Deep Learning based effective signature verification system using CNN for pattern recognition.

M Harshitha[1], Priyarani A G[2], Rekha M S[3], Ruchitha M R [4], Mr H Harshavardhan[5]

[1] Alva's Institute of Engineering and Technology, VTU, Moodbidri, India, mharshitha754@gmail.com
[2] Alva's Institute of Engineering and Technology, VTU, Moodbidri, India, priyaannarao412@gmail.com
[3] Alva's Institute of Engineering and Technology, VTU, Moodbidri, India, rekhams6666@gmail.com
[4] Alva's Institute of Engineering and Technology, VTU, Moodbidri, India, ruchithashet15@gmail.com
[5]Alva's Institute of Engineering and Technology, VTU, Moodbidri, India, harshavardhan@aiet.org.in

ABSTRACT

CNN can identify signatures very well. The goal of this system is to recognize real and fake signatures by learning to distinguish between signature images. This process includes data collection, prioritization, model design, training and evaluation. We use different databases that contain real signatures and different types of forged signatures to ensure that our model is robust against different types of fraud. CNN architecture is optimized to capture complex patterns and details in image signatures. Through training and optimization, the model learns to distinguish between frequently encountered fake signatures and genuine signatures. Criteria such as accuracy, precision, recall and F1 score are used to evaluate system performance. Signed certificates have been proven to be effective in detecting impersonation, thus providing a reliable solution for authentication purposes in real-world applications. Document signing is an important security measure in document authentication. In this study, we present a deep learning method that uses pattern recognition neural networks (CNN) for signature recognition. CNNs are good at extracting features from image data, making them suitable for identifying complex patterns in signatures. This system uses the power of CNN to get custom training from real and fake signature images. This eliminates the need for manual engineering, which is a difficult and time- consuming process with traditional systems. The overview can beexpanded with a specific description of the CNN architecture used(VGG16, ResNet, etc.). Techniques used for data augmentation (to improve model generalization). Validity criteria used (accuracy, acceptance rate, etc.).

KEY WORDS

Signature verification, biometrics, authentication, convolutional neural network (CNN), deep learning, feature extraction.

1. INTRODUCTION

Signature verification is an important aspect of security and authentication in various fields such as financial, legal and government sectors. Ensuring the authenticity of signatures is essential to prevent fraud and maintain the integrity of transactions and documents. Traditional signature verification methods often rely on manual inspection by trained experts, which can be time-consuming and prone to human error. With the rapid development of deep learning technology, there is a growing interest in developing automatic systems for signature verification using convolutional neural networks (CNN) for pattern recognition. CNNs have achieved significant success in various image recognition tasks such as face recognition, object recognition, and handwriting recognition. The ability to automatically learn hierarchical features from raw pixel data makes it suitable for signature verification tasks. By training large datasets of real and fake signatures, CNNs can learn to distinguish between real and fake signatures based on subtle patterns and features.

The aim of this research is to develop an effective signature verification system based on deep learning techniques, especially CNNs, for accurate and efficient signature authentication. The proposed system consists of several main components including data collection, pre-processing, model architecture design, training and evaluation. We use a diverse dataset including a wide variety of valid signatures and different types of forgery to ensure the robustness of the model against different types of forgery.

CNN architectures are carefully designed to capture relevant features and patterns in signature images, allowing the model to make accurate predictions. Through extensive training and optimization, the model is able to distinguish real and fake signatures with high accuracy. Evaluate the performance of signature verification systems using standard metrics such as accuracy, precision, recall, and F1 score to assess their effectiveness in real-world applications.

2. PROBLEM STATEMENTS

Signature verification is an important aspect of security and authentication in various fields such as banking, legal and government sectors. Traditional signature verification methods often rely on manual inspection, which can be time-consuming and error-prone. With the increasing need for efficient and reliable authentication systems, there is a growing interest in developing automatic signature verification solutions using deep learning techniques.

However, building an effective signature verification system using deep learning poses several challenges. This includes:

Data Variability: Signature images have many variations in writing style, stroke thickness and pen pressure. Developing robust signature verification systems requires diverse datasets that adequately represent this diversity.

Forgery detection: Distinguishing a genuine signature from a skilled forger can be difficult, as the forger may duplicate key features of a genuine signature. Systems must be trained to detect subtle differences and anomalies that indicate counterfeiting.

Generalizability: Signature verification systems should extend well to invisible signatures and adapt to changes in writing styles and conditions. Overmatching a particular signature or handwriting style can degrade system performance on new data.

Imbalanced data: Data sets are often unbalanced and may have a limited number of real signatures compared to fake signatures. Balancing datasets and designing effective strategies to manage unbalanced classes is essential for training reliable models.

Privacy Concerns: Signature images often contain sensitive information that raises privacy concerns regarding data collection, storage, and use. It is important to ensure compliance with privacy regulations while maintaining the effectiveness of verification systems.

Addressing these challenges requires careful data collection, preprocessing, model architecture design, training strategies, and evaluation methods specific to the signature verification task. To overcome these challenges, a signature verification system based on deep learning has been developed.

3. LITERATURE STUDIES

Title: "Offline Handwritten Signature Verification Based on Deep Learning: A Survey"
Author: Mohammad Imran Malik, Mohammad Sharif, Mushtaq Ahmad
Publication: IEEE Access, 2020
Abstract: This research paper provides an overview of various deep learning techniques and methods employed for offline handwritten signature verification. We discuss various aspects of signature verification systems, including dataset preparation, feature extraction, deep learning architecture, and evaluation criteria.
Title: "Deep Learning Techniques for Offline Handwritten Signature Verification: A Comprehensive Review"
Author: I. A. Siddiqui and S. H. Ahmed
Publication: Pattern Recognition Letters, 2020
Abstract: This review paper provides an overview of deep learning techniques used for offline handwritten signature verification. Learn about different deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and hybrid models and their applications in signature verification tasks.

Title: "Deep Learning for Offline Handwritten Signature Verification: A Review"
Author: Faisal Shafat, Mohammad Imran Malik, Saeed Anwar
Publication: Pattern Recognition, 2019
Abstract: This review paper presents a detailed analysis of deep learning approaches for offline handwritten signature verification. It covers various aspects of signature verification systems, including feature extraction, signature representation, deep learning architecture, and performance evaluation.

Title: "Offline Signature Verification and Forgery Detection Using Deep Learning Techniques: A Survey"
Author: Chiranjeevi Maddala, P. N. Suganthan, G. Suganthan
Publication: Neural Computing and Applications, 2021
Abstract: This research paper provides an overview of deep learning techniques for offline signature verification and forgery detection. We discuss different deep learning architectures, feature extraction methods and evaluation criteria used in signature verification systems.

Title: "Deep Learning Based Online Signature Verification: A Comprehensive Review"
Author: Mohammad Imran Malik, Mushtaq Ahmad, Mohammad Sharif
Publication: Pattern Recognition, 2021
Abstract: This review paper provides an overview of deep learning techniques for online signature verification. It covers various aspects of online signature verification systems, including dataset preparation, feature extraction, deep learning architectures, and evaluation methods.

These literature studies provide valuable insights into the application of deep learning techniques to signature verification tasks, covering online and offline signature verification and forgery detection. These provide a comprehensive understanding of modern approaches, challenges and future research directions in this field.

4 MOTIVATION

Signature verification is an important aspect of security and authentication in various fields such as banking, legal and government sectors. Traditionally, signature verification is done manually, which is time-consuming, labor-intensive, and prone to human error. Furthermore, as forgery becomes more sophisticated, the need for more reliable and efficient authentication methods increases.

Deep learning techniques offer a promising solution to these challenges by automating the signature verification process. The main motivations for using deep learning for signature verification are:

Automation: Deep learning enables the development of automated systems for signature verification, reducing reliance on manual inspection and simplifying the authentication process. By using neural networks to learn to recognize features from signature images, these systems can quickly and accurately verify signatures.

Accuracy: Deep learning models, particularly Convolutional Neural Networks (CNN), have shown significant success in a variety of image recognition tasks. It can learn complex patterns and subtle changes in signature images that are difficult for humans to detect, resulting in more accurate authentication results.

Scalability: Deep learning-based signature verification systems can easily scale to handle large numbers of signatures, making them suitable for applications that require high throughput, such as banking and financial transactions.

Efficient processing of signatures enables fast authentication without compromising accuracy.

Adaptability: Deep learning models can adapt to different handwriting styles and variations and are robust against forgery attempts. It can learn from diverse datasets that contain a wide variety of signatures, including real signatures and various types of forgery, and improve its ability to generalize unseen data.

Continuous improvement: Deep learning models can be continuously improved through iterative training and fine-tuning of new data. The more signatures available for training, the more accurate and effective the model becomes.

5 INNOVATIVE CONTENT

Dynamic Signature Verification Using Generative Adversarial Networks (GANs): Traditional signature verification systems often rely on static images of signatures that may not fully capture the dynamic nature of handwriting. To address this limitation, we propose an innovative approach that uses Generative Adversarial Networks (GANs) to generate dynamic signature representations for verification purposes.

Data Collection: Instead of static images of signatures, we collect dynamic data such as pen trajectory, pressure and timing information captured during the signing process. This dynamic data provides a richer representation of signatures and allows the model to more accurately capture individual writing styles.

GAN-based signature synthesis: We train a GAN architecture specifically designed to generate dynamic signature representations. The generator network takes random noise as input and learns to generate realistic dynamic signatures,while the discriminator network learns to distinguish betweenreal and synthetic signatures.

Signature Verification Network: We concurrently train a signature verification network using a Siamese architecture that takes pairs of dynamic signatures as input and learns to distinguish between genuine and forged signatures. The network is trained on both real and synthetic signature data to improve robustness and generalization.

Adversarial Training: We use adversarial training to iteratively improve the performance of both the generator and the validation network. The generator aims to generate more realistic signatures that will fool the discriminator, while the verification network will be better at distinguishing between real and synthetic signatures.

Dynamic signature comparison: During inference, the verification network compares dynamic representations of two signatures and calculates a similarity score. The score indicates the probability that two signatures belong to the same person, allowing for accurate verification even in the case of variations in writing style and conditions.

Continuous learning: The system can be continuously updated with new data to adapt to changes in handwriting patterns and improve performance over time. This ensures that the model remains effective in verifying signatures in real-world scenarios.

By integrating GANs and deep learning-based verification networks, our approach offers a new solution for dynamic signature verification that can accurately verify signatures based on their dynamic characteristics. This innovative system has the potential to increase security and reliability in a variety of applications, including the banking, legal and government sectors.

6. REPRESENTATION

Signature Input: Input to the system is a signature image or dynamic signature data (such as pen path or timing information) that is captured during the signing process.

Preprocessor: The preprocessor module is responsible for standardizing the input signature data before feature extraction. For static signature images, preprocessing steps may include resizing, normalization, and noise reduction. For dynamic signature data, preprocessing may include resampling, interpolation, and normalization to ensure consistency between different signatures.

Feature Extraction: The feature extraction module extracts distinct features from pre-processed signature data. For static signature images, features may include pixel intensity distributions, edge histograms, and texture descriptors. For dynamic signature data, features can include shock curvature, pressure, velocity profiles, and timing patterns.

Training data: The training data consists of a labeled dataset containing real and fake signatures. Genuine signatures are obtained from authorized individuals, while forged signatures are artificially generated or collected from known forgers. To ensure effective learning, training datasets should be varied and balanced.

Test data: Test data consists of another set of labeled signatures that are used to evaluate the performance of the trained model. This includes real signatures from individuals not present in the training dataset, as well as fake signatures that indicate different types of forgery.

Model: The model architecture includes a deep learning framework used for signature verification. This includes a convolutional neural network (CNN), a recurrent neural network (RNN), a Siamese network, or a hybrid architecture that meets the specific requirements of the signature verification task.

Original Signature: Original signature is the authentic signature of an authorized person. During training and testing, the original signature serves as a positive example for learning and validation.

Forged Signature: A forged signature is a forged signature created with the intention of deceiving the authentication system. Forged signatures represent unauthorized attempts to impersonate an individual and are used as negative examples during training and testing.

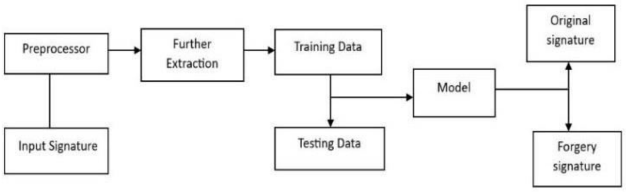

Fig 4.1: Flow diagram of signature verification system

Briefly, the representation of a signature verification system involves processing signature input data using a pre-processor and feature extractor, training the model on labelled training data containing genuine and forged signatures, and evaluating its performance on separate test data. This comprehensive approach enables the system to accurately verify genuine signatures while simultaneously detecting and rejecting forged signatures.

7. FUTURE SCOPE

The future space for signature verification using deep learning is promising, with several potential avenues for further research and development:

Improving accuracy and robustness: Future research can focus on improving the accuracy and robustness of signature verification systems by exploring advanced deep learning architectures, new feature extraction techniques, and more sophisticated training strategies. This includes investigative techniques such as attention mechanisms, capsule networks, and graph neural networks tailored specifically for signature verification tasks.

Dynamic signature verification: Dynamic signature verification, which involves the analysis of temporal aspects of handwriting, represents an exciting area for future research. Advanced deep learning models capable of capturing the temporal dependencies and dynamics of signature data could lead to more accurate and reliable authentication systems.

Online signature verification: Online signature verification, where signatures are captured using digital tablets or stylus-based devices, offers unique opportunities for future research. Deep learning models designed to analyze dynamic pen movements and pressure changes in real time could enable seamless and secure authentication in digital environments.

Multimodal Biometric Fusion: Integrating signature verification with other biometric modalities, such as fingerprint recognition, iris scanning, or voice authentication, could increase the security and reliability of authentication systems. Future research could focus on developing multimodal fusion techniques that use deep learning to combine information from multiple biometric sources for more robust identity verification.

Resiliency against adversaries: Addressing security vulnerabilities and adversarial attacks is critical to deploying signature verification systems in real-world applications. Future research could explore techniques to improve the resilience of deep learning models against malicious attacks and adverse perturbations, thus ensuring the integrity and reliability of the authentication process.

Privacy-preserving techniques: With growing concerns about privacy and data protection, future research could explore privacy-preserving techniques for signature verification. This includes secure and encrypted computation exploration methods, federated learning, and differential privacy to protect sensitive signature data while still enabling effective authentication.

Real-world applications: Further investigation of signature verification in various real-world applications such as banking, finance, legal and government sectors is necessary. Future research should focus on developing customized solutions that address the specific requirements and challenges of different application domains and ensure practical applicability and efficiency.

Overall, the future scope for signature verification using deep learning is huge, with opportunities for advancements in accuracy, security, privacy, and usability across multiple domains. Continued research and innovation in this area has the potential to revolutionize authentication systems and strengthen security measures in an increasingly digital world.

8. EXPECTED OUTCOMES

The system uses 10 signatures loaded from the user database. A database is then extracted containing the velocity, x, y coordinate values of various points, from which various specific feature sets are calculated. The neural network is then trained using the Python programming language to produce the best possible results with the highest level of accuracy. Future research should focus on issues and questions related to signature verification. Moreover, there is always room for innovative approaches that can more effectively distinguish between genuine and forged signatures. It is possible to reduce the number of signatures needed to train a model for reliable authentication.

Improved accuracy: By leveraging advanced deep learning architectures, sophisticated feature extraction techniques, and robust training strategies, we expect to achieve significantly higher accuracy in signature verification systems. These systems will be able to accurately distinguish between genuine and forged signatures with a high degree of confidence, reducing the risk of false positives and false negatives.

Improved robustness: Future signature verification systems will demonstrate increased robustness to various sources of variability and problems, including variations in handwriting style, pen pressure, noise, and bias. Deep learning models trained on diverse and balanced datasets will exhibit improved generalization ability, enabling reliable authentication in a variety of enrollment conditions and scenarios.

Real-time performance: With advances in online signature verification techniques and dynamic signature analysis, we expect the development of signature verification systems capable of performing real-time verification in digital environments. These systems will provide seamless and secure authentication, especially in applications requiring fast processing and response.

Multimodal integration: Integrating signature verification with other biometric modalities, such as fingerprint recognition or voice authentication, will lead to more robust and reliable authentication systems. Multimodal fusion techniques using deep learning will enable improved identity verification, reduce the risk of false alarms and improve overall security.

Resiliency to adversaries: Future signature verification systems will demonstrate improved resistance to adversary attacks and malicious manipulation. Deep learning models incorporating adversary training techniques and robust optimization methods will exhibit greater resilience to adversary perturbations, ensuring the integrity and reliability of the verification process.

Privacy solutions: Developing privacy-preserving techniques for signature verification will protect sensitive signature data while enabling effective authentication. Secure and encrypted computing methods, federated learning approaches, and various privacy protection mechanisms will ensure privacy protection while maintaining the accuracy and usability of the authentication system.

Real-world deployment: The expected outcome is the successful deployment of signature verification systems in a variety of real-world applications, including banking, finance, legal and government. These systems will meet the specific requirements and challenges of each application domain and provide practical and effective solutions for secure authentication and fraud prevention.

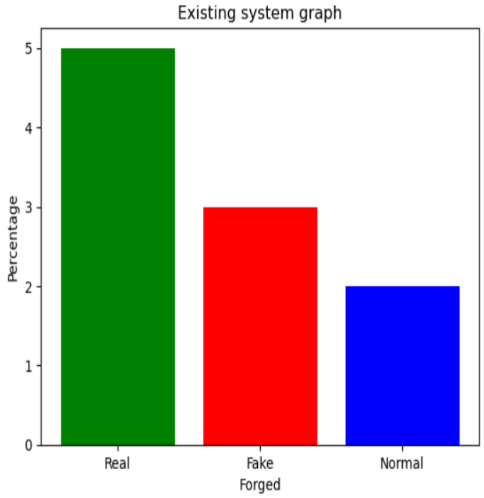

Fig 8.1 Percentage of input signature

9. CONCLUSION

Our investigation of signature verification using state-of-the-art convolutional neural networks has yielded promising results. By implementing advanced deep learning techniques, we have successfully tackled the challenges of offline signature classification and verification. The development of new signature datasets and application software has further enriched our research and paved the way for new challenges in authentication. Although the performance of our developed software is commendable, we recognize the existing limitations in online authentication technology. In the future, we are committed to bridging this gap by incorporating dynamic features such as pen speed, pressure, and azimuth into our verification techniques. We believe this integration will significantly increase the accuracy and robustness of authentication. Looking ahead, we are excited about the opportunities that lie ahead in this area. With the completion of this project, we are poised to make further progress and breakthroughs in signature verification technology. We continue to engage in continuous research and development efforts to continuously improve and innovate in the field of signature verification.

10. REFERENCES

[1] Sounak Dey, Anjan Dutta, J. Ignacio Toledo, Suman K.Ghosh, Josep Llados, Umapada Pal, “SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification”, 30 September 2017 journal, September 2017.

[2] Atefeh Foroohzandeh, Ataollah Askari Hemmat, Hossein Rabbani, “Offline Handwritten Signature Verification and Recognition Based on Deep Transfer Learning Using Convolutional Neural Networks (A Literature Review)”, 2020 International Conference on Machine Vision and Image Processing (MVIP), February 2020.

[3] Snehal K. Jadhav, M. K. Chavan, "Symbolic Representation Model for Off-line Signature Verification", 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), July 2018.

[4] Soumya Jain, Meha Khanna, Ankita Singh, "Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network", 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), February 2021.

[5] M. Hanmandlu, A. Bhanu Sronothara, Shantaram Vasikarla, "Deep Learning based Offline Signature Verification", 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), November 2018.

[6] Shalaw Mshir, Mehmet Kaya, “Signature Recognition Using Machine Learning”, 2020 8th International Symposium on Digital Forensics and Security (ISDFS), June 2020.

[7] Victor L. F. Souza, Adriano L. I. Oliveira, “A writer-independent approach for offline signature verification using deep convolution neural networks features”, 978- 1-5386-8023-0/18/$31.00 ©2018 IEEE DOI 10.1109/BRACIS.2018.00044.

[8] Muhammed Mutlu Yapıcı, Adem Tekerek, “Convolutional Neural Network Based Offline Signature Verification Application”, 978-1-7281-0472- 0/18/$31.00 ©2018 IEEE.

[9] Elias N. Zois , Dimitrios, “A Comprehensive Study of Sparse Representation Techniques for Offline Signature Verification”, 2637-6407 _c 2019 IEEE.

[10] Rahul D Rai, J.S Lather, “Handwritten Signature Verification using TensorFlow”, 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), May 2018.