tracing Forgery:* The following forgery has a model of the genuine signature, which he may hold against a window, or use carbon paper or a light box, and place another sheet of paper over the top, and literally trace the line.

f) *Cut-and-Paste Forgery:* A genuine signature is cut from one document and placed on the spurious document, then photocopied. If the lighting and resolution is properly adjusted, the document will appear genuine.
g) *Electronic Forgery:* The forgery simply digitizes a genuine signature by scanning at a high resolution, then inserts it into the spurious document and prints it.
h) *Freehand Signature Forgery:* The forger simply writes the victim's name without making any attempt to copy.

II. ERROR RATE

a) *False Rejection Rate (FRR)* is the percentage of identification instances in which false rejection occurs is called as FRR. It is also known as Type-I error.
b) *False Acceptance Rate (FAR)* means, it is the percentage of the total false acceptances divided by the total identification attempts. It is also known as Type-II Error.
c) *Average Error Rate (AER)* is the average of Type I and type II Errors.
d) *Equal Error Rate (EER)* is the location on Detection Error Trade-off curve where the FAR and FRR are equal. As the value of EER increase, the performance of the system gets decrease.

The verification process depends on the features that can be extracted from the static signature images only. Number of research has been pursued in handwriting analysis and pattern matching for a number of years. In the area of HSV i.e. Handwritten Signature Verification especially, offline HSV, different technologies have been used and still the area require more work. Based on the features extracted, the method of training, and model used for classification and verification the approaches used by different researchers are different.

II. MOTIVATION

The main problem arises here is the hand writing styles since every different people has its own approach to handwriting in different language. The signature verification system can be used in banking applications, government documents, signing of treaties between countries and student mark sheets. Such a system will remove the manual verification of signatures; two people verifying the same signature will have different opinions and will derive different conclusions about the authenticity of it. It is a more accurate method of verifying signatures of individuals. Offline handwritten signature verification is divided into some major steps: preprocessing, features extraction and feature verification. Features extraction is a vital component in every system; many proposed techniques have included this step with the results as shape features, geometric features, grid features, and textural features, fusion of local and global features. Almost all the methods have shown satisfactory results. However, prominent features selection is most important for accurate signature verification and also for increasing the accuracy. Several techniques are implemented for reduction of irrelevant features. These techniques are failed with a small number of features. Therefore, a feature selection technique is required for the selection of features subset from the features of high dimensionality for the representation of accurate and compact data.

The three main reasons for implementing a feature selection technique include:

1. Utilizing selected subgroup of features to improve verification accuracy in terms of false rejection rate (FRR), average error rate (AER) and false acceptance rate (FAR) by excluding the non-instructive features.
2. Finding out the lowest subgroup of features that could extremely raise the performance of system;
3. Designing simpler and faster model using only most relevant features.

To address this problem, a new technique is presented and implemented in this article for optimal features selection. Selection of these features can increase accuracy of the system. The proposed method is an amalgamation of several steps such as preprocessing and features extraction. The presented approach looks particularly appropriate for signature verification since it meets the challenge of discarding very poor forgeries while retaining the reliability of parallel combination schemes as well as attaining the improved verification performance of successive methods. The major goal of a grouping of several steps is to construct a verification system which reduces both FAR and FRR. Utilize SVM for measuring accuracy of extracted features and performance of features selection algorithm.

III. LITERATURE REVIEW

In paper, [1] A Method of Off-line Signature Verification for Digital Forensics, author Weiwei Pan, Guolong Chen describes Signature verification is an important part of digital forensics. In order to solve the shortcomings of manual identification in technical accuracy and subjectivity, this paper proposed an off-line signature identification method based on Support Vector Machine (SVM). A powerful feature set is collected by extracting grid features and global features of a signature picture. The method is applied for identifying different writing systems and the highest correct probability of identification arrives at 100%. The results indicated that the method is workable and can be an effectively technical support for digital forensics.

The paper presented by Takashi Ito, Wataru Ohyama, Tetsushi Wakabayashi and Fumitaka Kimura[2] proposes a new SVM based technique for combining signature verification techniques using off-line features and on-line features. The off-line feature based technique employs gradient feature vector representing the shape of signature image, and the on-line feature based technique employs dynamic programming (DP) matching technique for time series data of the signatures. The final decision (verification) is performed by SVM based on output from those off-line and online techniques. In the evaluation test the proposed technique achieved 92.96% verification accuracy, which is 1.4% higher than the better accuracy obtained by the individual techniques. This result shows that combining multiple techniques by SVM improves signature verification accuracy significantly.

The paper presented by Mrs. Madhuri R.Deore, Mrs. Shubhangi M. Handore[3] describes the signature identification can be offline or online. We used the image processing technique for offline signature identification here no dynamic feature are available

in offline identification. The contribution of this paper is it describes on various off-line signature recognition & verification schemes is represented this paper.
The paper presented by L. E. Martinez, C. M. Travieso, J. B. Alonso and M. A. Ferrer[5] describes a new method for off-line handwritten signature verification is described in this paper. It is compared with four different parameterization techniques using support vector machines (SVM) as a classification system. The results show which one is the most suitable parameterization technique for this system.
The paper presented by F. Boudamous, H. Nemmour, Y. Serdouk and Y. Chibani[7] describes Offline signature identification and verification systems encounter several challenges such as the diversity of signatories and the limited number of references. To address these problems we propose a new writer-independent system for signature identification and verification. Besides, a new feature generation scheme is proposed by using the Histogram of Templates (HOT). The identification and verification step is performed by SVM. Experiments are conducted on a standard dataset which contains off-line signatures of 55 persons. The results obtained are very promising.

IV. PROPOSED METHOD

SUPPORT VECTOR MACHINE (SVM)

Support Vector Machine (SVM) is proposed by Vapnik. In the process of optimization, setting the constraint conditions for the training error, the optimization objective is to minimize the confidence range. SVM is a learning method based on the minimization criterion, compared with some traditional learning methods, which obviously and has better generalization ability. The proposed system used for extracting the global as well as the grid features and also other global features are considered. For training purpose the Support Vector Machine is used and evaluated based on the accuracy and performance of the system. The System has five main stages they are Signature database acquisition, Pre-processing, Feature extraction, Training, Recognition and Verification.

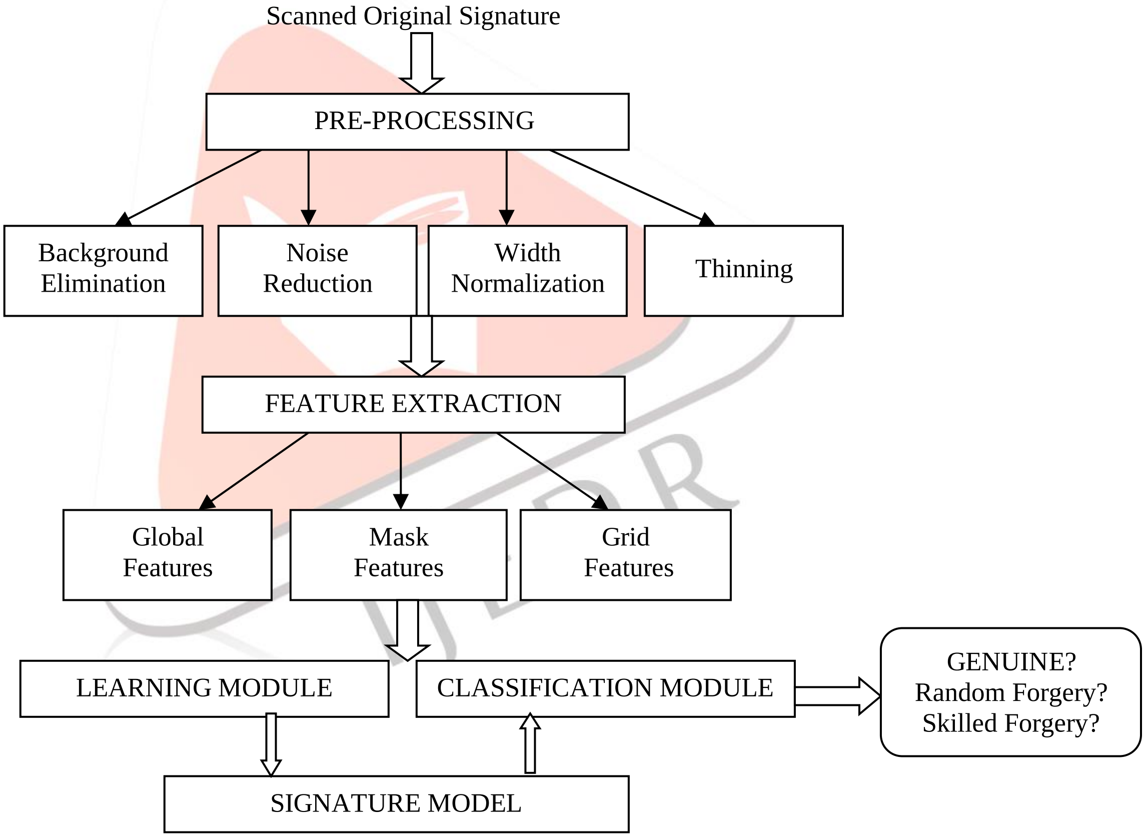


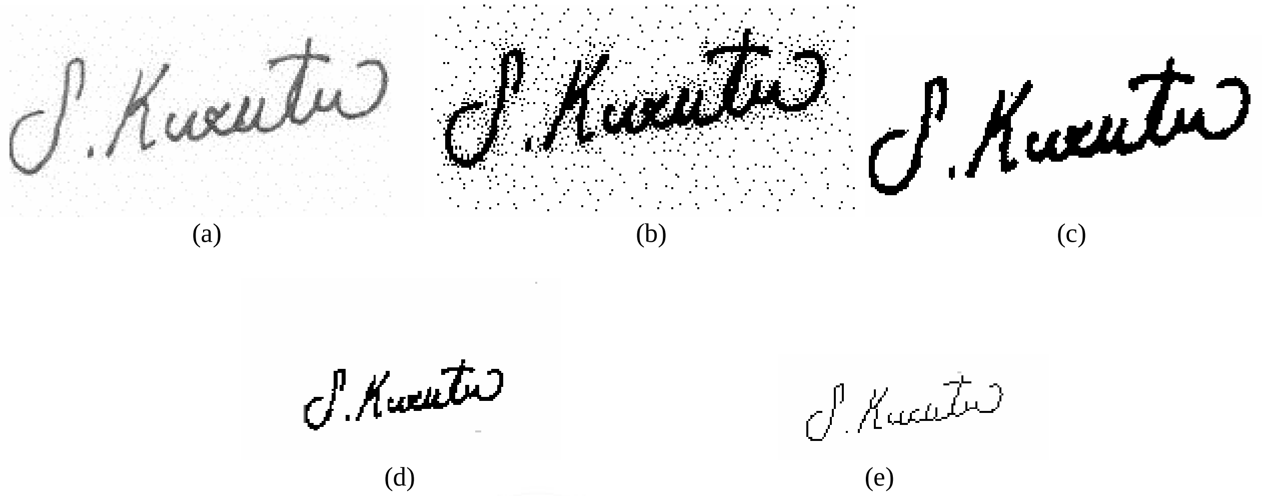
Figure 2: Block Diagram of Proposed System

A. *Signature Database Acquisition*

The handwritten signature images are collected in a white paper and scanned them for creating the train data as well as the test data. For scanning the signatures normal scanners can be used and images can be saved in any of the format like png, jpg etc. For proposed system particular number of genuine signatures should be collected from certain number of persons each with samples. Particular numbers of forged signatures of these persons are collected from different peoples each with samples. Out of samples of genuine signature from a person some are used for training and some used for testing and out of samples of forged signatures some are used for training and some used for testing.

B. *Preprocessing*

The preprocessing step is applied both in training and testing phases. The purpose in this phase is to make signatures standard and ready for feature extraction. The preprocessing stage includes four steps: Background elimination, noise reduction, width normalization and thinning. The preprocessing steps of an ex-ample signature are shown below:



(a) (b) (c)

(d) (e)

Figure 3: Preprocessing Steps: (a) scanning, (b) background elimination, (c) noise reduction, (d) width normalization, (e) thinning applied signatures
[11]Özgündüz, Emre & Şentürk, Tülin & Karslıgil, M. (2005).
Off-line signature verification and recognition by Support Vector Machine.

[1] BACKGROUND ELIMINATION

Data area cropping must be done for extracting features.

[2] NOISE REDUCTION

A noise reduction filter is applied to the binary image for eliminating single black pixels on white background. Neighbors of a chosen pixel are examined. If the number of black pixels is greater than number of white pixels, the chosen pixel will be black otherwise it will be white.

[3] WIDTH NOMARLIZATION

Signature dimensions may have intrapersonal and interpersonal differences. So the image width is adjusted to a default value and the height will change without any change on height-to-width ratio. At the end of width normalization width dimension is adjusted to 100.

[4] THINNING

The goal of thinning is to eliminate the thickness differences of pen by making the image one pixel thick.

C. Feature Extraction

Extracted features in this phase are the inputs of training phase. The features in this system are global features, mask features and grid features. Global features provide information about specific cases of the signature shape. Mask features provide information about directions of the lines of the signatures. Grid features provide overall signature appearance information.

[1] GLOBAL FEATURES

1.1. *Signature Area*: is the number of pixels which belong to the signature. This feature provides information about the signature density.

1.2. *Signature Height-To-Width Ratio*: is obtained by dividing signature height to signature width. Signature height and width can change. Height-to-width ratios of one person's signatures are approximately equal.

1.3. *Maximum Horizontal Histogram and Maximum Vertical Histogram*: the horizontal histograms are calculated for each row and the row which has the highest value is taken as maximum horizontal histogram. The vertical histograms are calculated for each column and the column which has the highest value is taken as maximum vertical histogram.

1.4. *Horizontal and Vertical Center of the Signature*: are calculated using the formula,

$$\sum_{x=1}^{Xmax} x \sum_{y=1}^{Ymax} b[x][y] \qquad \sum_{y=1}^{Ymax} y \sum_{x=1}^{Xmax} b[x][y]$$

$$\text{Centre}_x = \frac{}{\sum_{x=1}^{Xmax}\ \sum_{y=1}^{Ymax} b\,[x][y]} \qquad \text{Centre}_y = \frac{}{\sum_{x=1}^{Xmax}\ \sum_{y=1}^{Ymax} b\,[x][y]} \qquad (1)$$

1.5. *Local Maxima Numbers of the Signature*: the number of local maxima of the vertical and horizontal histogram is calculated.

1.6. *Edge Point Numbers of the Signature*: edge point is the pixel which has only one neighbour, which belongs to the signature, in 8-neighbor.

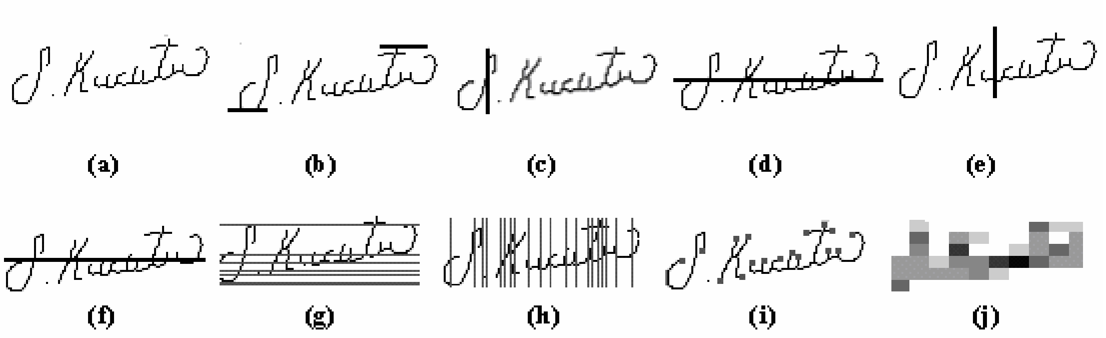


Figure 4: Feature extraction steps: (a) pre-processed signature and (b) height, (c) maximum vertical histogram, (d) maximum horizontal histogram, (e) horizontal centre, (f) vertical centre, (g) horizontal local maxima numbers, (h) vertical local maxima numbers, (i) edge points, (h) grid features of the signature
[11]Özgündüz, Emre & Şentürk, Tülin & Karslıgil, M. (2005).
Off-line signature verification and recognition by Support Vector Machine.

[2] MASK FEATURES

Mask features provide information about directions of the lines of the signatures. The angles of the signatures have interpersonal differences. Each mask is taken all around the signatures, which are same with the mask, is calculated.

[3] GRID FEATURES

Grid features are used for finding densities of signature parts. Signature is divided into equal parts and the image area in each divided part is calculated.

D. Training

The global and grid features extracted are given to the training stage as individually and combined. Here, Support Vector Machine (SVM) is considered for training and best method chosen by performance analysis. Support Vector Machine (SVM) classify two classes, it uses multiclass SVM for the classification of different signatures.

E. Recognition and Verification

After the training process next stage is to recognize a test signature and also verify whether the signature is genuine or forged. The Recognition and verification gives the final output by extracting the features from test images. The Recognition is done by mapping the test signature with the signature identification number given and the name of the signer.

V. ADVANTAGES

- Enrolment (training) is intuitive and fast.
- Signature Verification in general has a fast response and low storage requirements.
- Signature Verification is "independent" of the native language user.
- Very high compression rates do not affect the shape of the signature.

VI. FUTURE SCOPE AND CONCLUSION

Given the shortcomings of manual identification in technical accuracy and subjectivity, this system presents an offline signature identification system based on SVM. It is proven that the proposed system has the advantages of suitable for multi-language environments, higher verification rates and faster identification speed. However, verification rates within and between writing systems is prone to swing in some degree under different partitioning methods. This can be released in two ways. First, the qualified officers who collect the samples should ensure the integrity of signature images. Second, optimize the parameters of classifier model through more experiments.

The future work will find the optimal parameters for different writing system by using the SVM. It can be identified that further researches need to be done in this area to improve in term of computation time and accuracy. Therefore, it recommends the following future works:

- Adapt more approaches in verification step such as combining different approaches to achieve better results.
- Develop international databases to test developed algorithm when they are published to be sure about the authenticity of algorithms.
- Attempt to combine the online and offline approaches with the aim of obtaining reasonable results.
- Attempt to ask two signatures instead one during verification. This may help to achieve a better error rate.
- Try to improve the quality of extracted features including local and global features as these kinds of system mostly relying on its features.

VII. ACKNOWLEDGEMENT

The research has been supported by Mrs. Minal D. Shahakar, assistant professor of the Dr.D.Y.Patil Institute of Technology, gratitude goes to corresponding author: Monica M. Baloji, balojimonica@gmail.com, for providing successful experimental results.

REFERENCES

[1] W. Pan and G. Chen, "A method of off-line signature verification for digital forensics," 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), Changsha, 2016, pp. 488-493.

[2] Takashi Ito, Wataru Ohyama, Tetsushi Wakabayashi and Fumitaka Kimura, "Combination of signature verification techniques by SVM," 2012 International Conference on Frontiers in Handwriting Recognition, pp. 428-431.

[3] Mrs. Madhuri R.Deore, Mrs. Shubhangi M. Handore, "A Survey on Offline Signature Recognition and Verification Schemes," 2015 International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India. May 28-30, 2015, pp. 165-169.

[4] S. Fauziyah, O. Azlina, B. Mardiana, A. M. Zahariah and H. Haroon, "Signature verification system using Support Vector Machine," 2009 6th International Symposium on Mechatronics and its Applications, Sharjah, 2009, pp. 1-4.

[5] L. E. Martinez, C. M. Travieso, J. B. Alonso and M. A. Ferrer, "Parameterization of a forgery handwritten signature verification system using SVM," 38th Annual 2004 International Carnahan Conference on Security Technology, 2004., Albuquerque, NM, USA, 2004, pp. 193-196.

[6] Ruiz-del-Solar J., Devia C., Loncomilla P., Concha F. (2008) Offline Signature Verification Using Local Interest Points and Descriptors. In: Ruiz-Shulcloper J., Kropatsch W.G. (eds) Progress in Pattern Recognition, Image Analysis and Applications. CIARP 2008. Lecture Notes in Computer Science, vol 5197. Springer, Berlin, Heidelberg.

[7] F. Boudamous, H. Nemmour, Y. Serdouk and Y. Chibani, "An-open system for off-line handwritten signature identification and verification using histogram of templates and SVM," 2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Fez, 2017, pp. 1-4.

[8] M. Hanmandlu, A. B. Sronothara and S. Vasikarla, "Deep Learning based Offline Signature Verification," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2018, pp. 732-737.

[9] S. Chandra and S. Maheskar, "Offline signature verification based on geometric feature extraction using artificial neural network," 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, 2016, pp. 410-414.

[10] M. Diaz, M. A. Ferrer, S. Ramalingam and R. Guest, "Investigating the Common Authorship of Signatures by Off-Line Automatic Signature Verification Without the Use of Reference Signatures," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 487-499, 2020.

[11] Özgündüz, Emre & Şentürk, Tülin & Karslıgil, M. (2005). Off-line signature verification and recognition by Support Vector Machine.