MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Digital Detectives: The Intersection of Artificial Intelligence and Signature Forgery Detection

Kapoor A[1] and Sinha S[2]*

[1]National Forensic Sciences University, India
[2]Forensic Science Laboratory, India

***Corresponding author:** Sweta Sinha, Forensic Science Laboratory, Sector 14, Rohini, 110085, Delhi, India, Tel: +91-7838664526; Email: sweta.fsl@gmail.com; sweta_sinhain@yahoo.com

Mini Review
Volume 10 Issue 1
Received Date: January 06, 2025
Published Date: February 28, 2025
DOI: 10.23880/ijfsc-16000440

Abstract

Signatures are the most socially accepted behavioral biometric trait which is widely used as a means of personal identification routine transactions. Signatures peculiarly represent an individual due to the presence of certain class and individual characteristics which are subconsciously accommodated within a person and become one of his normal habits with the passage of time. This signature when replicated, results in intersection of two different individual characteristics with traces of replication, which on close examination can be detected by an experienced forensic document examination expert. This paper represents a comparative study for detection of forgery between the document expert's opinion and role of Artificial Intelligence in it. It has been concluded that in order to increase the value of evidence in the court of law, the expert's opinion should be supported with the results derived from automated methods, so that objectivity can be applied to this subjective area of document examination which is majorly based on the observation skills and the experience of an expert, where the opinion of different experts can vary.

Keywords: Signature; Behavioral biometry; Forensic document examination expert; Comparison; Identification; Verification

Abbreviations

CNNs: Convolutional Neural Networks; RNNs: Recurrent Neural Networks; EER: Equal Error Rate; TS: Takagi-Sugeno; HMM: Hidden Markov Models.

Introduction

A signature is a mark or a symbol uniquely produced by a person as an indicator of his/her identity. Signatures are highly individualized due to the distinctiveness in the formation and representation of the letters in the signature and thus act as extraordinary means of personal identification and verification [1-20]. Signatures are the most socially accepted biometric trait since centuries [21-30] and this can be supported by the fact that they are widely used in making promises and giving guarantees in various day to day activities like business deals, signing checks, legal papers, marriage and divorce papers, passports, PAN card, contracts, certificates, mark-sheets, doctor's prescription, wills, etc. The problem arises when someone tries to replicate someone else's signature [26] in order to frame someone in a situation or to conceal his identity .

The forensic document examiners compare these questioned signatures to the known signatures, acquired either directly from the suspect or taken as a specimen,

present in official records. In order to prove the charge of forgery against any person, one needs to prove all the elements of forgery which includes false-making (which takes into consideration the authenticity of the documents), legal liability (which means that the document or signature put some legal liability on the individual if it had been the original one), forger's identity (the identity of the forger must be established) and the intent to defraud (the intention of the forger must be investigated in order to prove that forgery has been committed).

Apart from the traditional approaches, whereby the decisions are based on the subjective understanding of the expert, several new technologies have been emerged, including Machine learning and Artificial intelligence, which finds its application not only in the field of biometric authentication; but also in Forensic science. Deep learning approach is often considered promising because of its efficiency in image recognition and detection [31-34]. The analysis conducted with the help of various Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) boosts the accuracy and robustness of the analysis by extracting and comparing spatial and temporal features from signature data; and thereby have been proven highly efficient in reducing the false positives and false negatives in both online and offline signature verification domains [33].

Characteristics of a Forged Signature

During imitation, the forger struggles to replicate the signature while suppressing their own writing traits, which usually slows down the process. This reduced speed leads to hesitations, tremors, and a decline in line quality, detectable under a microscope. The number and placement of pen lifts differ from the original, and blunt starts and stops indicate a lack of fluency. Unnecessary pen lifts may occur as the forger corrects the position of the pen. Additionally, the movement and skill of the writer cannot be changed or modified. The possibility that the skill of the forger is higher than that of the writer, that will be depicted on careful examination of the questioned and known signatures. Also, in the traced forgeries, mathematical similarities are found which contradicts the basic principle of signature examination and gives a clear indication about traced forgery.

Assessing the Results of Forgery Detection by Automated Techniques

Signature examination is inherently subjective, highlighting the need for a more objective and scientifically grounded approach, which can be facilitated through automated signature verification tools [18]. These approaches are classified into two categories: writer-dependent, where a specialized classifier is used for each individual writer, and writer-independent, where a single classifier is employed for all writers and trained to detect forgeries. The writer-independent approach is generally favored, as the system can be trained using previously collected specimens [12].

Automated signature verification is conducted in two forms: offline verification, which is performed when only the static image of the signature is available, and online verification, which utilizes the spatial and temporal characteristics of the writing process (i.e., dynamics) [17,19,20]. Static signature verification presents more challenges and is prone to higher error rates compared to dynamic verification [17]. A comparison of the performance of offline and online verification systems revealed that the offline system had an equal error rate (EER) of 9.15%, while the online system, using the same set of signatures, achieved a significantly lower EER of 2.85% [6].

For offline automated signature recognition and forgery detection, methods such as Convolutional Neural Networks (CNN) and the Crest-Trough approach, which utilizes the SURF and Harris corner detection algorithms, achieve accuracy rates of 85-90% for forgery detection and 90-94% for signature recognition [26]. Alternatively, offline recognition can be performed using fuzzy modeling with the Takagi-Sugeno (TS) model, where angle features are extracted and compared via a box approach, yielding relevant results [20]. In dynamic online signature verification, feature-based methods using pen down duration, velocity, and pressure as characteristic features yielded an equal error rate (EER) of 10.66% for skilled forgeries and 6.95% for random forgeries. Additionally, it was found that if the total signature duration exceeds 10 seconds, there is a 96.9% probability that the signature is forged [30]. Various models are employed in signature modeling and stability detection, each emphasizing different features with specific weights [14,12]. Hidden Markov Models (HMM) are particularly effective and widely accepted due to their adaptability to personal variability [12,31]. Graphical models, used for both online and offline signature verification, represent the signature's shapes, nodes, and edges. Attention is also directed towards examining pseudo-dynamics of signatures, where forensic document examiners analyze trace features under a microscope [12]. Additionally, Explainable AI (XAI) is emerging as a tool for signature verification, enhancing the interpretability of machine learning models and supporting their use in legal decision-making processes [33].

Comparing the Accuracy of Results Given by Forensic Document Examination Expert and Automated Systems:

Efforts are underway to align expert opinions with automated system results to strengthen legal evidence

[6]. When comparing automated systems' performance in identifying genuine, simulated, and disguised signatures with forensic document examiners, accuracy ranged from 75-90%, with forensic examiners achieving 84.8% [18]. This suggests automated results are close to experts, but further focus is needed on disguised signatures due to higher error rates. Additionally, research is advancing in regaining signature dynamics from static images, leading to forgeries with higher false acceptance rates than simulated ones [11,19]. Standardizing terminology for signature forgeries is also necessary, as current terms vary among researchers.

Challenges and Path Ahead

Although much work has been done in developing and testing of various machine learning models, there are still challenges that are being encountered, which holds back the use of these models in the criminal justice system. This includes:
Variability: As compared to other biometric features, the signature of a person is bound of have high intra-class variability i.e., variations in one's own writing, which arises as a cumulative result of a number of factors and sometimes low inter-class variability i.e., in cases of skilled forgeries, moreover a 100% match is also a forgery i.e., traced forgery, which the model might depict as a match to the genuine signature. Due to all these, it is challenging to computerize this biometric detection.

Training: Perhaps the most difficult task is to train the computational model as to what is and what is not is to be considered a match, owing to the high variability of this behavioral biometric trait. Moreover, the success of the model also depends on the diversity of the training dataset.

Quality of Data: It is indeed a challenge to train the neural network with the datasets having insufficient extractable features, based on the model makes a decision for a match or a not-match. The data must contain the extractable features in both stages of training and verification. However, collecting and labeling such data can be resource-intensive and time-consuming.

Computational complexity: The development and designing of such an algorithm or a machine learning model which can understand the complexities of this behavioral trait is in itself a great challenge.

Evolving Forgery Techniques: With the advancements in the techniques of performing the forgery, the AI-based systems must be made robust enough to dodge through the deceit and must be able to adapt and learn continually with time.

Security and Privacy: In the distributed systems, where there is a log of the genuine signatures required for matching, there is always a concern on security due to high chances of data being hacked or compromised or rather duplicated or altered and thereby shaking the very basis of developing the models in the first place.

Conclusion

It can be concluded that the method of forgery detection by forensic document examination experts is highly subjective and needs a bit of objectivity for which various algorithms and computational models are being made and their performance is being analyzed. The gap between the expert's opinion and the results given by various online and offline signature verification systems should be bridged so that the value of the evidence presented in the court of law is increased, the process of forgery detection can become more reliable and the results can be reproducible as the opinion of different experts can vary. However, with the combined knowledge of the dynamic process of production and static image of the signature more information can be extracted about the genuine writer and the forger, which helps the experts in examination and comparison. The strengths of the AI-based and Machine learning-based models, when combined with the robust architectural principles which lay the building blocks of the field and the human intelligence, collectively, can achieve a great balance between the accuracy of the analysis, its robustness, scalability and security.

References

1. Bates BP (1970) Identification System of Questioned Documents (ISQD). Charles C Thomas Publishers.

2. Vikas B, Mohinder S, Suryakant M (2017) Forensic examination of digitally Fabricated signatures in printed documents. Problems of Forensic Sciences 112: 111-122.

3. Gajanan B, Vijay M (2013) Digital image forgery detection using passive techniques: A survey. Digital Investigation 10: 226-245.

4. Carolyne B, Bryan F (2016) The modular forensic handwriting method. Journal of Forensic Document Examination 26: 7-83.

5. Carolyne B, Bryan F, Kaye B, Doug R (2010) Forensic handwriting examiners' opinions on the process of production of disguised and simulated signatures. Forensic science international 195: 103-107.

6. Vivian B, Franke H, Katrin C, Louis V (2009) ICDAR 2009 Signature Verification Competition. pp: 1403-1407.

7. Boyer KW, Govindaraju V, Ratha NK (2007) Special Issue on Recent Advances in Biometric Systems, IEEE Trans. on Syst, Man and Cybernetics-Part B 37(5).

8. Brault JJ, Plamondon R (1993) A Complexity Measure of Handwritten Curves: Modeling of Dynamic Signature Forgery. IEEE T-SMC 23(2): 400-413.

9. Desai B, Kalyan JL (2013) Forensic Examination of Handwriting and Signature. International Journal of Innovative Research and Development 2.

10. Ellen D (2005) Scientific Examination of Documents: Methods and Techniques. In: 3rd (Edn.), Boca Raton: CRC Press.

11. Jean H, Renato L, Andreas H, Rolf I (2007) A New Forgery Scenario Based on Regaining Dynamics of Signature pp: 366-375.

12. Impedovo D, Pirlo G, Plamondon R (2012) Handwritten Signature Verification: New Advancements and Open Issues. 2012 International Conferenceon Frontiers in Handwriting Recognition pp: 367-372.

13. Kelly JS, Lindblom BS (2006) Scientific Examination of Questioned Documents, second edition, Taylor & Francis. CRC.

14. Kim SH, Park MS, Kim J (1995) Applying Personalized Weights to a Feature Set for On-line Signature Verification. In: 3rd International Conference on Document Analysis and Recognition (ICDAR-3), IEEE Computer Society, Montréal, Canada 1: 882-885.

15. Koppenhaver K (2007) Forensic Document Examination, Principles and Practice Humana Press.

16. Chandra L (2010) Cross Examination of Handwriting Expert pp: 17.

17. Leclerc F, Plamondon R (1994) Automatic signature verification: the state of the art 1989–1993. In Progress in Automatic Signature Verification. World Scientific Publ Co pp: 13-19.

18. Marcus L, Heuvel C, Bryan F, Muhammad I (2010) Forensic Signature Verification Competition 4NSigComp2010 - Detection of Simulated and Disguised Signatures. 12th International Conference on Frontiers in Handwriting Recognition, pp: 715-720.

19. Liwiki M, Malik MI, Berger C, Hauvel E, van der R, Found B, et al. (2020) Automatic Signature Verification – Where Are We Now and Where Should We Go?. Pattern Recognition (Submitted).

20. Vamsi M, Yusof M, Hafizuddin M, Madasu H, Kurt K (2003) Off-Line Signature Verification and Forgery Detection System Based on Fuzzy Modeling 2903: 1003-1013.

21. Mehta MK (1972) Identification of Handwriting and Cross Examination of Experts. pp: 103-166.

22. O'Reilly C, Plamondon R (2009) Development of a Sigma-Lognormal Representation for On-Line Signatures. Pattern Recognition, Special Issue on Frontiers in Handwriting Recognition 42: 3324-3337.

23. Osborn AS (1973) Questioned Documents, Patterson Smith Publication Corporation.

24. Plamondon R (1995) A Kinematic Theory of Rapid Human Movements: Part I – Movement Representation and Generation. Biological Cybernetics 72(4): 295-307.

25. Plamondon R, Djioua M (2006) A Multi-Level Representation Paradigm for Handwriting Stroke Generation. Human Movement Science 25(4-5): 586-607.

26. Jivesh P, Vinanti P, Santosh B (2020) Offline Signature Recognition and Forgery Detection using Deep Learning. Procedia Computer Science 170: 610-617.

27. Sharma BR (2003) Forensic Science in Criminal Investigation & Trials pp: 585-591.

28. Jodi S, Bryan F, Doug R (2002) Forensic Handwriting Examiners' Expertise for Signature Comparison. Journal of forensic sciences 47: 1117-1124.

29. Srihari SN, Xu A, Kalera MK (2004) Learning Strategies and Classification Methods for Off-line Signature Verification. 9th International Workshop on Frontiers in Handwriting Recognition (IWFHR-9), Kichijoji, pp: 161-166.

30. Ruben T, Vera-Rodriguez R, Julian F, Ortega-Garcia J (2015) Feature-Based Dynamic Signature Verification under Forensic Scenarios.

31. Van B, Garcia-Salicetti S, Dorizzi B (2007) On Using the Viterbi Path Along with HMM Likelihood Information for Online Signature Verification. IEEE Trans. on Syst., Man and Cybernetics – Part B 37(5): 1237-1247.

32. Stewart LF (2017) The Process of Forensic Handwriting Examinations. Forensic Research & criminology International Journal.

33. Chavan M (2019) Advancing Signature Verification with Machine Learning and AI: A Proactive Cybersecurity Approach.

34. Hsin-Hsiung K, Che-Yen W (2020) An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach. Applied Science.