IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Handwritten Signature Recognition System

Sudhanshu Sharma[1], Tanmay pareek[2] and Niket Sharma[3]

[1] Guided By Mr. Deepak Moud [2] Ass. Professor
[3] Poornima Institute Of Engineering And Technology,Jaipur [4]Affi. By Rajasthan Technical University, Kota

Abstract –

In today's generation, machine learning researchers are successfully studying the verification and validation of hand written signatures. Each individual has a distinct signature that is primarily utilised for reasons related to private verification and identification of significant papers or legal transactions.Finding out whether the signature is genuine or fake is the goal of signature authentication. The aim of this paper is to gain the multi-classclassification and high accuracy with sample of training signatures. Using a variety of image processing methods, images are preprocessed to separate the signature elements from the backgroundpixels. In this paper, for the creation of the model we have used 24 genuine signature's of 75 different user's and 10 forged signature of 75 different user's. For the classification of name's and real – forged classification we have used a pretrained network transfer learning namedVGG16 model in which 1.2 million images were used to train a convolutional neural network to classify 1000 distinct categories.

Keyword –

Convolution Neural Network, VGG16 Model, Signature Authentication, Signature Verification, Transfer Learning

Introduction –

Signature verification and forgery detection refer to the process of immediately and automatically evaluating documents to determine whether they are authentic or not. The process of automatically and instantaneously evaluating documents to determine whether they are authentic or not is referred to as "signature verification" and "signature validation or forgery detection."There are two primary types of signature verification: static and dynamic. While a person makes their own signatures on a computer, smartphone, tablet or other similar device, which are then verified dynamically or online, static verification, also known as off-line verification, is a form of authentication that occurs offline.By comparing the signature in issue to a previous sample of a person's signature, the database is then created.

Problem Statement –

Today, a wide range of operations, including banking, healthcare, and education, are carried out online. However,as internet platforms are used more frequently, fraud has also increased, especially in the banking industry. These online scams can seriously affect people because their hard-earned money is being stolen in an unethical and illegal manner.Those who rely on online banking services are quite concerned about the increase in online fraud. Phishing schemes, identity theft, and unauthorised access to personal financial accounts are just a few examples of the fraudulent behaviours that can be committed. Unfortunately, as cybercriminals develop more sophisticatedtactics, it becomes harder to identify and stop online fraud.

As a result, it's critical for people to exercise caution and exercise due diligencewhen engaging in online banking operations. This can entail creating secure passwords, refraining from disclosing private information online, and routinely checking bank account activity for any unusual transactions. In order to safeguard their clients from online fraud, financial institutions such as banks must also make steps to strengthen their security protocols.

Literature Survey –

Signature verification: A study –The cutting-edge techniques now employed in offline signatures verification systems. They acknowledge that, despite the wide range of methods employed, these systems' accuracy still has to be increased, especially in the case of professionalforgeries. The author then discusses and contrasts several strategies, examining their accuracy, false acceptance rate (FAR), and false rejection rate (FRR). They point out that more study is required to enhance offline signature verification because the accuracy currently attained by present techniques is not very great. The author speculates that future research inthis area might involve combining various classifiers to provide better verification outcomes.[1]

A Comprehensive Study on Offline Signature Verification – The value of signature as a behavioural biometric in a variety of contexts, including banking, passports, and financial paperwork.Unfortunately, it might be difficult to confirm these signatures, particularly offline where there is no informationavailable regarding the signing procedure. A technique that can differentiate between authentic and forgeried signatures is required to prevent fraud. Over the past three decades, a lot of research has been done in this area, and to improve the precision of signature verification systems,

handmade characteristics and deep learning techniques are now being used. Nonetheless, there is still more to be done, and further study is required to find solutions to the problems that offline signature verification still faces.[2]

Offline Handwritten Signature Verification – Literature Review – Despite much study in the area, handwritten signature verification still faces several difficulties. In the offline scenario using scanned images, it is difficult for Signature Verification Systems to distinguish between real signatures and fakes. Although improvements have been suggested, such as the use of Deep Learning techniques, the system's accuracy could yet be increased. The paragraph ends by highlighting the need for more study to address the problems with handwritten signature verification that still persist.[3]

A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning Techniques –The significance of handwritten verification of signatures is covered in this article as a two-class classification issue in the fields of computer vision and machine learning. Itis essential to pick an efficient machine learning technique given the frequent use of signatures in legal papers and financial transactions to prevent losses brought on by forgeries. The paper examines the state-of-the-art work in feature extraction, classification, and various dataset comparisons while comparing both online and offline signature verification, as well as the challenges involved. Additionally, it offers a table-formatted summary of the benefits and drawbacks of the machine-learning methods used for signature authentication. The paper lists the most important datasets that are accessible in both online and offline areas and explains the general steps of the verification system.[4]

Handwritten Signature ForgeryDetection using Convolutional Neural Networks – It has been successfully applied to create a system that can learn from signatures and predict whether or not a signature is a forgery. Various government agencies where handwritten signatures are used for authentication or approval can use this method. The structure of our completely connected layer is not ideal, despite the fact that this technique employs CNNs to learn the signatures. According to this might be regarded as an extremeapplication. For each user in the model developed in this study, two classes are created. (genuine and forgery). The model would have 200 classes to predict if the genuine and forgery signatures of 100

individuals were provided, which would make the learning process more difficult.A future improvement would be to conduct in-depth research on loss functions and create two or more custom loss functions that could forecast the user to whom the signature belongs and whether or not it is a forgery.[5]

Verification of Handwritten Signatures - an Overview –The subject of study for automatic signature verification is particularly appealing. In recent years, in addition to the internet's ongoing expansion and the ICT industry's growing security requirements In society, there is a resurgence of interest in the topic of automatic signature verification. An overview of the field of automatic signature verification is provided in this paper. The most pertinent research directions are highlighted by a discussion of the key features associated with each stage of the signature verification process. They include genetic algorithms for individualised featureselection, multi-expert classification systems for reliable signature verification, and enhanced strategies for signature analysis that can concentrate on the stable/variable components of signatures.[6]

Handwritten Signature Verification using TensorFlow – In CNN, a new system was developed for the detection of fake signatures, and the system demonstrated a 90% detection accuracy. By building a larger database, the system can be enhanced to enable rigorous learning throughout the training phase. Additionally, the availability of strong GPUs would hasten the learning process. With these GPUs, the system can analyse higher resolution images quite easily. The trained networks can then be transferred to a low power hardware, like the Raspberry Pi, and used to verify new signatures while using a fraction of the power. Additionally, the research's significance stems from its widespread use in identifying banking frauds, which helps to resolve numerous legal problems.[7]

A Hybrid HMM/ANN Based Approach for Online Signature Verification –In this paper, a hybrid HMM/ANN model-based heuristic method for online signature verification was presented. We believe that this is the first instance of this approachbeing used for online signature verification. In contrast to other works that are also based on HMM/ANN, a group of ANNs areused as probability estimators for an HMM in order to create a prediction system that is effective. Using this hybrid model, several encouraging experimental findings are made. There are two key areas where this work could be improved: 2) The use of additional time sequences, such as coordinates and pressure, which can also be employed as informative features together with the angle series. I) The coupling of this methodology with other methods.[8]

Offline signature verification based on geometric feature extraction using artificial neural network – The use of geometrically based feature extraction for offline signature verification was investigated in this research. Using the back propagation learning technique and 18 sets of unique users with variable numbers of training and testing samples, the effectiveness of the suggested method is evaluated. CEDAR dataset was used for experiments. Future work will focus on developing better pre-processing techniques to increase the precision of geometric-based feature extraction.[9]

Handwritten Signature Verification using Deep Learning – Every person has a distinctive signature that is primarily used for personal identification and to confirm the authenticity of significant papers or legal transactions. Static and dynamic signature verification are the two types available. Whereas dynamic (on- line) verification occurs as a person makes his or her signature on a computer tablet or a similar device, static (off-line) verification takes place after an electronic or document signature has been made. For a lot of documents, offline signature is ineffective and slow. We have seen an increase in online biometrics individual verification such as fingerprint, eye scans, etc. to overcome the limitations of offline signature verification. In this study, we used Python to develop a CNN model for offline signatures. After training and validating the model, testing accuracy was 99.70%.[10]

Handwritten Signature Verification using Local Binary Pattern – Featuresand KNN The authors were inspired to create their own system by theapproximately 40 articles that researchers have been working on in relation to building a recognition system. The researchers deserve praise from the authors for sharing their knowledge and experience. Although recognition rates are crucial, other elements including application, application requirements, time and space requirements, algorithm complexity, and cost must also be taken into account when creating a system.[11]

Machine learning-based offlinesignature verification systems: A systematic review –This systematic review focuses on machine learning-based verification models for offline signatures, which are commonly used in biometric authentication in financial and administrative applications. The review analyzed 56 articles published between 2014 and 2019, examining datasets, preprocessing techniques, feature extraction methods, verification models, and performance evaluation metrics. The review found that deep learning-based

neural networks had achieved the most promising results on public datasets, but also identified 15 open research issues for future development.[12]

Learning features for offline handwritten signature verification using deep convolutional neural networks – The use of offline signatures for verifying identity is difficult in the presence of skilled forgeries. To address this, a new approach is proposed that usesConvolutional Neural Networks to learn representations from signature images in a Writer-Independent format. This approach includes knowledge of skilled forgeries and achieved state-of-the-art performance on four datasets, while also showing that the learned features generalize beyond the GPDS dataset.[13]

A Recurrent Neural Network baseddeep learning model for offline signature verification and recognition system –The proposed system in this article uses Recurrent Neural Network (RNN) based methods to verify and recognize offline signatures of different persons. The system extracts structural and directional features locally from each signature sample and uses two RNN models, LSTM and BLSTM, to study the generated feature vectors. It outperforms the state-of-the-art results and achieves superior performance compared to CNN based results. The system is tested on six public signature databases.[14]

A Survey of Offline Handwritten Signature Verification Based on Deep Learning – This paper provides a comprehensive review of the literature on offline handwritten signatures over the past decade, with a focus on deep learning-based signature verification methods. The authors evaluate the current state of thefield and suggest possible future research directions, as the application of handwritten signature technology has seen significant development in recent years. The paper aims to provide a roadmap for the continued development of this technology.[15]

Methodology –

In this project, the most challenging task is collection of dataset and after collecting dataset how to train a model so that it can classify the name and verify real or forged signature, how to create the directory of dataset, what will we the hierarchy structure of the dataset, how to define the dataset so that our model can easily able to classify the name and verify the real or forged signatures. So at first, we have taken the 24 real signature of different peoples and 10 forged signature of the same peoples. And we have collected the signature of 100 different peoples it means we total have

2400 real signature and 1000 forged signature of different people and total of 3000 plus signature we have for our dataset and after the collection of dataset we define our directory in such a way that our model can easily classify the name and real, forged signature from the directory. For this project we have created two main directories as we created two different VGG16 model for image classification. The first directory is for classifying the name of the user who's signature is this and the second directory is for classifying the signature is real or forged. In the directory where we have to classify name, inside that directory we have created 100 folders of 100 different peoples and inside these folders we put all the signatures which are real as well as forged and we put the real and forged signature together because in case the image of signature in cheque is fake so that our model at least predict that this signature is fake of that person that's why we put real and forged signature together in the same directory. To classify the signature is real offorged in the second directory we created two different directories one is real and other is forged. All the real signature of 100 peoples put together in the real directory and all the forged signature of 100 peoples put in forged directory.We have developed a machine learning model using the VGG16model for two main tasks, signature recognition and verification. The project is divided into two sections, with the first section focusing on signature recognition and extraction, while the second section focuses on signature verification and validation.In the first section, we develop a model to recognize and extract signatures from an image. This may involve identifying specific patterns or features that distinguish a signature from other elements in the image, such as text or graphics.The second section is further divided into two halves, one for validation and one for verification. In the validation phase, we train a model to compare a signature to a known reference signature and determine if they match. This could be used to authenticate the identity of the person who signed a document.In the verification phase, we develop a model to compare two signatures and determine if they were made by the same person. This could be used to detect forgeries or to compare signatures from different documents.To accomplish these tasks, we train two separate models using the VGG16 architecture, one for validation and one for verification. These models will be combined in the final phase of the project to provide a complete signature verification and validation system.

Conclusion –

This paper presents the machine learning and deep learning model which is used to

extract signature from the cheque and with the help of the extracted signature image the model is capable enough to tell which user's signature is this and the signature is real or fake. With this model the main problem of current scenario can be solved which is bank fraud. By appying this approch we can minimize the bank frauds by verifying and validating siganture online.

Future Scope –

In this project as we are validating and verifiythe signature from the image of a cheque accuracy is the major proble we faced. So accuracy can still be increased, and more models can be evaluated and compared to see which method works the best. And as we created our own dataset and we don't use the publically availabe dataset so there is the limitation on dataset which resuts in low accuracy because model is trained on low dataset. In the future we can increase the dataset so that our model will predict the outout correctly and accuracy also increased.Although many methods are employed in this area, accuracy needs to be improved, particularly for skilled forgeries.Since the accuracy of the current systems has not been very good, more research on signature verification is necessary.

References –

[1] Mushtaq, Saba & Mir, Ajaz. (2013). Signature verification: A study. Proceedings - 4th IEEE International Conference on Computer and Communication Technology, ICCCT 2013. 258-263. 10.1109/ICCCT.2013.6749637.

[2] Sharma, Neha&Gupta, Sheifali & Mehta, Puneet. (2021). A Comprehensive Study on Offline Signature Verification J. Phys.: Conf. Ser. 1969 012044. 10.1088/1742-6596/1969/1/012044.

[3] Hafemann, Luiz Gustavo & Soares de Oliveira, Luiz. (2017). Offline Handwritten Signature Verification - Literature Review.

[4] Hashim, Zainab&Ahmed, Hanaa M.&Alkhayyat, Ahmed Hussein. (2022).A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning TechniquesScientific Programming. 1058-9244. 10.1155/2022/8170424.

[5] S. Impedovo and G. Pirlo, "Verification of Handwritten Signatures: an Overview," 14th International Conference on Image Analysis and Processing (ICIAP 2007), 2007, pp. 191-196, doi: 10.1109/ICIAP.2007.4362778.

[6] Gideon, S. J., Kandulna, A., Kujur, A. A., Diana, A., & Raimond, K, "Handwritten Signature Forgery Detection using Convolutional Neural Networks" (2018), Procedia Computer Science, 143, 978–987. doi:10.1016/j.procs.2018.10.336.

[7] R. D. Rai and J. S. Lather, "Handwritten Signature Verification using TensorFlow," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2018, pp. 2012-2015, doi: 10.1109/RTEICT42901.2018.9012273.

[8] Z. -H. Quan, D. -S. Huang, K. -H. Liu and K. -W. Chau, "A Hybrid HMM/ANN Based Approach for Online Signature Verification," 2007 International Joint Conference on Neural Networks, 2007, pp. 402-405, doi: 10.1109/IJCNN.2007.4370990.

[9] S. Chandra and S. Maheskar, "Offline signature verification based on geometric feature extraction using artificial neural network," 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), 2016, pp. 410-414, doi: 10.1109/RAIT.2016.7507937.

[10] Alajrami, Eman & M. Ashqar, Belal A. & , Abu-Nasser, Bassem S. & , Khalil, Ahmed J. & Musleh, Musleh M. & Barhoom, Alaa M. & Abu-Naser, Samy S., "Handwritten Signature Verification using Deep Learning," 2019 InternationalJournal of Academic Multidisciplinary Research (IJAMR), 2019 pp. 39-44.

[11] Tejas Jadhav, "Handwritten Signature Verification using Local Binary Pattern Features and KNN," 2019 International Research Journal of Engineering and Technology (IRJET), 2019 pp. : 2395- 0072

[12] M. Muzaffar Hameed, Rodina Ahmad, Miss Laiha Mat Kiah, Ghulam Murtaza, "Machine learning-based offline signature verification systems: A systematic review," Signal Processing: Image Communication,Volume 93,2021,116139,ISSN 0923-5965,https://doi.org/10.1016/j.image.2021.116139.

[13] Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira, "Learning features for offline handwritten signature verification using deep convolutional neural networks," Pattern Recognition,Volume 70,2017,Pages 163-176,ISSN 0031-3203,https://doi.org/10.1016/j.patcog.2017.05.012.

[14] Rajib Ghosh, "A Recurrent Neural Network based deep learning model for offline signature verification and recognition system," Expert Systems with

Applications,Volume 168,2021,114249,ISSN 0957-4174,https://doi.org/10.1016/j.eswa.2020.114249.

[15]Y. Muhtar, W. Kang, A. Rexit, Mahpirat and K. Ubul, "A Survey of Offline Handwritten Signature Verification Based on Deep Learning," 2022 3rd International Conference on Pattern Recognition and Machine Learning (PRML), Chengdu, China, 2022, pp. 391-397, doi: 10.1109/PRML56267.2022.9882188.