WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Signature Verification and Forgery Detection System

M. B. Sudhan[1], Abhilasha Sarkar[2], Aditi Viswanath[3], Akshita Koul[4], Amipra Srivastava[5]

[1]Head of Department,Department of Computer Science and Engineering,MVJ College of Engineering, Bangalore, Karnataka, India.
[2,3,4,5]Undergraduate Scholar, Department of Computer Science and Engineering, MVJ College of Engineering, Bangalore, Karnataka, India
DOI: https://doi.org/10.55248/gengpi.2023.4.4.35359

A B S T R A C T

The signature is an important, unique and essential mark of authentication. Each person has an individual signature, which is primarily used for personal identification and confirmation of the authenticity of important documents or legitimate transactions. Today, signatures are widely used as a means of identity verification in many fields such as banking, real estate, and finance.

Keywords: SigNet, ReLu, Support Vector Machine (SVM), SVFGNN, False Rejection Rate (FRR), False Acceptance Rate (FAR), & Equal Error Rate (EER), Harris algorithm, Surf algorithm, pixel-based method, Neural Networks (NN), k-Means, OTSU Thresholding.

1. Introduction

Signature verification and forgery detection systems are used to verify a person's identity by verifying a signature. These systems can be used both online and offline. Online signature verification and forgery detection systems are used to verify a person's identity by verifying a signature in an online environment. A reference signature is usually stored in a secure database and is used to compare a person's signature to ensure its authenticity. The system can also detect possible fake attempts by comparing the signature with a reference signature. Offline signature verification and forgery detection systems are used to verify a person's identity by verifying a signature in an offline environment. These systems use several methods to capture a person's signature and compare it to a reference signature. Both online and offline signature verification and forgery detection systems are important tools for authenticating a person's identity. These systems are used in a variety of industries, including banking, healthcare and government. They are also used to protect against fraud and identity theft.

2. Literature Survey

2.1 SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification

In this paper, it proposes a detailed method for detecting forged signatures in offline signature verification using Siamese neural networks. Siamese grids are designed to capture two different, similar, or different images and calculate a distance measure between higher-level features to determine their similarity. The authors used a preprocessing step to scale all images to a fixed size of 155 × 220 using bilinear interpolation. The similarity measure used in this network includes the Euclidean distance between tree representations on either side of the Siamese network. The loss function used is divergent loss, which ensures that images of the same class are closer to each other than images of different classes. The activation function used is ReLu, which helps make the network more efficient [1].

To evaluate the performance of the signature verification algorithm, the authors considered four widely used databases, including CEDAR, GPDS300, the GPDS synthetic signature database, and the BHSig260 Signature Corpus. They experimented with these datasets and found that their model outperformed the peak results of most standardized signature datasets. In addition to these experiments, the authors also performed experiments on synthetic datasets to simulate real counterfeit coins and cross-domain datasets to test the network's ability to detect fraudulent behavior in different handwriting styles. The authors found that their Siamese network, called SigNet, can model generic prototypes of original imitations from synthetically generated data. Overall, this paper demonstrates the effectiveness of Siamese neural network models in offline signature verification and highlights the importance of preprocessing, loss function, and activation function selection to obtain high-performance results.

2.2 Online Signature Verification System

This aims to achieve the ability to distinguish between authentic and fake signatures. This feature is implemented using a support vector machine (SVM). Here, the signature is represented as a boundary consisting of x-y coordinates, and the data is then stored as a text file in the signature database. SVMs are commonly used in pattern recognition and regression problems [2].

The method consists of different steps: the first step is to take the input signature, read the signature in x-y coordinates, and the points in it allow us to correctly know the point of the pencil, such as the pencil is pointing up, the pencil points down. The second stage is data acquisition, in which real-time signatures entered by special pens and digital discs are read into the processor for processing and then stored in a database called the signature database. The third step is preprocessing, which follows a three-step procedure, namely normalization, sampling time, and resampling distance. The fourth step improves feature extraction, adding variety that helps distinguish categories. The generated features are added to the database and the image features are matched to the input image. To demonstrate the correctness of the program that sends signature images with its characteristics, the authors of this paper used two methods.

2.3 Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks

This proposes offline signature verification using a neural network (SVFGNN) that integrates global network and features. It combines generic and network functions to create a set of signature verification functions. In this case, the test signatures are compared with the database signatures based on the set of features defined using the neural network [3].

The proposed model is divided into three phases: the preprocessing phase, the feature extraction phase, and the validation phase. In the preprocessing stage, from the signatures collected with the scanner, signature features are extracted through a preprocessing step consisting of denoising, volume normalization, and skeletonization. In the feature extraction stage, two sets of features are used, such as network features and global features, where the network information features divide the image into an appropriate number of rectangular regions, and the general features provide state-specific information about the structural signature. In the validation phase, a neural network (NN) is trained, in which a standard backpropagation neural network classifier is used for validation. The proposed neural network consists of 30 input variables extracted from signature features, and then designed to verify one signature at a time. It should also be noted that using the proposed algorithm improves the FRR and FAR values compared to the existing algorithms.

2.4 Online Signature Verification: A Review

To identify and verify identity, we only try to use human signatures signed by people, which is a secure way to identify people, especially in areas related to banking and other financial and legal transactions, but some techniques are used with loopholes and abuses; The purpose of these people is to commit fraud. That's why technology is evolving rapidly, not only to keep up with the next trends, but also to stay one step ahead of scammers. Technology exists to facilitate the work of humans so that transactions can be done online or offline as per the convenience. What we are talking about here is a biometric technology that can be used as a means of confirming an individual's identity. It consists of two types: - (1) physical (2) behavioral [4].

In physical biometrics, a person's iris and fingerprints can be used to identify and confirm a person's identity. In behavioral biometrics, it can be thought of as a signature or a voice. We're talking about signatures here. Signatures are a widely accepted method of verifying a person's identity. It is used for checks, legal transactions and title documents. Signature verification can be done in two ways:- Online and offline signature verification. Online signature verification: In this system, real-time dynamic features such as pen pressure, paper contact, time to complete signature, number of stops, and maximum contact pressure are considered of the pencil Offline Verification System: In this system, no hardware like pen is required and it relies on the static properties of the signature image. The online signature verification process consists of 7 steps:

1. Acquisition 2. Preprocessing 3. Feature Extraction 4. Training 5. Comparison 6. Matching 7. Verify the signature

2.5 Writer-Independent Online Signature Verification Based On 2-D Representation of Time Series Data Using Triplet Supervised Network

The use of Online Signature Verification (OSV) is critical to achieving a paperless office, but it still faces significant challenges. To solve this problem, this paper proposes a new OSV framework for the freelance writer (WI). The framework consists of three parts: (1) a two-dimensional rendering method that converts time-series signature data into linear images with mixed static and dynamic information. (2) A per-channel weight learning (CWL) mechanism built into the feature extractor to detect possible relationships between three dynamic attributes (elevation, azimuth, and pressure). (3) Three-way supervised network (TSN) consisting of three streams of weighted convolutional neural network (CNN) to calculate the distance [anchor, positive, test]. The experimental results showed that the proposed model outperforms the classical CNN and the lightweight model by no less than 1.29% and 11.3% in eligible forged signatures, respectively. Also, TSN patterns are more effective than previous OSV algorithms in detecting WI patterns. This proposes a new framework for author method-independent online signature validation. The framework consists of three core components: a two-dimensional representation of time series data, channel weight learning (CWL), and a construction of three supervisory networks. The time series data collected from the Wacom tablet is converted into image data of a certain size (499 * 227), showing the features of the spatial trajectory and preserving the main dynamic information.[5].

2.6 Signature Verification System using Different Algorithms

The proposed system uses the Harris algorithm, the Surf algorithm, and pixel-based methods to efficiently verify signatures. This paper emphasizes the need for collections of signatures rather than signatures for verification, the basic reason being that a single signature cannot show all the factors of its

signature that may vary under different circumstances. It is claimed that with these algorithms we can find small details for efficient verification of signatures compared to manual examination [6].

According to the proposed system, we will first apply the Harris algorithm, which will detect the signature angles. The basic working principle of the Harris algorithm is to compare two images or two signatures and find a good patch, that is, a corner point, which is very characteristic. If there is a match, the process continues, otherwise the signature is rejected. In the second step of the process, the navigation algorithm is applied. Although the navigation algorithm works very similarly to the Harris algorithm, it can find several other features that the former missed. This way, we can specify the index point to compare with the sample signature, and if it matches, the system will proceed to the next step. Then use a pixel-based approach. This step helps us find the black and white pixel density. The calculated strength is compared to the sample signature as a final signature verification procedure.

2.7 Signature Verification System using Neural Networks

This proposes to use a neural network as a classifier for signature validation based on the extracted dynamic features, i.e. signature x and y coordinates and velocity components. Then, the extracted features are considered and a feature feedback network is formed for classification [7].

Three types of forgery have been mentioned regarding signature forgery. Accidental infringement, unqualified infringement and qualified infringement. Accidental forgery is when the signature forger does not know the victim's signature but intends to forge the victim's signature. Unconditional forgery is a form of forgery in which the intruder knows the victim's signature but cannot copy it exactly. Skilled forgery is when the forger is fully aware of the victim's signature and is skilled enough to transcribe it. The paper suggests that we should have a system that protects against any spoofing described above. Using a neural network to verify signatures is beneficial because it is very easy to use and capable of solving complex problems. Dynamic functions such as x-y coordinates, pressure, time, etc. is a function of time, so the paper highlights that not even a skilled forger can replicate all of these parameters. This makes these dynamic functions suitable for signature verification.

2.8 Learning The Micro Deformations by Max-Pooling for Offline Signature Verification

The term "micromorphing" refers to subtle changes in signature strokes or writing style that distinguish real signatures from professionally forged ones. The study shows that convolutional neural networks (CNNs) can identify these subtle distortions using a technique called max pooling, which involves tracking the coordinates of the highest values in a pooling window. By incorporating this location data as an additional feature of convolutional features, the proposed method achieves better performance than existing systems on four publicly available datasets in English, Persian, and Hindi. The results show that CNNs have the ability to accurately detect subtle distortions and improve signature verification systems [8].

The basic concept of this research is to preserve subtle changes in signatures that would normally be missed by standard use of maximum summation. These location coordinates are called displacement elements. While previous work introduced the idea of using localization or maximum offset functions for character recognition, this study shows that offline signature verification can be significantly improved. Indeed, subtle deformations are necessary for the signature verification task, and a compensation function is produced to represent these deformations. Extensive experiments and analysis on the GPDS synthetic offline signature database validate the effectiveness of the proposed system, which is superior to all other known offline signature verification systems. In addition, the method achieves the latest results on benchmark datasets in different languages, including English, Persian, and Hindi.

2.9 OSVFuseNet: Online Signature Verification by Feature Fusion and Depth-Wise Separable Convolution Based Deep Learning

Although online signature verification (OSV) techniques have been used in production systems for many years, significant challenges remain in training a model to accurately classify test signatures using only a limited number of training samples for test signatures. However, the development of convolutional neural networks (CNNs) has greatly improved the efficiency of OSV systems. Online Signature Verification consists of two main steps. The first step is to extract unique and useful features from signature data collected online. The second step is to develop a robust model or framework that can use the extracted features to determine the credibility of associated signatures. In the traditional feature extraction process, many dynamic local features, such as x and y coordinates, feature layout, azimuth, pressure, etc., are extracted when the user is connected to a specialized device. Record in each sample. This presents "OSV FuseNet", a framework based on separable deep convolutional neural networks for online signature validation. The framework uses both well-designed and deep learning-based features, and combines them through a feature-level fusion and feature classification process to remove their respective limitations by complementing each other. The use of depth-separable convolution operations significantly reduces the number of operations and parameters required by the framework [9].

2.10 SM-DTW: Stability Modulated Dynamic Time Warping for Signature Verification

It discusses a new idea called "stability" in signature verification, which explains why a signature may vary slightly each time it is signed. The most consistent parts of a signature across multiple executions are considered the most important for verifying its authenticity. To incorporate this idea into signature verification, a new algorithm called the Stability Modulated Dynamic Time Warping has been developed, which compares the most similar parts of two signatures to calculate the distance between them. This algorithm has been tested on two datasets commonly used to evaluate signature verification systems and has shown to improve the accuracy of the current system and performs comparably to other top-performing signature

verification systems. It explains how a signature is made up of small movements executed in a specific order to create a unique pattern, and the motor plan for the signature is independent of the body part used to sign. However, the specific execution may vary slightly due to factors such as visual and proprioceptive feedback, also highlights how different algorithms have been developed to exploit the concept of signature stability, including model-based, feature-based, and data-based approaches. This new approach differs from others in that it explicitly represents motor plans in terms of stability regions and uses this information to evaluate signature similarity. The main goal of the study is to provide experimental evidence to support the idea that multiple executions of a signature should produce very similar trajectories, as the signing habits of a subject are encoded in the motor plan that has been learned [10].

2.11 Discriminative Feature Selection for On-Line Signature Verification

This paper presents methods to select consistent and discriminative features to distinguish authentic from false signatures collected as real-time dynamic signals on collective devices. Based on the global experimental design and the optimized orthogonal experimental design, two methods were proposed to identify these characteristics among the candidates. The paper also analyzes feature consistency to improve robustness, selects more consistent features for discriminant feature selection, and modifies the signature of its reference model based on the Gaussian mixture model to reduce fluctuations caused by changes in the 'internal and external writing environment before validation, in order to improve the verification efficiency, it is proposed to improve the dynamic time warping with signature curve constraints. Experiments are conducted with MCYT open access database and SVC200 Task2, and the results verify the effectiveness and robustness of the proposed method. The article highlights the importance of pre-processing signatures before verification to reduce the effects of distortion or fluctuations during capture and rendering. When using pattern matching techniques, DTW is usually used to match signatures, but as the number of signature sampling points increases, this leads to a large amount of computation and a decrease in the efficiency of the system In summary, this paper provides methods to identify consistent and discriminative features, align signatures with their reference patterns, and increase verification efficiency to distinguish authentic signatures from forged signatures collected as real-time dynamic signals on crowdsourced devices [11].

3. Conclusion

With the rapid development of technology, the old rules are becoming obsolete. As a result, new technologies are being developed to fight fraud and crime, and tools are updated as people discover vulnerabilities. Signature verification and forgery detection systems have been developed to deal with forged and rewritten signatures to provide clear and accurate disclosure of a person's identity and prevent any type of identity crime. By reviewing several literature survey articles, we come to the conclusion that the Harris algorithm has been proven to be more perfect and more accurate in its operation. In the future, we plan to use the Harris algorithm as one of the core algorithms to lay the foundation for our project.

REFERENCES

[1]. SounakDeya, AnjanDuttaa, J. Ignacio Toledoa, Suman K.Ghosha, JosepLlados´a , Umapada Pal ”SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification” Issue 30, September,2017.

[2]. Julita A., Fauziyah S., Azlina O., Mardiana B., Hazura H., ZahariahA.M.”Online Signature Verification System” Issued April 2009.

[3]. Shashi Kumar D R, K B Raja, R. K Chhotaray , Sabyasachi Pattanaik ”Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks” Vol. 2(12), 2010.

[4]. Poonam Chaudhary and Vijay Kumar Singh,” Online Signature Verification: A Review”, Volume-3, Issue-2, Feb 2016.

[5]. LiyangXie, Zhongcheng Wu, Xian Zhang, Yong Li, Xinkuang Wang “Writer-Independent Online Signature Verification based on 2-D Representation of Time Series Data using Triplet Supervised Network” June 2022.

[6]. S. Priya, A.K.R.N.Supreeth, K. Somesh, A. Hruday Kumar ” Signature Verification System using Different Algorithms”, Volume-8, Issue-6S3, April 2019.

[7]. Tushara D, ShrideviRaddy, Shreya KM, Spoorthy Y,” Signature Verification System using Neural Networks”, NCCDS - 2021 Conference Proceedings.

[8]. Yuchen Zheng, Brian Kenji Iwana, Muhammad Imran Malik, Sheraz Ahmed, WataruOhyama, Seiichi Uchida “Learning the Micro-Deformation by Max-Pooling for Offline Signature Verification” October 2021.

[9]. Chandra Sekhar Vorungunti, Viswanath Pulabaigari, Rama Krishna Sai Subrahmanyam, Gorthi, Prerana Mukherjee “OSVFuseNet: Online Signature Verification by Feature Fusion and Depth-Wise Separable Convolution Based Deep Learning” October 2020.

[10]. Antonio Parziale, Moises Diaz, Miguel A. Ferrer, Angelo Marcelli “SM-DTW: Stability Modulated Dynamic Time Warping for Signature Verification” April 2019.

[11]. Xia Xingua, Song Xiaoyu, Luan Fangun, Zheng Jungang, Chen Zhili, Ma Xiaofu “Discriminative Feature Selection for Online Signature Verification” February 2018.