ISSN No:-2456-2165

Signature Forgery Detection

Dr. Praveen Kumar K V
Professor
Sapthagiri College of Engineering

Pramit Kumar Mandal
[1SG20CS079]

Rishav Anand
[1SG20CS086]

Sakshee Singh
[1SG20CS092]

Tsewang Choskit
[1SG20CS106]

Abstract:- The usage of advanced signature verification technologies is required because of the growing dependence on digital transactions and authentication technology. This survey looks at the current state of dynamic signature representation techniques, with a focus on learning without forgeries. The efficacy of enhancing the security of signature-based authentication systems through the combination of 1D CNNs and the novel signature embedding approach Synsig2Vec is assessed.

The survey's first section addresses the dangers of forgery attacks and the weaknesses of employing traditional signature verification methods. It then explores the state- of-the-art Synsig2Vec methodology, which provides a more thorough representation by capturing the dynamic characteristics of signatures. By adding 1D CNN, the feature extraction procedure is further enhanced and the model's accuracy in differentiating real signatures from fakes is increased.

Keywords:- *Signature Verification, Forgery Detection, Synsig2Vec, 1D CNN, Dynamic Signature Representation, Authentication Systems.*

I. INTRODUCTION

In a time when online purchases are nearly ubiquitous, the security of dynamic signature authentication has become a serious issue. Expertly forged signatures are often impossible to identify from genuine ones using conventional procedures. This survey explores a novel approach to this problem, namely the combination of 1D CNN with the dynamic signature embedding technique Synsig2Vec, to boost the counterfeiting resistance of signature verification systems.

The subject of signature authentication is rapidly evolving, and novel approaches are useful for overcoming the weaknesses of the current methods. By capturing the complex dynamics of signatures, Synsig2Vec presents a potential path and offers a richer representation for reliable authentication. The model's capacity to extract significant features from dynamic signature data is further strengthened by its synergy with 1D CNN. The reason for this short survey is to give a succinct summary of the current state-of-the-art in dynamic signature representation for forgery-free learning. We explore the possible advantages of integrating 1D CNN with Synsig2Vec to build more robust and secure signature verification systems. The methods used, comparisons, and wider ramifications of this integration will all be covered in detail in the parts that follow, providing insightful details regarding the state of dynamic signature authentication.

II. CLASSIFICATIONS

- *Deep Learning*

Machine learning is just a subset of deep learning. These networks allow the brain to "learn" from large quantity of data by mimicking the procedure and functions of the human brain. Even with just one layer, such a network can make intelligent assumptions; however, more hidden layers can assist refine and optimize the network for greater accuracy.

- *Convolutional Neural Network*

CNN is a type of deep learning model that is specifically designed for image classification. CNNs use convolution operations to extract features from images. Next, these features are put into use for the classification of images. CNNs have been shown to be verycrucial for image classification tasks, such as classifying objects in images, detecting faces, and recognizing handwritten digits

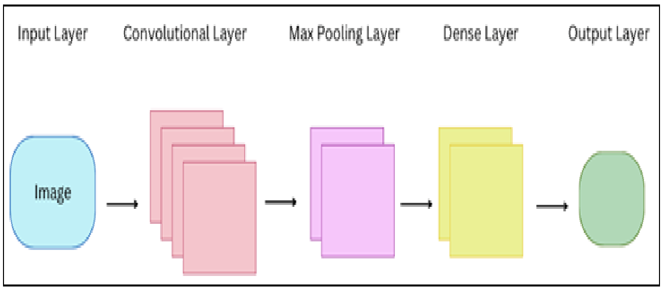

Fig 1: CNN Architecture

- ➢ *Recurrent Neural Network*

One kind of deep learning model created especially for problems involving natural language processing is the recurrent neural network (RNN). The sequential associations between words in a phrase can be taught to RNNs. Such a feature makes them suitable for applications like machine translation and text classification.

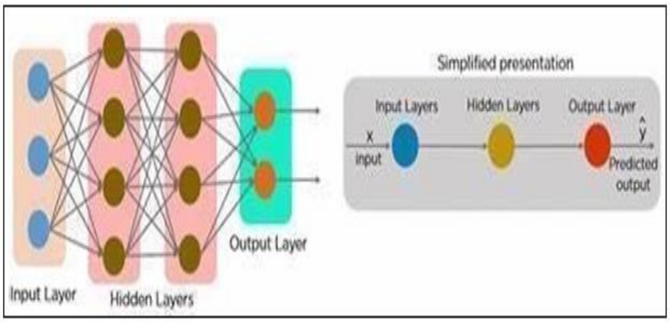

Fig 2: RNN Representation

- ➢ *Deep Belief Networks*

They consist of several layers of Restricted Boltzmann Machines (RBMs). Neural networks that can be used to represent a collection of data's probability distribution are called RBMs. Natural language processing and picture classification are just two examples of the classification jobs where DBNshave proven to be successful.

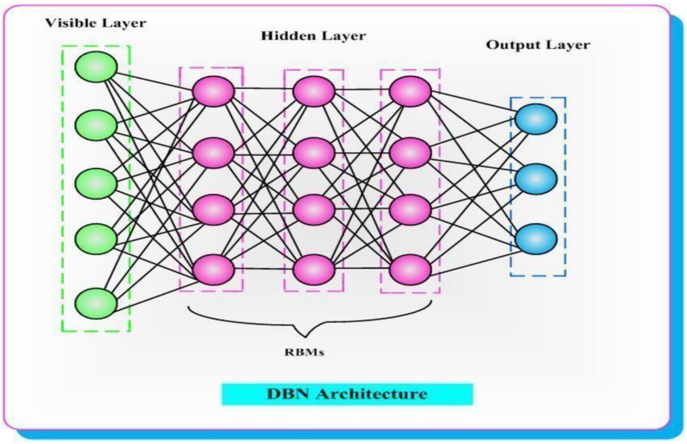

Fig 3: DBN Architecture

- ➢ *Long Short-Term Memory*

An RNN type called long short-term memory (LSTM) networks is made especially for applications requiring long-term memory. LSTMs are useful for applications like speech recognition and machine translation because they can be used to recall information from prior inputs.

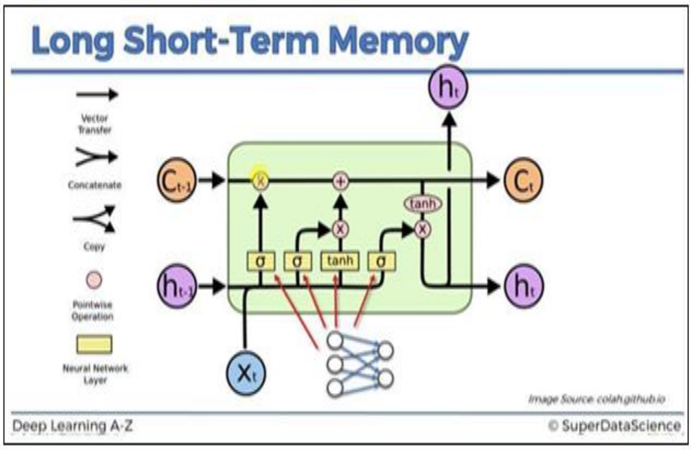

Fig 4: Long Short-Term Memory Model

- ➢ *Generative Adversarial Networks*

One kind of model that can be used on semi-supervised classification is the generative adversarial network, or GAN. Classifying data points when only a small portion of them have labels is known as semi-supervised classification. Synthetic data that resembles realdata can be produced with GANs. A classifier can then be trained using this artificial data.

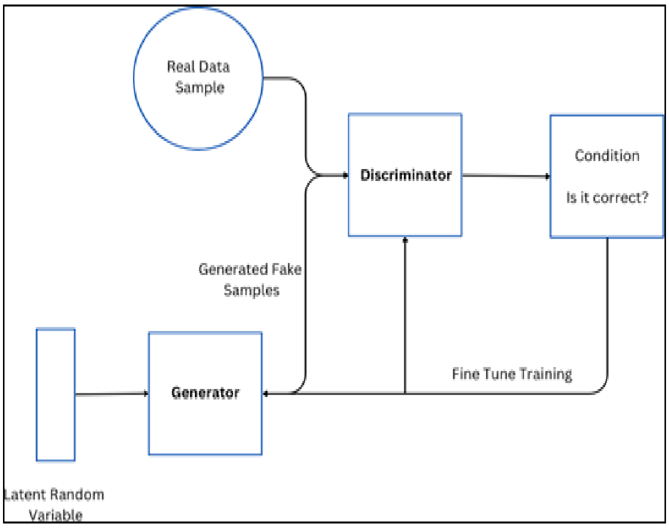

Fig 5: Generative Adversarial Network

III. RELATED WORK

For the difficulties of collecting big datasets, the usage of deep learning to dynamic signature verification has received little attention. The field's existing research can be loosely categorized into two groups. Local representations are learned by the first category (Lai and Jin 2019; Wuet al. 2019). It does this by applying dynamic time warping (DTW) to the learnt feature sequence while preserving the temporal information of the input. To do this, certain training methods, including a modified gated recurrent unit (Lai and Jin 2019) and signature prewarping (Wu et al. 2019), may be required. Fixed-length global representations are learned by the second category (Tolosana et al., 2018; Ahrabian and Babaali, 2018; Park, Kim, and Choi, 2019).

[Park et al.] extracted features from dynamic signature strokes using CNN and time interval embedding, and then aggregated over the strokes using recurrent neural networks. As statedin the introduction, to be able to improve performance while validating this kind of sample, the fore mentioned methods necessitate training with expert forgeries, which may not be feasible in many circumstances. Due to the recent synthesis technique, our approach merely requires real signatures and uses a lightweight CNN to learn global representations. Dynamic ASV systems are trained using ΣŸ-based synthetic signatures in two related experiments. (Diaz et al. 2018) created synthetic auxiliary template signatures to improve a number of Manhattan-based, DTW-based, and HMM-based non-deep learning systems. Their investigation did not validate the effectiveness of synthetic signatures in deep learning. (Ahrabian and Babaali 2018) used the Siamese network and recurrent autoencoder to train and test on completely fake signatures. It was not looked into if fake data could become accustomed to confirm signatures found in the actual world. Additionally, in contrast to these two studies, our approach—which is unprecedented in the domain of ASV—learns to rank the signals synthesized with varying degrees of distortion.

IV. LITERATURE SURVEY

K. Latha et al. [1]: In the current digital era, the extensive use of digital photographs has become essential in many sectors, including criminal investigation and clinical science, where image authenticity is vital. Detecting image forgery have been a challenging area of study, requiring significant time and effort. Recent advancements propose a hybrid approach involving deep learning (DL) and machine learning to enhance image forgery detection. This technique addresses issues like color manipulation by classifying photos as authentic or modified using a DL algorithm. The investigation of picture criminology was born outside of the rapid accessibility and manipulation of private photographs brought about by the widespread use of social media for image sharing. This is especially important for journalism since it highlights how crucial it is to confirm the legitimacy of photos that are used in the media.

Vincent Christlein et al. [2]: The paragraph discusses the significance of spotting copy-move forgeries in images in addition to the current research being done in blind image forensics to address this issue. The act of pasting and copying content inside of one image, usually with postprocessing in between, is recognized as copy-move forging. Finding the optimal postprocessing situations for copy- move forgery detection algorithms and processing stages is the aim of this research. The study evaluates 15 popular feature sets used in existing algorithms using a shared pipeline. Among the aspects that are the focus of the investigation are outlier detection, matching, filtering, and estimations of Affine transformations. Performance is assessed at the pixel and picture levels.

Ms. Manjula Subramaniam et al. [3]: The project aims to deal with the prevalent issue of signature forgery in important documents like bank cheques, passports, and driving licenses. The focus is on developing a system for detecting real or fake signatures using CNN and deep learning. This choice is motivated by the recognition that signatures evolve over time due to various behavioral changes, making it essential to have a mechanism that is capable of diverse training datasets to enhance detection accuracy. The project specifically targets offline signature forgery detection, where signatures are handwritten on documents and require image processing for analysis.

Daniel J. Inman et al. [4]: In the previous ten years, CNNs, have emerged as the industry standard for machine learning applications. Artificial Neural Networks (ANNs) that are feedforward and have alternating convolutional and subsampling layers are known as CNNs. Deep 2D CNNs, which have millions of parameters and numerous hidden layers, may learn intricate patterns and objects as long as they are trained on a sizable visual database with ground-truth labels. This special skill, when combined with the right training, makes them the main tool for a wide range of engineering applications using 2D signals, such pictures and video frames. However, this might not be a practical choice in many applications compared to 1D signals, particularly if data is limited or specialized to the application. To solve this problem, 1D CNNs were recently proposed, and in a number of applications—including early diagnosis and personalized biomedical data classification, structural health monitoring, finding and identifying anomalies in power 7 electronics, and electrical motor fault detection.

Songxuan Lai et al. [5]: Verifying handwritten signatures can be difficult since a forger can expertly mimic a writer's signature. In this research, we present a deep learning-based dynamic signature verification framework, SynSig2Vec, to counter the expert forgery attack without training with any skilled forgeries, since skilled forgeries are typically hard to acquire for training. In particular, SynSig2Vec is composed of a 1D CNN model named Sig2Vec for extracting signature representations and a revolutionary learning-by- synthesis technique for training. The learning-by-synthesis technique learns to rank these synthesised samples in a learnable representation space based on average precision optimisation after first using the Sigma Lognormal model to synthesise signatures with varying degrees of distortion for real template signatures.

Sandesh Kandel et al. [6]: The proposed system addresses the challenges associated with verifying handwritten signatures, a critical aspect in various sectors such as banks and organizations. Identifying real and fake signatures can be hard due to similarities, making a counterfeit detection system crucial. To improve performance and efficiency, the system employs machine learning concepts, specifically a Convolutional Neural Network (CNN), trained on a dataset of diverse signatures. The goal is to achieve a 5% accuracy improvement over existing systems. CNN is used to predict specific features, aiding in the detection of forged signatures. Given the dynamic nature of signatures over time, the system accounts for factors causing variations that may go unnoticed by ordinary individuals. Access to the system is restricted to authorized personnel to maintain confidentiality. The software proves versatile, applicable in scenarios like loan processing, legal document signing, and various applications, aiming to prevent financial losses and protect organizational reputation.

Eman Alajrami et al. [7]: Signature verification is a crucial aspect of personal identification and document validation, encompassing both static (offline) and dynamic (online) methods. While static verification involves assessing signatures after creation, dynamic verification occurs during the signing process on digital devices. Offline verification, though commonly used, is deemed inefficient and slow for large document volumes. To address this, online biometric methods such as fingerprints and eye scans have gained popularity. This paper focuses on creating a CNN model in Python for offline signature verification, achieving a testing accuracy of 99.70% after training and validation. The focus is to automaticallyand instantly verify signatures to ascertain their authenticity and detect forgery. Static verification involves comparing a document signature with previous samples stored in a database, while dynamic verification occurs during the creation of a signature on digital devices.

Navya V K et al. [8]: Forgery and fraud in signature verification pose significant challenges in maintaining security and authenticity in various domains. It introduces a Signature Forgery Detection and Verification system that employs image processing, optical character recognition (OCR), and machine learning techniques to detect forged signatures and ensure their authenticity. The Signature Forgery Detection and Verification system enhances the security andaccuracy of signature verification processes. By combining image processing, OCR, and machine learning techniques, it provides a comprehensive solution to identify potential forgery attempts and verify the authenticity of signatures. The system finds practical applications in various domains, contributing to fraud prevention and ensuring secure transactions.

D. Kavitha et al. [9]: Ten advances in image identification have been made possible by the availability of deep networks. With the ease with which images and movies can be shared, in addition to the accessibility of powerful editing tools, manipulating digital data has never been more simpler. We suggested strategies to identify such schemes. Two key features of using deep CNNs for image forgery detection were suggested in our paper. First, we investigate and test several preprocessing techniques using CNN architecture. Subsequently, we assessed various transfer learning methods for pre-trained ImageNet (via fine-tuning) and applied them to our CASIA V2.0 dataset. Thus, it discusses pre-processing methods using a basic CNN model before demonstrating the potent impact of transfer learning models.

Kshitij Swapnil Jain et al. [10]: Since every individual has a different signature, signatures are important across a range of sectors, including banking and finance. The problem, though, is that different signatures designed by the same person may have similarities. CNN is used in forgery detection systems,which are presented as a solution to identity crimes. The purpose of this software is to verify signatures on various platforms, such as applications, loans, and signing legal documents. Unlike passwords, signature verification is unique and unchangeable, which makes it significant. There are two types of signature verification methods: offline and online. While online verification uses more gear that is directly connected to a computer, offline verification uses less hardware and only requires taking pictures with a camera.

V. CONCLUSION

In conclusion, each paragraph emphasizes the significance of state-of-the-art technology, particularly deep learning and convolutional neural networks, in resolving issues related to picture and signature forgery detection. Reliable methods for verifying the authenticity of images across a range of businesses are required due to the widespread use of photos in the digital era and the popularity of sharing photos on social media. Particular emphasis is placed on the challenges of detecting copy-move forgeries in images; research indicates that block- and key point-based features perform effectively under a range of postprocessing conditions.

TITLE	AUTHOR	YEAR	METHODOLOGY USED	ADVANTAGES	DISADVANTAGES	APPLICATIONS
On Using Siamese Networks and Autoencoders to Verify Handwritten Signatures Online	Kian Ahrabian Bagher Babaali	2019	integrated voting technique using a1D-CNN and a priority model	Reduced data limitations: our suggested method's erroneous acceptance andrejection rates, combined with the most cutting-edge methods on previously mentioned	score 82.8% and 84.1 %.	Autoencodersfor feature learning, Security and fraud prevention.
iDeLog: Iterative Extraction of Dual Spatial and Kinematic Parameters from SigmaLognormal Data	Miguel A. Ferrer,Moises Diaz, Cristina CarmonaDuarte , and Rejean Plamondon	2022	The new process, whichwe refer to as iDeLog inthis work, determines the speed profile and eight-connected trajectory of a given lengthy and intricate movement.	Achieves high accuracy (96.16%) and sensitivity/precision for various forgery signature images, especially skilled forgeries.	might not be appropriate for identifying signatures depending on particular personal information or minute variations within a single signature.	Image processing and analysis ,remotesensing ,biomedical imaging.
An Assessment of Frequently Used Copy-Move Forgery Detection Techniques	Vincent Christlein, Christian Riess,Johannes Jordan, , Zenan Shi , Haipeng Chen , and Dong Zhang	2022	PCA and Zernike	When creating the forgeries, we aimed to create realistic copy-moveforgeries in high resolution picturesfrom consumer cameras (number of copied pixels,thetreatment of the boundary pixels and the content of the snippet)	lower accuracy for complex or diverse images, especially with smaller pixels andlow quality.	Forensic investigation ,image authentication ,biometricsystem.
Transformer - ANN for Image Manipulation Localization by OperatorInductions	Zenan Shi , Haipeng Chen , and Dong Zhang	2023	CNN,SMT, TANet,OIM	In the encoding, we use CNNs and Transformer to extract depth characteristics of the source image concurrently,so there are inevitably some redundant features	Can be computationally expensive to trainand run, limiting real time applications.	Image forensic, digital media authentication, Deep learning model interpretability.
A Novel Deep learning and Machine Learning powered approach for Image Forgery Detection	Ms. N. Nanthini ,Mr. Santosh Kumar Sahoo ,Dr.S.A.Sivakumar , Dr.S.Sasipriya ,Dr.BalachandraPattanaik , Dr.B.Maruthi Shankar	2022	ML,DL, Image ForgeryDetection, DCNN, CASIA v2.0, DVMM.	The exhibition exactness is determined on the CASIA v1.0 approval set, and the test setis 98 and 99%, individually	With the assistanceof DCNN, we extricate highlightsfrom test Images and characterize Image classifications.	Media and journalism, Document verification, Art authentication.

REFERENCES

[1]. An Assessment of Well-Known Copy-Move Forgery Detection Methods IEEE Student Member Vincent Christlein, Associate Member Christian Riess, Student Member Johannes Jordan, Student Member Corinna Riess, and Member Elli Angelopoulou

[2]. DETECTION OF SIGNAL FORGERIES USING MACHINE LEARNING N. Arpith Mathew, Teja E.,

[3]. and Ms. Manjula Subramaniam Peer-reviewed, fully refereed, open-access International Research Journal of Modernization in Engineering Technology and Science

[4]. 1D CNN and applications: A survey Serkan Kiranyaz , Onur Avcib , Osama Abdeljaber c ,

[5]. Turker Ince d , Moncef Gabbouj e , Daniel J. Inman f

[6]. SynSig2Vec: Acquiring Representations via Synthetic Dynamic Signatures for Practical Verification-Based Approach eesxlai@foxmail.com, eelwjin@scut.edu.cn Songxuan Lai, Lianwen Jin, Luojun Lin, Yecheng Zhu, Huiyun Mao School of Electronic and Information Engineering, South China University of Technology

[7]. Machine Learning-Based Signature Forgery Detection in Document Authentication SystemsSandesh Kandel

[8]. Signature Verification : Alajrami , Belal A. M. Ashqar , Bassem S. Abu-Nasser , Ahmed J. Khalil ,

[9]. Musleh M. Musleh , Alaa M. Barhoom , Samy S. Abu-Naser

[10]. SIGNATURE FORGERY DETECTION SYSTEM Navya V K, Abhilasha Sarkar, Aditi Viswanath, Akshita Koul, Amipra Srivastava

[11]. Identifying Image Forgeries with CNNs N. Rajini Hema International Journal of Recent Technology and Engineering (IJRTE) Volume 8, Issue 1S4, June 2019 ISSN: 2277-3878

[12]. Signature Forgery Detection 2022 Conference on Power, Energy,Control and Transmission Systems (ICPECTS)

[13]. HANDWRITTEN SIGNATURES FORGERY DETECTION Kshitij Swapnil Jain, Udit Amit Patel, Rushab Kheni