A Quantitative Analysis on Automatic Signature Verification through Machine Learning Mechanism

[1]Riya Patil, Information Technology
[2]Snehal Solat, Information Technology
[3]Shailaja Shriramula, Information Technology
[4]Radha Lokhande, Information Technology
[5]Guide name: Prof. Priyanka kedar, Information Technology, Dhole Patil College of Engineering Pune.

Abstract — Handwritten signatures are one of the oldest and most widely used biometric authentication techniques in administrative and financial institutions due to its simplicity and uniqueness. As technology progresses, authentication methods have also evolved. Handwritten signatures are now being used extensively for various purposes where authentication of the individual is required. The manual verification is one of the most problematic ways for the authentication that requires a lot of time. Therefore, to improve the process and allow for the faster and precise authentication, a large number of related researches have been analyzed in this survey paper. The devised approach utilizes Convolutional Neural Networks to attain the signature verification, which will be detailed further in the future researches.

Keywords: *Convolutional Neural Networks, Biometric Authentication.*

I. INTRODUCTION

The process of authentication of a document has been highly essential since the early days of mankind. There have been seals and other official marking that have been used throughout the history, but a signature has come forth as one of the most powerful and highly recognized forms of authentication even today. The signature of an individual is one of the most useful biometric characteristics that has been one of the most utilized forms of authentication of a document or a transaction. A signature is widely considered as one of the most legal forms of authentication that are utilized at banks and government agencies.

The signature are considered for the purpose of authentication due to the fact that the signatures have some characteristics that are behavior oriented and based on the biometrics of the particular user. Along with this fact, the low cost of implementation and acceptance almost unanimously allows for a robust and a highly effective authentication mechanism. The signatures can be made up of nicknames, names, legal credentials and other forms of identity that is personal and closer to the user.

Signatures are the kind of biometric authentication that can be utilized in a variety of authentications such as cheques, formal documents, or letters. The signatures thus need to be verified to determine if they are authentic and written by the actual hand of the individual or they are a forgery committed by a person with nefarious intent. The incorrect authentication of the signature can be problematic as this could lead to another illegal individual getting access to the resources of someone else. The verification of signatures is extremely important task in the modern world which has its basis in authentication.

Biometrics equipment is used to safeguard a wide range of security mechanisms. The goal is to recognize personality based on biological or psychological characteristics. The first element, identification, is dependent on the evaluation of physical attributes such as fingerprints, faces, iris, signatures, and so on. Biometric identification technique, on the other end, is recognized as the most common instrument and the least expensive based on morphological recognition is handwritten signature for a broad array of technologies, such as organization forms, formal contracts, and financial transactions.

It is a fallacy that a person's legitimate signature would be indistinguishable whether done several times. Synchronization of the muscles, nerves, eyes, arms, and fingers with the brain is required for signature. Other elements influencing the signature include the user's surrounding, health, maturity level, demeanor, and psychological response at the time of signing. As a result of the multiple variables at work, some components may not seem the same in every signature. The expertise and accuracy with which a signature fabrication is performed makes identification much more challenging and critical. The forger's priority is generally to produce an appropriate replica of the real signature rather than just to sign eloquently.

Therefore, the manual verification of signatures is a tedious and a highly error prone activity. There has been a considerable increase in the number of forgeries that are getting more and more sophisticated by the day. To reduce such occurrences and perform accurate evaluation of the signatures, an effective and automatic methodology needs to be introduced. For this purpose, this research paper has been utilized to perform the background review on the previous and existing systems for sign verification to reach our

approach, which will be elaborated further in the upcoming editions of this research.

This literature survey paper segregates the section 2 for the evaluation of the past work in the configuration of a literature survey, and finally, section 3 provides the conclusion and the future work.

II. RELATED WORKS

M. Mshengu [1] states that a virtual signature verification technique dependent on HOG and NCC pattern matching was suggested, described, and tested in this paper. Although HOG characterization has traditionally been used for offline signature authentication, it was effectively used in this research. On the SVC2004 dataset, the estimated exactness extend from 60 to 80 percent, according on the variation of signature covering technique utilized. According to the authors, the remaining half treatment is typically seems to have a great potentiality because it is highly probable to generate the least EER.

S. Soisang [2] explains a new texture feature centered on local binary patterns utilising Gradient Quantization Angle (GQA) (LBP). The Local Binary Gradient Quantization Angle Patterns are a novel textural characteristics methodology (LBGQAP). In addition, we integrated ANN classifiers to solve the offline handwritten signature verification challenge. CEDAR datasets were used for the experimental investigation. The findings demonstrated that LBGQAP provides better performance in terms of train and test consistency. Furthermore, the Precision Recall and F-Measure values of the LBGQAP are higher than those of the LBP.

S. Jain [3] reviews prior work in the subject of signature forgery detection the proposed approach used a state-of-the-art fully connected Siamese Neural Network architecture to execute an effective signature fraud identification technique. Data gathering, pre-processing, segmentation using CNN, and assessment employing contrastive loss are all part of this technique. This approach achieved a high recognition rate that was almost flawless, and contrast loss is reduced.

Aravinda C.V [4] have included information on publicly accessible offline handwritten signature datasets as well as information about the datasets we utilised for these experiments. Furthermore, the authors described the steps they took to create a rather large collection of offline handwritten signatures. Especially comparison to any other available to the public dataset, the newly produced dataset is extremely huge. The author intended to publish this new dataset freely accessible on their college's website so that others might utilise it for scientific purposes.

C. S. Vorugunti [5] explains the suggested OSV approach for dealing with the data scarcity issue in online signature verification. The authors employed Generative Adversial Networks to construct synthetic signature samples, in which a generator model learns to generate false samples based on discriminator error. Finally, the experimental research demonstrated that GANs can do complicated tasks like online signature verification in a human-like manner. In distinguishing between actual and fraudulent samples, the model achieved greater classification accuracies. The suggested model was assessed by the researchers, and it produced the best results when contrasted to current state-of-the-art models.

B. M. Rankinc [6] created a method for automated spectral signature evaluation that may be used to determine the detectability of certain objects/materials and make sensor selection decisions The technique is based on feature composition in a spectrum and has been demonstrated to be generic for a variety of sensing modalities, particularly passive VNIR and LWIR spectroscopy. Furthermore, the algorithm's quantitative output is often connected with target identification performance.

Hsin-Hsiung Kao [7] offer an online handwritten signature verification technique based on a deep CNN network that uses a single known sample. The researchers ensure the reliability of the experimental results by employing a number of techniques, including the removal of background noise and preprocessing, the design of controlled groups for various sample sizes and network architectures, and the use of visualisation techniques to provide model interpretability. The experimental results show that automated signature verification may be performed with a single known sample.

Deniz Engin [8] have provided a detailed research on writer independent offline signature verification in a real-world setting, in which obscured signatures of bank clients are validated versus their cleaned reference signatures. The researchers presented a stamp removal strategy based on CycleGAN to clean signatures prior sending them to a CNN model to retrieve the signature representations. The authors also evaluated and examined the implications of various verification settings, fine-tuning procedures, and signature representation methodologies. A human assessment was also performed to demonstrate the difficulties of the situation.

Prarthana Parmar [9] Signature is defined as a behavioural biometric that is used to verify human identification. Handwritten signatures are the most commonly utilised biometric attribute since handwriting is an unconscious activity and specific pen motions are invariant and cannot be easily altered when forgery is performed. This strategy was chosen after studying all of the methodologies for all of the procedures to identify offline signatures in this research article. This approach is the most recent method being explored, therefore it has a greater future potential for development. Improvements are

observed in boosting the accuracy of discovering resemblance in signatures and providing better assistance in determining whether the signature is genuine or counterfeit.

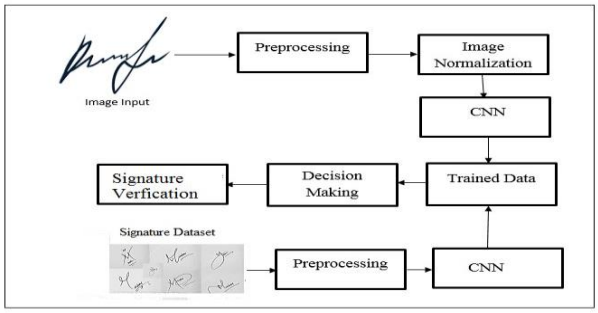
Neha Sharma [10] Offline signature verification is employed in many applications, hence there is a need for a system that can distinguish real signatures from faked signatures. The authors have explored numerous signature verification needs, kinds, and methodologies or models that may be used for this purpose in this study. The authors also discussed the researchers' efforts over the previous three decades. Many strategies, whether engineering- or deep-learning-based, have been used to accomplish this objective. Deep Learning-based approaches have recently gained popularity due to their ability to learn from raw data or pixels.

Tushara D [11] states that signatures are used in all financial transactions to authenticate human identification, but these verification systems are still relied on manually verifying the signature with permitted signatures. As a result, a system based on computer-based categorization is necessary. In this study, an online signature verification system based on neural network classification is suggested. The provided system takes many signatures from the user database and extracts a database of x, y coordinate and velocity values at various places from which a separate specialized feature set is calculated.

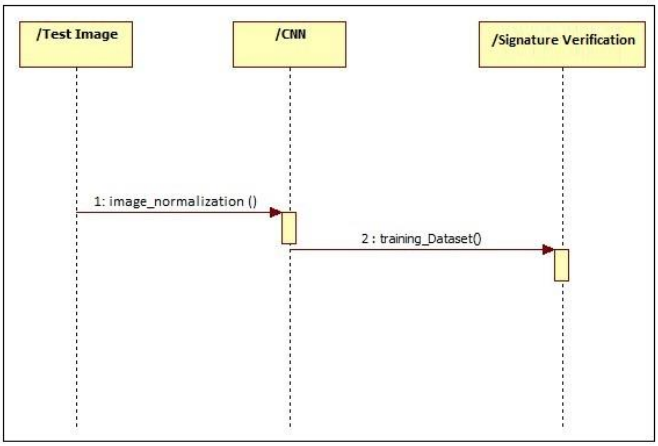
Mustafa S. Kadhm [12] this article describes a rapid, accurate, and dependable signature verification method. The system reached an extremely high level of verification accuracy. Furthermore, the preprocessing approaches employed in the suggested feature extraction strategy based on HSC enabled the system to achieve higher accuracy results. Furthermore, the suggested ANN design improves the obtained results with the least amount of error based on three public distinct signature image databases. The authors of this study indicated that in the future, CNNs might be used efficiently in real-time verification systems for feature extraction and classification utilizing the weighted Softmax activation function, which has been successfully utilized in many identifiability problems.

Nehal Hamdy al-Banhawy [13] an overview of frequently used preprocessing methods, feature extraction methods, and methodologies for online and offline handwritten signature recognition and verification systems was provided. In addition, a comparison of suggested systems used in recent studies for verification techniques, identification techniques, feature extraction, and in offline and online systems with presenting of database utilized and outcomes for each system is provided. Based on the comparison, it was determined that employing SURF, SIFT, and histogram of oriented gradients techniques in conjunction with mathematical modification for feature extraction yielded better results.

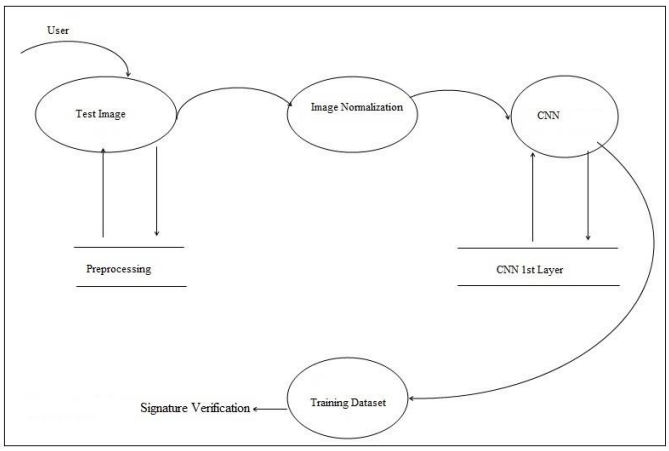
III. SYSTEM ARCHITECTURE

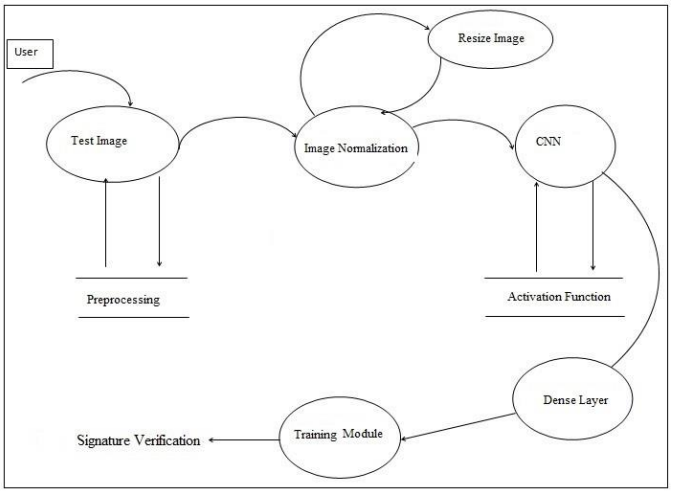


IV. SEQUENCE DIAGRAM



V. DATA-FLOW DIAGRAM





VI. CONCLUSION AND FUTURE SCOPE

This survey article has been effectively utilized to achieve an efficient and effective signature verification methodology for automated verification. Numerous research articles have been analyzed in this survey paper to understand the methodology of the automatic signature verification. A number of existing systems as well as previous researches have been effective in determining the various characteristics of an automatic signature verification system. There have been a number of drawbacks and other inconsistencies that have been observed in the conventional methodologies that need to be rectified. The process of automatic signature verification is quite complicated and complex which is extremely problematic to perform manually. The process of manual authentication of the signature can also be the source of some errors that can be disastrous in critical situations. Therefore, an effective methodology for automatic signature verification using Convolutional Neural Networks has been proposed, which will be elaborated further in the upcoming editions of this research.

REFERENCES

[1] M. Mshengu and M. V. Gwetu, "Online Signature Verification through Scaled Histogram of Oriented Gradients," 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), 2019, pp. 1-5, doi: 10.1109/ICABCD.2019.8851050.

[2] S. Soisang and S. Poomrittigul, "New Textural Features for Handwritten Signature Image Verification," 2021 7th International Conference on Engineering, Applied Sciences and Technology (ICEAST), 2021, pp. 20-24, doi: 10.1109/ICEAST52143.2021.9426314.

[3] S. Jain, M. Khanna and A. Singh, "Comparison among different CNN Architectures for Signature Forgery Detection using Siamese Neural Network," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 481-486, doi: 10.1109/ICCCIS51004.2021.9397114.

[4] A. C.V, L. Meng and U. K. R. K.R, "An approach for signature recognition using contours based technique," 2019 International Conference on Advanced Mechatronic Systems (ICAMechS), 2019, pp. 46-51, doi: 10.1109/ICAMechS.2019.8861516.

[5] C. S. Vorugunti, P. Mukherjee and V. Pulabaigari, "Online Signature Profiling using Generative Adversarial Networks," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020, pp. 894-896, doi: 10.1109/COMSNETS48256.2020.9027369.

[6] B. M. Rankin, T. P. Lippa and J. B. Broadwater, "Spectral Information Content Algorithm for Automated Signature Assessment," IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, 2020, pp. 1790-1792, doi: 10.1109/IGARSS39084.2020.9323899.

[7] Kao, Hsin-Hsiung & Wen, Che-Yen. (2020). "An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach. Applied Sciences." 10. 3716. 10.3390/app10113716.

[8] Engin, Deniz & Kantarcı, Alperen & Arslan, Secil & Ekenel, Hazım. (2020). "Offline Signature Verification on Real-World Documents", 2020.

[9] P. Parmar et al, "A Survey of Handwritten Signature Verification System Methodologies", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN: 2349-5162, Vol.6, Issue 5, page no.1-6, May – 2019.

[10] Neha Sharma et al, "A Comprehensive Study on Offline Signature Verification", 2021 J. Phys.: Conf. Ser., 2021.

[11] Tushara D, Shridevi Raddy, Shreya K M, Spoorthy Y, 2021, Signature Verification System using Neural Networks, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCCDS – 2021 (Volume 09 – Issue 12),

[12] Mohammed, Mamoun & Kadhm, Mustafa & Ayad, Hayder. (2021). An accurate signature verification system based on proposed HSC approach and ANN architecture. Indonesian Journal of Electrical Engineering and Computer Science. 21. 215-223. 10.11591/ijeecs.v21.i1.pp215-223.

[13] Nehal Hamdy Al-banhawy, Heba Mohsen, Neveen Ghali2, "Signature Identification and Verification Systems: A Comparative Study on the Online and Offline Techniques", Future Computing and Informatics Journal, 2020.