A Study on Online & Offline Signature Verification

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

Abstract:* Online & offline 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. Future research on systems should have a major emphasis on finding ways to make them more resilient in the face of the larger variations that may be seen in the real world. However, it would be better if the system could perform just as well with a single reference as opposed to the minimum need of three references, which is necessary for many different financial operations. These kinds of outliers bring to light the need of using a user-based scoring system. One of our objectives for the foreseeable future is to develop a method of score normalization that is both more effective and more user-friendly.

Keywords:* DSVM, Online Signature, Offline Signature, FPGAS,

I. INTRODUCTION

Dynamic signature verification models (DSVMs) are one method, but there are many more that may be used to verify signatures both online and offline. In this article, I will discuss the fundamentals of digital signature verification and present some examples of offline signature verification methods. In biometric systems, a biometric signature is an electronic document pattern that is kept in a database. Signing papers on a computer or other electronic device is the norm when working with electronic documents. The use of biometric signatures in authentication and authorisation procedures is becoming more common. When it comes to biometric systems and apps, verifying a user's biometric signature is a must. Biometric signatures offer the required authentication procedures, characteristics, and patterns to lower the mistake rate at which users' data may be accessed. In order to collect reliable data from signatures, biometric systems make use of digital signature pads. Digital pads identify the best data needed for BSV, increasing verification reliability. BSV also use the behavioral biometric approach to recognize user signature behavior. The qualities and specifics of signatures may be verified with the use of the data provided by digital pads. Users' actions provide detailed information that may be used as signatures in authentication procedures with a high degree of precision.

Reduced paperwork and increased safety are two of the primaries uses for biometric systems. Online and offline biometric systems alike make use of digital signatures. Verifying digital signatures in a biometric system is a challenging undertaking. The process of verifying a biometric signature (BSV) employs a number of different strategies. Online digital signature verification uses fieldprogrammable gate arrays (FPGAs). FPGAs use a recognition algorithm to pick up on the subtleties and patterns of digital signatures. Signature verification delay may be decreased by using an FPGA to record the precise locations, sounds, and patterns of signatures. BSV also use the VFPU technique for determining signatures using floating-point numbers. VFPUs are determined using a benchmark database that stores precise signature values. For the digital BSV procedure, the hidden Markov model (HHM) is employed. Offline digital verification in biometric systems is where the HHM really shines [9]. Important characteristics from the biometric database are extracted using a feature extraction approach in HHM to offer context for BSV. By giving users clear guidelines, the HHM improves the biometric system's security while also making it more practical.

It is common practice to utilize dynamic biometric signature verification to confirm the true identities of users. In order to authenticate a user successfully, dynamic biometric signature verification is often used. Dynamic signature verification employs a hybrid method that draws on both locally available data and data from around the globe. The digital signatures in the database are checked for variations and trends using hybrid algorithms. The verification data required to lower identification latency is provided by both global and localized information. In order to authenticate signatures, CNNs employ a feature extraction approach to extract crucial characteristics and specifics. CNNs improve the efficiency and effectiveness of biometric systems by decreasing the number of authentication errors and the amount of time required for authentication. It is standard practice to utilize the ANN algorithm for verifying dynamic signatures. For authentication purposes, ANNs use the pixel-matching method (PMT) to identify identical signature pixels. The PMT has a high detection rate and increases the authentication ratio in biometric systems and applications.

II. LITERATURE REVIEW

Stauffer et al. (2020), Many commercial and legal transactions across the globe need legally binding handwritten signatures. In other words, signatures have served as a method of verification and validation for hundreds of years. However, there is a possibility of abuse due to signatures' widespread usage. Automatic signature verification was offered as a means of reducing this vulnerability. Signature verification systems attempt to identify forgeries given a suspect signature. Numerous signature verification frameworks have been presented during the last few decades. These structures often fall into either "online" or "offline" categories. Temporal information regarding the signing process is provided for online signature verification, but not for offline signature verification. Therefore, verifying signatures offline is often considered more difficult. This chapter provides a full overview of offline signature verification and a discussion of the techniques generally used throughout the process.

Banerjee et al. (2021), Online signature verification may be more convenient for many people, but its offline version is still very useful in places like rural parts of developing nations where access to smartphones and reliable internet may be limited. After the signature image's signal has been processed, four distinct types of features—statistical, shape-based, similarity-based, and frequency-based—are retrieved. Then, to cut down on the number of features that need to be considered, they've developed a new wrapper feature selection technique using the Red Deer Algorithm, a recently suggested meta-heuristic approach, to ensure that only the most important characteristics are retained for use in the signature authentication and verification procedure. The authentication and verification procedure has been completed using a Naive Bayes classifier confidence score. Our model has been tested on the English CEDAR dataset, the Persian UTSig dataset, the Dutch Sigcomp 2011 dataset, the Chinese Sigcomp 2011 dataset, and the Bengali SigWIcomp 2015 dataset. The obtained findings demonstrate the superiority of the suggested model over its predecessors.

Tahir et al. (2021), The widespread usage of signatures as a means of identity verification nowadays is sufficient cause to implement an Automatic Verification System (AVS). The choice between offline and online verification is made by the application. The information that is dynamic at the time a signature is formed is used by an online system. On the other hand, images (a scanned signature) are used in an offline system. In this research, we show how to verify signatures offline using just a small collection of geometric characteristics with basic shapes. The above-mentioned attributes are extracted from a subset of a subject's actual signatures, and are then used to create an average signature for that subject. Signatures are used as a model against which other signatures may be authenticated. Euclidean distance is used to find out how similar two signatures are inside the feature space. If the calculated Euclidean distance is less than a predetermined threshold (equivalent to the lowest level of allowable resemblance), then the subject's signature on the test document is verified as genuine. This study provides specifics on the declared capabilities, processing, implementation, and outcomes.

Pinzón-Arenas et al. (2019), This paper describes the creation of a DAG-CNN based on the writer-independent technique, with the goal of classifying and validating the offline signatures of three users. The trained network is then tested and validated; the results demonstrate the features learned by the network and verify that this neural network configuration can be used in applications for offline signature identification and verification with overall accuracies of 99.4% and 99.3%, respectively.

Hafemann et al. (2017), Verifying the identity of a signer based only on a handwritten signature might be problematic in situations when a forger obtains the signature of an individual and tries to recreate it on purpose. The performance suffers as a result; even the best systems in the literature make around 7% of verification mistakes. A battery of tests was run using the GPDS, MCYT, CEDAR, and Brazilian PUC-PR datasets. They achieved state-of-the-art performance on GPDS-160 by achieving an Equal Error Rate of 1.72%, which is a huge improvement above the 6.97% observed in the literature. They also demonstrated that these features outperform state-of-the-art on datasets other than GPDS without requiring any changes to the representation.

Hafemann et al. 2016), Over the course of many decades, several disciplines, including graphology, computer vision, and signal processing, have made significant contributions to the research of offline, fully automated handwritten signature verification. One approach they propose is to use feature learning. Our experimental results show that learned features are useful for discriminating between users across many datasets.

Soleimani et al. (2016), In this study, we introduce Deep Multitask Metric Learning (DMML), a unique classification approach for offline signature verification. DMML takes into account not just the training samples of the class in issue when determining whether or not a signature is legitimate, but also the similarities and differences between authentic and counterfeit samples from other classes. Therefore, DMML trains a distance metric for each class along with other classes utilizing the concepts of multitask and transfer learning. DMML's architecture consists of a common layer that takes a writer-independent approach, followed by layers that are specifically designed to learn author-specific details.

Malik et al. (2014), There are two main goals for this study. To begin, it introduces a new method for analyzing the stability of a signature by focusing on the signature's individual components. The results of the local stability analysis are then used to develop a one-of-a-kind signature verification system, which is then evaluated using the authentic, forged, and disguised signatures from the 4NSigComp2010 forensic signature verification competition's publicly available dataset. The proposed system's 15% EER is much less than those of the competing systems.In addition, they evaluate the proposed system against other systems that have been previously reported using the same data. Even compared to existing systems, the suggested system performs better.

III. RESEARCH METHODOLOGY

Verifying a signature is a crucial step in many industries, including finance, authenticity of documents, and forensics. The demand for reliable online and offline signature verification systems has increased dramatically in tandem with the widespread use of digital documents and the proliferation of online commerce. The purpose of this study is to look at Dynamic Signature Verification Models (DSVM) and other methods currently in use for signature authentication.

Mathematical model of Dynamic Signature Verification Method

Mathematical models are used in the biometric authentication approach known as dynamic signature verification, which analyzes and verifies the validity of a signature based on dynamic factors including the signer's pen pressure, speed, acceleration, and timing. A generic mathematical model for verifying dynamic signatures is as follows:

- Data Acquisition:
    - ✓ Signature acquisition: The user signs on a digital device using a digital pen or stylus to capture the signature. This produces a series of data points that may be interpreted as the signature.
- Preprocessing:
    - ✓ The signature is reliably represented by sampling the obtained data points at predetermined intervals.
    - ✓ The signature may be made insensitive to changes in pen size, location, and orientation by normalizing the collected data.
- Feature Extraction:
    - ✓ Features like pen speed, acceleration, direction changes, and pressure may all be derived from the time-series data, which fall under the category of "time-domain features."
    - ✓ Features may also be extracted from the stroke length, height, breadth, and aspect ratio of the signature, all of which are spatial properties.
    - ✓ Statistical characteristics: The data may be analyzed by computing statistical measurements such as the mean, standard deviation, skewness, and kurtosis.

IV. CONCLUSION AND FUTURE WORK

Law enforcement, security, and several corporate procedures all rely heavily on dependable signature verification systems. It has a wide variety of uses, including on checks, certifications, contracts, etc. Modules for database administration, noise reduction and pre-processing, feature extraction, learning, and verification are all a part of the integrated signature verification system. Threshold-based methods are used for both matching and making decisions, and both methods have near-term practical implications. The system's performance was encouraging. The overall performance of the system is improved by using different threshold values for matching for testing and training features vectors. Checks may be scanned and their status as bounced or cleared can be determined with the help of this process. It first checks the account number against the database, then checks the signature against the masters, and finally displays the percentage of matches. The money is then added to or subtracted from the designated account.

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.