Online & offline signature verification using DSVM or other techniques

Muskan Sharma
Amresh Kumar, A.P Cse Deptt
CBS Group Of Institutions, Jhajjar
CSE Engg

Abstract: ***Businesses, governments, and security agencies all rely heavily on online and physical signature verification methods. Checks, certifications, contracts, and other official papers are only some of the many possible applications. Modules for database administration, noise suppression and pre-processing, feature extraction and learning, and signature verification are all a part of the unified signature verification system. Threshold-based techniques are used in matching and decision-making, both of which have immediate practical effects. The system's effectiveness prompted cautious hope. Matching the testing and training features vectors with different threshold values improves the system's overall performance. This is due to the fact that the two groups of vectors exhibit different properties. This technique may be used to scan checks and determine whether or not they have bounced or been cleared. The signature is checked against the master list, then the account number is checked against the database, and finally the percentage of matches is shown. After that, the selected account receives the additional or subtracted amount. More work has to be done in the future to develop methods to make systems robust against the bigger variances that may be encountered in the actual world. While three references are required for many financial processes, it would be preferable if the system could function just as effectively with just one. The necessity for a user-based grading system is shown by these outliers. Our long-term plan includes creating a more efficient and user-friendly approach to score normalization.***

KeyWord: ***Online & offline signature verification, DSVM, biometric systems, Feature Extraction***

1. INTRODUCTION

One way that may be used to verify signatures both online and offline is known as dynamic signature verification models (DSVMs), however there are many more methods that can also be employed. In this essay, I will go through the principles of verifying digital signatures and then show several instances of offline techniques for verifying signatures. A biometric signature is an electronic document pattern that is stored in a database. These signatures are used in biometric systems. When dealing with electronic documents, it is customary to sign legal documents using a computer or another kind of electronic equipment. The use of authentication and authorization processes that make use of biometric signatures is becoming more widespread. Verifying the user's biometric signature is an absolute need when it comes to biometric systems and applications. Biometric signatures provide the necessary authentication techniques, traits, and patterns to decrease the error rate at which users' data may be accessed. This may be accomplished by lowering the rate at which a user's password is entered incorrectly. Digital signature pads are used by biometric systems in order to ensure

the reliability of the data collected from users' signatures. Increased verification reliability is achieved by the use of digital pads to determine the BSV data that is of the highest quality. The behavioral biometric technique is also used by BSV in order to identify the user signature behavior. Utilizing the information that is offered by digital pads, it is possible to validate the characteristics and particulars of signatures. The activities of users give in-depth information that may be utilized as signatures in authentication methods that are very accurate.

One of the primary applications for biometric systems is the reduction of paperwork, and another is an improvement in safety. Digital signatures are used by both online and offline biometric authentication systems. The verification of digital signatures inside a biometric system is a difficult task to do. Several distinct methods are used throughout the process of confirming the authenticity of a biometric signature (also known as a BSV). The use of field-programmable gate arrays, or FPGAs, enables online verification of digital signatures. FPGAs make use of a recognition algorithm in order to pick up on the nuances and patterns that are present in digital signatures. Utilizing an FPGA to capture the specific places, sounds, and patterns of signatures is one way to cut down on the delay that occurs during signature verification. The VFPU method is also used by BSV in order to calculate signatures with the usage of floating-point integers. The VFPUs are calculated with the use of a benchmark database that maintains accurate signature value information. The hidden Markov model, abbreviated as HHM, is used for the digital BSV method. The HHM truly excels when it comes to the offline digital verification that is required in biometric systems [9]. In HHM, a method known as feature extraction is used to the biometric database in order to obtain significant traits for the purpose of providing context for BSV. The HHM enhances the security of the biometric system while also making it more usable for everyday usage. This is accomplished by providing users with clear guidance.

2. RESEARCH METHODOLOGY

In a wide variety of fields, including as banking, the legitimacy of papers, and forensics, validating a signature is an essential stage in the process. Alongside the growing use of digital documents and the meteoric rise of online business, there has been a concomitant explosion in the need for trustworthy signature verification systems that can operate both online and offline. This investigation's objective is to investigate Dynamic Signature Verification Models (DSVM), in addition to existing techniques for signature authentication that are now in use.

2.1 methodology of offline signature verification

Verifying the legitimacy of a signature that was not created in real time is called offline signature verification. In order to determine how similar or different two signatures are, a comparison between the provided signature and a reference signature is performed. The following is a standard procedure for authenticating signatures not online:

- Get both the signatures to be validated and the reference signatures. Digital input devices like graphics tablets and touchscreens may be used to gather signatures, or the actual signatures can be scanned or digitized.
- The first step in the verification procedure is the preprocessing of the captured signature pictures to get rid of any noise or artifacts. Normalization, contrast enhancement, and scaling are common preprocessing techniques for images.

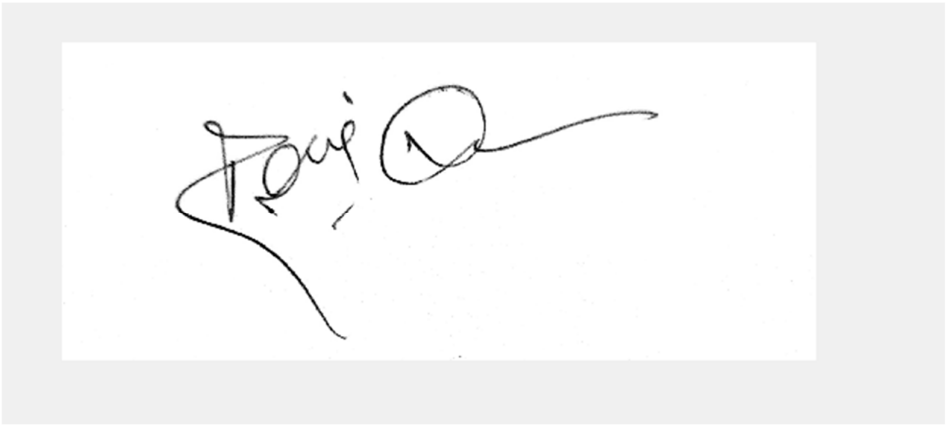
- Signature photos capture unique traits, therefore one step in the process is to extract such features. These characteristics should be adaptable to different writing styles and accurate in recording the individual traits of the signature. These characteristics are often used:

- The retrieved characteristics must be transformed into a format that is useful for comparison. Methods such as normalization, scaling, and encoding into a fixed-length feature vector may be used for this purpose.

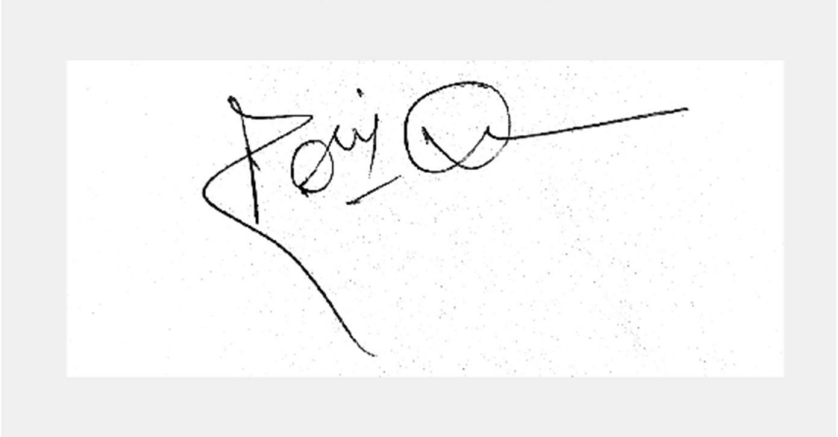
3. RESULT AND DISCUSSION

When doing verification offline, only static characteristics are taken into account, however when conducting verification online, both static and dynamic features are included. After the signature has been written, offline recognition may take place. Later, an optical scanner is used to read the data from the picture and turn it into a digital format. Features retrieved from the static signature picture trace alone must be used in the verification procedure. Since most modern financial transactions are still conducted on paper, off-line signature verification is vital for identifying the writer identity, while being complex to design. This emphasizes the need of reliable signature verification. Data gathering, pre-processing, feature extraction, comparison procedure, and performance assessment are the five subproblems that must be solved during the construction of any signature verification system. The only thing that has to be dealt with in offline verification are scanned or photographed signatures. To verify a signature offline, a picture of the signature must be obtained. Graphometry provides a detailed description of this picture as a representation of a particular person's handwriting style. The goal of such a system is to identify forgeries based on individual and group differences in variability. The applied system must be able to identify intra-personal variability as forgeries while ignoring inter-personal fluctuation and marking them as authentic.Since the signature template used in off-line signature recognition is generated by an imaging device, we have access to only static features of the signatures themselves. The individual's physical presence during verification is not required. Therefore, off-line signature verification is useful in many contexts, such as document verification, financial transactions, etc. Offline signature recognition systems need careful design to attain the requisite accuracy because of the small number of attributes available for verification. The way information is gathered is what separates offline from online activities. Offline SRVS involves obtaining a scanned or photographed image of a handwritten signature, whereas online SRVS relies on a dedicated peripheral device to collect data. In this study, we offer a method for offline signature verification and recognition. The three-part approach includes a "pre-processing" phase in which an assortment of procedures and filters are applied to an already-good signature picture in order to make it even better. The preprocessing step's goal is to choose the most effective signature picture for the feature extraction stage, and this is more of an art than a science. The global feature, the texture feature, and the grid information feature [3] are all very potent tools. After calculating those three attributes for each trademark picture, the data moves on to the neural network step. The classifiers in a neural network have two stages: In the first classifier step, three back propagation (BP) neural networks are used, each of which is trained separately from the others and using data from only one of the three characteristics. The second-stage classifier receives information from both of each BP's outputs. The second stage classifier is made up of two RBF neural networks. The second classifier (RBF) is responsible for integrating the output of the first classifier (BP) to get a conclusion for the system [4]. Signatures drawn

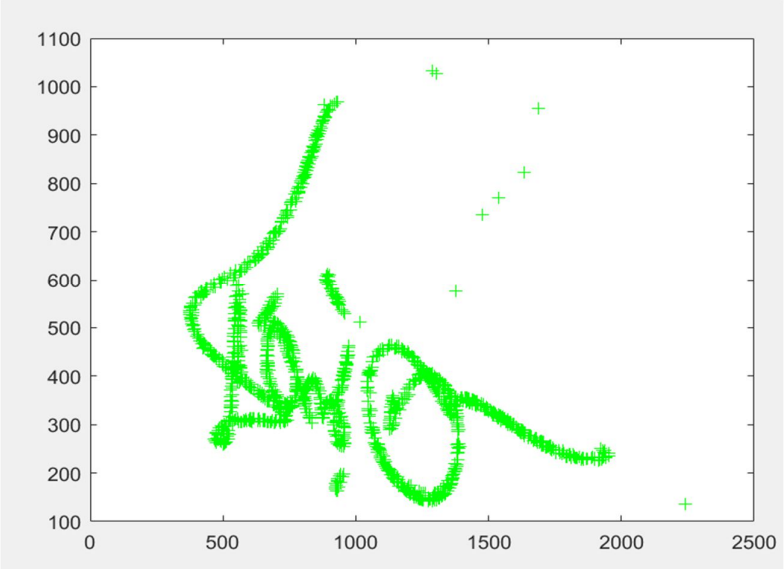
with a regular pen are the focus of offline verification. Several methods for both groups have been offered.



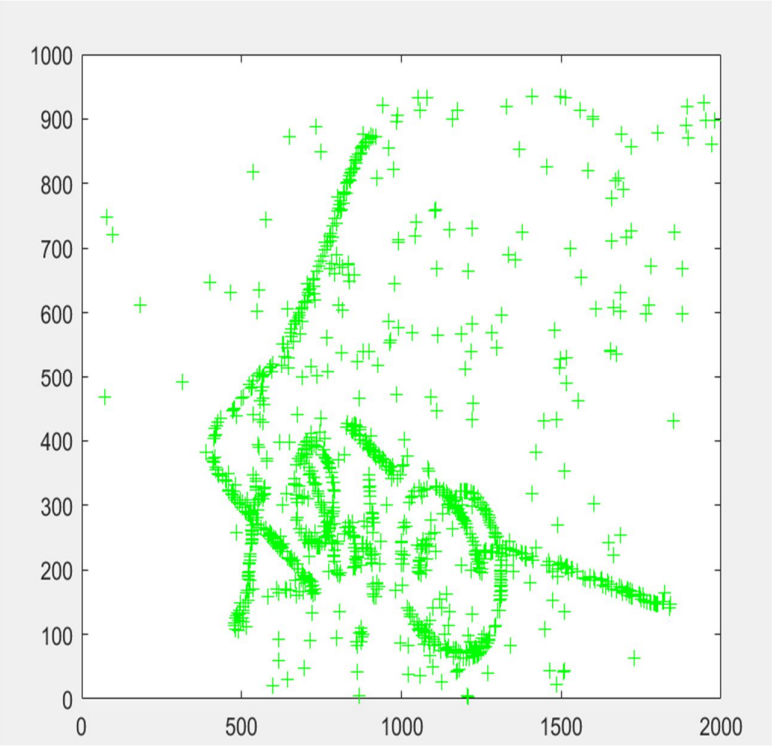
4. Fig. Signature of image 1



5. Fig. Signature of image 1



6. Fig. Pre-processing of image-1



7. Fig. Pre-processing of image -2

8. Fig. Signature matched of images

4. CONCLUSION AND FUTURE WORK

Dependable signature verification systems are essential to the operations of various business processes in addition to law enforcement and security protocols. It may be used

in a broad number of contexts, such as on checks, certificates, contracts, and other legal documents. The integrated signature verification system includes modules for database management, noise reduction and pre-processing, feature extraction and learning, as well as verification. Matching and decision-making are both processes that make use of threshold-based approaches, and both processes have practical repercussions that are quite close in time. The performance of the system provided a cause for optimism. Utilizing distinct threshold values for matching the testing and training features vectors helps to enhance the system's overall performance. This is because the two sets of vectors have distinct characteristics. With the use of this method, checks may be scanned, and their standing—whether they have bounced or been cleared—can be established as a result. First, the signature is compared to the masters, then the account number is compared to the database, and lastly, the percentage of matches is shown. After that, the amount of money is either added to or removed from the account that has been chosen.

REFERENCES

1. Stauffer, M., Maergner, P., Fischer, A., & Riesen, K. (2020). A survey of state of the art methods employed in the offline signature verification process. *New trends in business information systems and technology: digital innovation and digital business transformation*, 17-30.
2. Okawa, M. (2019). Template matching using time-series averaging and DTW with dependent warping for online signature verification. *IEEE Access*, *7*, 81010-81019.
3. Okawa, M. (2020). Online signature verification using single-template matching with time-series averaging and gradient boosting. *Pattern Recognition*, *102*, 107227.
4. Okawa, M. (2021). Time-series averaging and local stability-weighted dynamic time warping for online signature verification. *Pattern Recognition*, *112*, 107699.
5. Banerjee, D., Chatterjee, B., Bhowal, P., Bhattacharyya, T., Malakar, S., & Sarkar, R. (2021). A new wrapper feature selection method for language-invariant offline signature verification. *Expert Systems with Applications*, *186*, 115756.
6. Tahir, N. M., Ausat, A. N., Bature, U. I., Abubakar, K. A., & Gambo, I. (2021). Off-line handwritten signature verification system: Artificial neural network approach. *International Journal of Intelligent Systems and Applications*, *13*(1), 45-57.
7. Ghosh, R. (2021). A Recurrent Neural Network based deep learning model for offline signature verification and recognition system. *Expert Systems with Applications*, *168*, 114249.
8. Pinzón-Arenas, J. O., Jiménez-Moreno, R., & Pachón-Suescún, C. G. (2019). Offline signature verification using DAG-CNN. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(4).
9. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognition*, *70*, 163-176.
10. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2016, July). Writer-independent feature learning for offline signature verification using deep convolutional neural networks. In *2016 international joint conference on neural networks (IJCNN)* (pp. 2576-2583). IEEE.

11. Soleimani, A., Araabi, B. N., & Fouladi, K. (2016). Deep multitask metric learning for offline signature verification. *Pattern Recognition Letters*, *80*, 84-90.
12. Malik, M. I., Liwicki, M., Dengel, A., Uchida, S., & Frinken, V. (2014, September). Automatic signature stability analysis and verification using local features. In *2014 14th International Conference on Frontiers in Handwriting Recognition* (pp. 621-626). IEEE.
13. Faraj, K. H. A., Abbas, N. H., Yasen, K. N., A Razak, L. F., & Malallah, F. L. (2018). Offline handwritten signature recognition using histogram orientation gradient and support vector machine. *Journal of Theoretical and Applied Information Technology*, *96*(8).
14. Zois, E. N., Alewijnse, L., & Economou, G. (2016). Offline signature verification and quality characterization using poset-oriented grid features. *Pattern Recognition*, *54*, 162-177.