IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12365

SIGNATURE VERIFICATION SYSTEM

Aarohi[1], Dr. A. Rengarajan[2]

Masters Student, School of CS&IT, Jain (Deemed-To-Be University), Bengaluru[1]

Associate Professor, School of CS&IT, Jain (Deemed-To-Be University), Bengaluru[2]

Abstract: Handwritten signature identification and verification has grown to be an active region of research in latest years. Handwritten signature identification systems are used for identifying the person amongst all customers enrolled within the gadget even as handwritten signature verification systems are used for authenticating a consumer via evaluating a specific signature with his signature that is stored in the gadget. This paper affords an evaluation for commonly used methods for pre-processing, function extraction and classification techniques in signature identity and verification structures, similarly to an assessment between the structures implemente in the literature for identification strategies and verification strategies in on line and offline systems with taking into consideration the datasets used and outcomes for every system.

Keywords: Handwritten signature, verified signature

I. INTRODUCTION

A signature is an identifying mark written by a person on a document or text. Signatures are the primary authentication and authorization mechanism. Signature verification can be done online or offline. This signature verification is natural and intuitive. In offline methods, the signature is usually handwritten and the verification process uses features extracted from scanned images of the handwritten signature.

Online method signing is performed using a digital pen, then the signing data is stored in a database and used later in the verification process. Some forging detection characteristics are taken into account, such as x-y coordinates, pressure, time. These dynamic characteristics are a function of time, whereas the static characteristics are independent of time. Even a skilled forger cannot forge the same print as the user. Therefore, these dynamic features help detect counterfeiting.

Since the signature varies from person to person and person to person, it is a very powerful biometric to authenticate a user. Signature verification is a very difficult pattern recognition problem. Due to intraclass variations, it is difficult even for experts to identify forged signatures. Tampering related to signature detection is classified into three types, which are: 1) random tampering 2) unqualified tampering 3) qualified tampering. Random forgery is a type where the person who wants to forge a signature only knows the name of the person they are going to forge, but not the signatures of those people. An unqualified forgery is one in which the person who wants to copy the real signature knows how the real signature was signed, but cannot reproduce it exactly. A qualified forgery is a type in which the person copying the signature knows very well how and the different variations of the genuine signature and the copy closely match the signature.

II. LITRETURE REVIEW

1. Online signature recognition using neural networks: User authentication is becoming important for conducting business transactions, accessing data and for security purposes. Automated signature authentication is now gaining popularity in research due to its adoption in legal and social fields and widespread use for authentication purposes. The main objective of this work is to build a signature recognition system using certain eigenvalues so that labels with maximum accuracy can be obtained. For this, some features have been extracted and modeled. These features serve as input models to the neural network and construct corresponding targets.; Babita P

2. Dz Offline signature recognition using Global features, per. Ms. Archana Patil, Ms. Pallavi Patil, presented the most popular method of biometrics in the field of personal verification. Among these global characteristics, the main characteristics such as area, height and width are extracted. A Euclidean distance model is used to simultaneously find a match between the test signature and the signature stored in the database. The algorithm gave a satisfactory result of 89% of the identified by the method proposed in this article.

3. Pansare et al. presents a method that consists of an image processing, extraction of geometric elements, neural network training with extracted features and validation. Check phase involves using the extracted features of the test signature to a trained neural network that was used to classify it as a real or fake.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12365

4.Online signature verification using deep representation: Authentication is known as an integral part of social life. In recent years, there has been a growing interest in personal identity verification. Increasing security requirements have placed biometrics at the center of attention for so many. Biometric technology has become an important area in the authentication of persons and has been used in the identification and authentication of persons. The term biometric refers to individual recognition based on a person's distinguishing characteristics.; Mohammad Hajizadeh Saffar, Mohsen Fayyaz, Mohammad Sabokrou, Mahmood Fathy:

5.proposed a new approach to confirm on-line signature verification with aid vector machines based totally on LCSS kernel feature; Christian Gruber, Thiemo Gruber, Sebastian Krinninger

6. The similarities of the 2-time collection are determined through the period of an LCSS the usage of a kernel function. This new method shown that the SVM LCSS, can authenticate people very reliably if simplest six genuine signatures are used for education. It became out that the LCSS-based totally similarity assessment of on-line signature records is even superior to DTW-based techniques; Sebastian Krinninger

7.A technique in which type of forgery and authentic signature is executed by means of binary class first by means of simple engineered functions, then through gadget mastering techniques as logistic regression, MLP and sooner or later by a deep mastering approach with a convolutional neural community. The deep studying technique on the signature verification trouble confirmed promising effects but there is nevertheless need for improvement; Beatrice drott and Thomas Hassan-Reza

8.New proposed a new version primarily based technique, GMM into the DTW framework to affirm the net signatures; Abhishek Sharma and Suresh Sundaram

9.New supplied a online handwritten signature verification gadget based on discrete wavelet transforms (DWT) features extraction and feed forward lower back errors neural community type; Dr.Maged M.M.Fahmy

III. PROBLEM STATEMENT

Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number and order of the strokes, In an online signature verification system , the users are first enrolled by providing signature samples (reference signatures). When a user presents a signature (test signature) claiming to be an individual, this test signature is compared with the reference signatures for that individual. If the dissimilarity is above a certain threshold, the user is rejected. During verification, the test signature is compared to all the signatures in the reference set, resulting in several distance values. One must choose a method to combine these distance values into a single value representing the dissimilarity of the test signature to the reference set, and compare it to a threshold to decide.

IV. PROPOSED METHODOLOGIES

Our signature verification system consists of two main components: signature extraction and signature verification. In the signature extraction phase, we use a pre-trained CNN to extract features from the signature image. Specifically, we use the VGG16 network, which is a widely used CNN for image recognition tasks. We remove the last few layers of the mesh and add a fully connected layer that produces a 128-dimensional feature vector. The extracted features are then normalized to have zero mean and unit variance.

In the signature verification phase, we use the extracted features to train a support vector machine (SVM) classifier. We train the SVM on a dataset of genuine and forged signatures. The dataset consists of 1200 genuine signatures and 1200 forged signatures, each signature being a 300x150 grayscale image.

❖ BENEFITS: -

There are many benefits to using Signature verification system, including an automatic signature verification system is more efficient than manual verification. It can process a large number of signatures in less time, reducing the workload for human experts and improving overall efficiency. Traditional signature verification methods rely on subjective judgment by human experts. In contrast, our proposed system will use objective criteria to verify the authenticity of signatures, thereby eliminating the risk of human error or bias. signature verification system can be adapted to different signature styles and types, making it suitable for use in various fields such as banking, law enforcement, and forensics.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12365

This system will be resistant to changes in signature style, size and quality, making it suitable for use with signatures captured using various devices such as scanners or smartphones.

V. OBJECTIVES

The objective of a signature verification system is to determine whether a signature is genuine or forged. This is typically done by comparing a signature in question to a previously authenticated signature from the same individual. The system uses image processing techniques and machine learning algorithms in Python to analyze the features of the signature and make a determination of authenticity. The ultimate goal is to be able to accurately identify forged signatures, while minimizing the number of false rejections (genuine signatures that are incorrectly identified as forged).

VI. EXPECTED OUTCOMES

Our proposed signature verification system is expected to achieve high accuracy in verifying the authenticity of signatures. Using deep learning techniques and a large dataset of genuine and forged signatures, our system will be able to detect even subtle differences between genuine and forged signatures. Automated signature verification systems can process a large number of signatures in less time than human experts. Our proposed system will be able to rapidly process signature images, making it suitable for use in various fields such as banking and law enforcement. By accurately verifying the authenticity of signatures, our proposed system will improve security and prevent fraudulent activities such as identity theft and forgery.

VII. SYSTEM ANALYSIS

Signature verification system ensures various features such as accuracy, efficiency, robustness, usability, security, scalability, maintenance which are important requirements in a modern system.

FEW Applications:

- Finance and banking
- Government organizations
- Retail sector
- Online transactions
- Air travel
- Insurance and compliance documents
- Other legal documents

VIII. CONCLUSION

Signatures are very essential for the authentication of a character in banks or workplaces and many others. Numerous automated structures are getting into picture for the verification of the signatures. technology is improving day-by day in the subject of authentication because the forgery cases are also been enjoy loads. Offline signature verification is less complex in comparison to on-line signature verification. Solid dynamic traits are recognized with the help of SVM classifier. diverse steps are studied in verification of signature. Evaluation on FRR and far can also be finished for their performance to get better results.

Signature is used in all monetary transactions for authorization of identification of human but nonetheless that authentication device is based totally on with the aid of evaluating the signature with authorized signature manually. So a system is needed that's primarily based on the computer based totally type. on this paper an internet signature verification device is proposed that is based totally on neural network-based class.

REFERENCES

[1] https://www.hindawi.com/journals/mpe/2022/4641559/
[2] https://github.com/vijaywargiya/ipmanagement-blockchain
[3] https://scholar.google.com/
[4] R. G. Brown, J. Carlyle, I. Grigg, and H. Mike, Corda: An Introduction, Wiley-blackwell, Hoboken, NJ, USA, 2016.
[5] C. Gruber, T. Gruber, and B. Sick, Online Signature Verification with New Time Series Kernels for Support Vector Machines. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 500–508.
[6] B. Drott and T. Hassan-Reza, "On-line handwritten signature verification using machine learning techniques with a

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12365

deep learning approach," 2015, student Paper.
[7] M. M. Fahmy, "Online handwritten signature verification system based on dwt features extraction and neural network classification," Ain Shams Engineering Journal, vol. 1, no. 1, pp. 59 – 70, 2010.
[8] Gupta, H., Bansal, M., & Bansal, A. (2018). A Survey of Deep Learning Techniques for Image Segmentation and Object Detection. arrive preprint arXiv:1806.09986.
[9] Pansare, A., & Bhatia, S. (2013). Handwritten Signature Verification using Neural Network. International Journal of Advanced Research in Computer and Communication Engineering, 2(8), 3254-3259
[10] Offline signature recognition using Global features Authors: Archana Patil and Pallavi Patil Source: Presented in International Conference on Computing, Communication and Automation (ICCCA2015)