PAGES: 5-11
1/3/24
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY(JSRT) VOLUME-2 ISSUE-1 JANUARY
Registered under MSME Government of India ISSN: 2583-8660

Signature Verification System Using SSIM In Image Processing

Dr. Megha Rani Raigonda[1], Shweta[2]

[1]*Assistant Professor, Department of Computer Science and Engineering (MCA), Visvesvaraya Technological University Kalaburagi, Karnataka, India. megharaigond@gmail.com*

[2]*Post Graduate Student, Department of Computer Science and Engineering (MCA), Visvesvaraya Technological University Kalaburagi, Karnataka, India shweyeganur11@gmail.com*

ABSTRACT

The verification of signatures is an essential function in several domains, including financial, legal, and administrative processes. Thanks to advancements in image processing, automatic signature verification methods have become more popular. Using structural similarities and image analysis, the proposed research offers a novel approach to signature verification. To compare and assess signatures, it uses the SSIM index. The procedure begins with pre-processing the signature pictures to improve their quality and eliminate any artifacts or noise that may have been obtained from Adobe's stock library. Then, the structural similarity between the reference signature and the input signature is calculated. The perceptual resemblance of two images is measured using structure, contrast, and brightness. The goal of the proposed research is to use this measure to record the signature's structural features and spot changes or deviations. The SSIM value that comes out of the comparison is checked against a threshold that has already been set. To validate an input signature, the calculated similarity must be greater than a certain threshold. The document is marked as suspicious or possibly falsified if it does not comply. Experimental results have shown that the method is effective in differentiating between authentic and counterfeit signatures. By doing away with the need for subjective human judgment and physical examination, this technology provides a reliable and unbiased way to authenticate signatures. Increased automation and trust in signature authentication systems are possible because to the proposed method's encouraging results in accurately differentiating genuine signatures from fakes.

Keywords: Image Processing, Algorithm Structural Similarity Index Measure, Verification

I. INTRODUCTION

Verifying the legitimacy and accuracy of papers has become critical in the digital era for many industries, including banking, law, and government. Verifying a person's signature is an essential part of document verification as it confirms their identification and helps identify possible fraud. In this setting, image processing techniques have become potent instruments for automating the verification of signatures.

This paper introduces a new method for verifying signatures using image processing principles of structural similarity. The proposed framework aims to provide a reliable and efficient approach for verifying signatures by comparing the architectural features of a given signature to those of a benchmark signature. This system promises to improve the security and accuracy of signature authentication by using a combination of advanced image processing methods and statistical assessments. It will make a significant contribution to the protection of important documents in both physical and digital forms.

Verifying a digital signature on data involves utilizing an algorithm for digital signatures and a public key. You may think of it as an authentication method.Signature verification is used to certify an individual's identity by esteemed organizations such as banks and intelligence agencies. Signature comparison is a common technique used in branch capture, especially in banks. Software for verifying signatures checks both real signatures and images of signatures against a database of previously recorded signatures. All legal transactions are authorized by the signature. Therefore, the need to verify signatures is increasing. Personal, handwritten signatures are unique and impossible to forge. Not only is signature verification a hot topic in the realms of pattern recognition and image processing, but it is also crucial in many other areas, such as privacy, security, and access control. Signature verification refers to the process of confirming an individual's identity using just their handwritten signature. There are two main types of signature verification systems [1].An electronic device, such as a tablet, is used in the Online Signature Verification System to capture information such as pressure, speed, direction, etc. Offline Signature Verification System: This system allows users to write their signatures offline and then

check them using a saved image of their signature. There are two separate ways to check offline signatures. One, called writer dependent signature verification, entails creating models of both genuine and counterfeit signatures for every writer. After that, the writer's training sample is compared to the test sample of signatures. The main drawback of this approach is that it requires the creation of a model for every new writer to be validated. The second approach, sometimes called writer-independent signature verification, is used by forensic experts and has an accuracy rate of 84%... Since it is not necessary to create a model for every writer in order to validate their signature, this method is considered the most practical. Here, a small number of authors chosen at random are used to construct a general model. The problem of writer-independent signature verification, however, is more complex because of the large morphological variance across authors [3]. 10 Signature verification has been the subject of much study and is still under investigation, particularly in its offline implementation. Since several pieces of dynamic information are unavailable when using offline verification, online signature verification has shown far greater verification rates. Consequently, verifying a signature online is usually more effective. In most cases, a signature indicates a style of writing rather than a set of letters, numbers, or phrases [4,5,6].

Here is how the remainder of the paper is structured: Work in this area is detailed in Section 2. Section 3 discusses and draws the proposed plan.Discussion of Results is shown in 4.Section 5 concludes the work and includes the cited sources.

II. RELATED WORK

An Algorithm-Based Signature Verification System We proposed a signature verification approach that uses pixel and stroke data in our study. As a basic and vital form of identification, everyone's signature is now required. Given that everyone has their own unique fingerprint, it's possible that no two people are exactly same. Not only is this verification technique unreliable in many locations, it is also absent in others. Compared to offline verification, online verification is far more effective. A combination of the pixel-based approach, the Harris algorithm, and surfing allows us to ascertain whether or not the signature is associated with a particular person. We provide our proposed method for verifying signatures with the use of pixels, strokes, etc. Easily comparing signatures is within its capabilities. Supporters of a one-signature solution may boast about how well it works, but perfect signatures on the first try aren't always achievable [7].A technique for automatically classifying signatures based on image invariants and dynamic features is proposed. Our method for validating signatures, which takes into account both the static and dynamic aspects of a signature, may be used both online and offline. A collection of scale-, rotation-, and displacement-invariant characteristics are computed for each subsegment using the proposed method in order to partition each signature into its perceptually relevant components [8].A number of computer vision and pattern recognition challenges have recently been won by deep convolutional neural networks. Due to their central role as biometrics in banking systems, administrative software, and financial applications, offline handwritten signature verification and identification is a particularly important and difficult technology. The purpose of this study is to evaluate the evidence for signature verification and recognition using deep transfer learning at the Iranian Graduate University of Advanced Technology's Department of Applied Mathematics, Faculty of Sciences and Modern Technology [9].The skill of deciphering signatures made by hand Approach using convolutional neural networks One of the most basic forms of behavioral biometrics, handwritten signature recognition is used in many authentication and identification applications. The two most common methods for detecting signatures are online and offline. The online technique is a dynamic procedure that considers the amount of pen strokes used when signing, the pace of writing, and changes in the angle of the stylus [10].Essential parts of contemporary security management include offline signature recognition and forgery detection using deep learning authentication. Strong authentication techniques are in high demand to meet various security goals, especially as human interactions with machines become more automated. [11].

III. PROPOSED METHODOLOGY

The proposed approach for verifying signatures makes use of image processing techniques, most notably the concept of structural similarity. Verifying signatures by comparing them to reference signatures stored in a database is the primary objective of this technology. Acquiring the signature picture is the first step; it is then pre-processed to improve its quality and eliminate artefacts and noise. Using techniques for image processing, the system extracts important elements from the input signature as well as the reference signature. A crucial method used is structural similarity index (SSIM), which compares the two pictures' local pixel patterns for how similar they are. For both local and global comparisons, SSIM evaluates the input signature's structural

similarity to the reference signature. As an added layer of security, the system may improve signature verification by extracting more distinguishable features using edge detection and contour inspection.

Structural Similarity Index Measure

The SSIM algorithm is crucial in determining how similar two signature pictures are in a signature verification system that uses SSIM for picture processing. SSIM is a strong metric for comparing the structural similarity of pictures by taking structure, contrast, and brightness into account. By examining both global and local features, this method decomposes the signature pictures into their component parts. The system starts by improving the quality of the signature photos and eliminating artifacts and noise in a preprocessing step. The system then calculates the SSIM index, a measure of how similar the two signatures are. An essential part of the vetting procedure is this index. While verifying, the system determines the SSIM scores for two signatures: the reference signature, which is considered authentic, and the questioned signature. A higher SSIM score indicates that the two signatures are more structurally comparable. The system then decides if the signature in question is identical to the real one, confirming the signature's validity, based on a preset threshold or machine learning models.
Schematic for an image processing-based signature verification system using SSIM. One way to forecast how people would rate various digital media, including movies and TV shows, is via the structural similarity index measure (SSIM). To find out how similar two photos are, SSIM is used. In order to assess or forecast picture quality using the SSIM index, one must start with an original, uncompressed, or distortion-free image. This is because the index is a complete reference metric. The SSIM index is an improvement over older approaches like the peak signal-to-noise ratio (PSNR) and the maximum signal-to-error (MSE) technique, which did not work with how the human brain processes visual information. Other methods, like MSE or PSNR, estimate absolute errors, which is different. The notion that nearby pixels have substantial interdependencies is known as structural information. These interdependencies provide crucial details on the visual scene's object structure. On different picture windows, the SSIM index is computed. Two windows x and y with a common size of N×N are measured by:

Mathematical Formula

$$SSIM(x,y) = \frac{(2\mu_x\mu_x+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad \text{Eq.(1)}$$

Where :

μ_x average of x μ_y average of y σ_x^2 the variance of x σ_y^2 tvariance of y

σ_{xy} the covariance of x and y

$c_1 = (k_1L)^2, c_2 = (k_2L)^2$ two variables to stabilize the division with weak denominator.

L the dynamic range of the pixel-values (typically this is $2^{\#bits\ per\ second} - 1$) $k_1 = 0.01$ and $k_2 = 0.03$ by default.

To evaluate quality, the aforementioned method is solely useful for picture brightness. From -1 to +1, the resultant SSIM index may be found. The samples must be totally real in order to get a rating of +1.
Usually, a window of 8 × 8 pixels is used to compute the measure. Although experts suggest using groups of windows to simplify the computations, the window itself may be moved by a pixel. Multiscale SSIM (MS-SSIM) is an improved version of SSIM that mimics the early visual system's multiscale processing by running it at various sizes using a multi-step downsampling procedure. Results from tests using several databases of subjective video and picture data reveal that it is on par with or even outperforms SSIM.

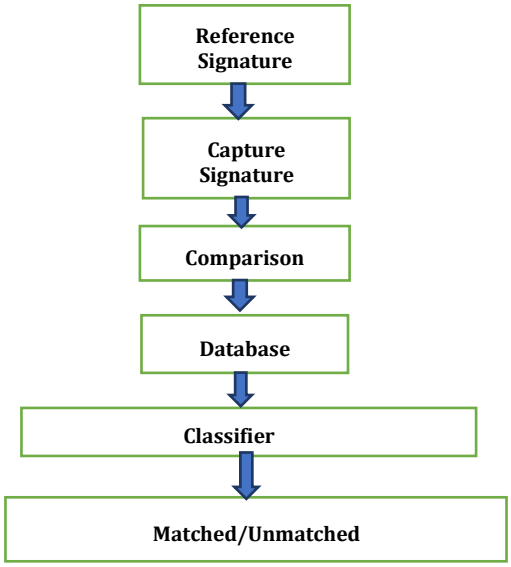

Fig 1:Block diagram of signature verification system

Methodology for signature verification system using image processing

A. Contour Detection

To find a signature on an image, we need to be able to identify its edges. In this case, I will find the areas around the signature point by using John F. Canny's Canny edge detection method. Looking at the rectangle could help us with a few things, including picking out the right form. The outlined area of the shapes has to be bigger than the rest of the shapes. The sample photo at the top appropriately encloses the signature, however there are some vacant spaces. How can we get rid of those extra spaces? Morphological methods may be used in this context.

B. Change in Appearance (Morphology)

Morphological alterations may be done to images in a variety of ways, such as removing white space, reconnecting broken pictures, thickening fonts, etc. Put simply, morphological processes are used to eliminate picture noise. Erosion, dilation, opening, and closing are the basic components. Click on this link to learn more about this idea.

C. Image Acquisition

Getting the original image is the first order of business. Devices like scanners and cameras may be used for this particular task. It is possible to quickly get the signature by scanning it from paper or using a digital input device.

D. Feature Extraction

This stage involves retrieving relevant features from the preprocessed signature image. Important features of the signature are captured by these characteristics, which include pixel intensity patterns, curvature, and stroke direction.

E. Signature Representation

The retrieved attributes are then used to construct a compressed signature representation. The goal of this representation is to accurately portray the signature's unique qualities while simultaneously simplifying the data for computing efficiency.

F. Database Management (Optional)

At this stage, it is necessary to store the digital signatures of authorized users together with their identities, in case the system uses a database of known signatures for comparison.

G. Verification Algorithm

After receiving an input signature, the verification algorithm checks it against a reference signature or a database of recorded signatures. Euclidean distance, cosine similarity, and Support Vector Machines (SVM) for classification are some of the approaches that may be used for this comparison.

H. Decision Making

It is the similarity score or the verification algorithm's output that determines if the input signature is valid or not. The intended security level of the system determines the threshold for similarity, with the goal of minimizing erroneous acceptance or rejection rates.

IV. RESULTS AND DISCUSSION

As seen in Figure 2, the suggested method makes use of matching signature photos. Scanned signature images may be compared to template signature images using SSIM in a signature verification system. A greater SSIM score indicates a higher degree of similarity between the two pictures. You may use this to check whether the scanned signature is real or fake. When it comes to signature verification systems, SSIM is a necessary component. For the majority of your signature verification system implementation and experimentation, you should use Python. Picture databases in case you're working with GPDS or SVC datasets, which are particular to signatures.While react might be a useful tool for building an intuitive front end or web-based interface to showcase your signature verification system's findings, it wouldn't form the backbone of your image processing or verification infrastructure.

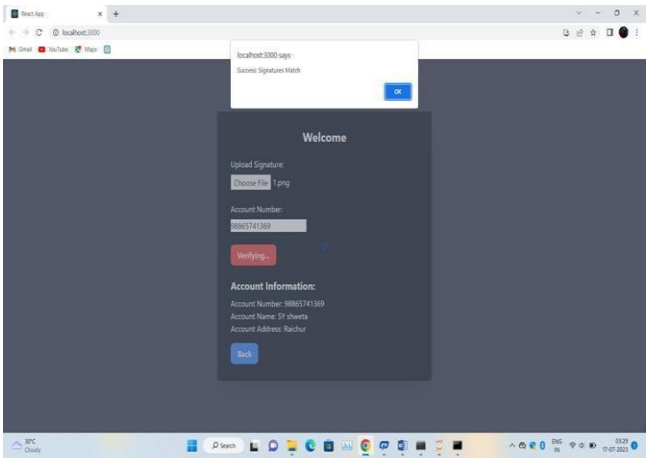

Figure 2: signature match for signature verification system

- Before processing either the scanned signature image or the template signature picture, noise and artifacts are removed.
- When comparing the scanned signature to the template signature, the SSIM value is determined.
- The value is set to a threshold. The scanned signature is deemed authentic if the SSIM value exceeds the threshold value. If it doesn't, it's probably fake.

As seen in Figure 3, the suggested method is to avoid matching signature photos. The image processing signature verification system that used SSIM did not match. In other words, the algorithm failed to detect a match between the two signatures. A few of explanations might be at play here:

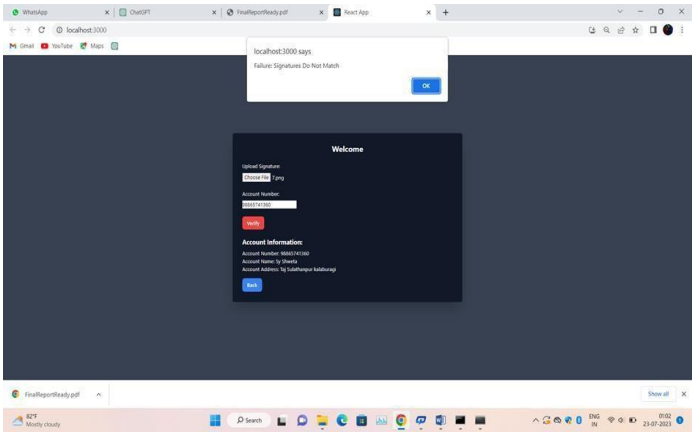

Figure 3:Signature do not match for signature verification system

- It is possible that the signatures were too dissimilar.
- Maybe the signatures weren't good enough for the system to use for feature extraction.
- It is possible that the system was not taught correctly or was misconfigured.

V. CONCLUSION AND FUTURE WORKS

An invaluable asset in the field of signature authentication has been the creation and deployment of a signature verification system that use the Structural Similarity Index (SSIM) in image processing. Image processing, one of the most popular and cutting-edge fields right now, was used in this research to compare signature images, matched signatures, and non-matching signatures. As a result of this initiative, signature verification is now more accurate, easier, and quicker while also reducing the likelihood of human mistake. Customers will feel much more safe and trusted if no organization implements this approach since it makes the task simpler to comprehend and execute. Therefore, we argue that this system alters the way a number of financial institutions, businesses, etc. operate. The combination of signature photos with additional biometric data, such as handwriting dynamics or behavioral patterns, might lead to more secure and resilient authentication methods in the future. This kind of technique could be the subject of future research.

REFERENCES

1. Forgery detection by local correspondence, J. K. Guo. PhD dissertation, 2000, College Park, Maryland, USA. Azriel Rosenfeld is the director.
2. A study of biometric technology with a look at trends and opportunities by J. A. Unar, W. C. Seng, and A. Abbasi. (2014).
3. Devansh Priye, & Sumit Sangwan. (2023). A Study of Students Stock Market Participation and Awareness. Journal of Scientific Research and Technology, 1(8), 70–90. https://doi.org/10.61808/jsrt73
4. Dr. Shubhangi D C, Dr. Baswaraj Gadgay, & S. Anita. (2023). Leverage Machine Learning To Infer Proof of the Nipah Influenza. Journal of Scientific Research and Technology, 1(9), 13–20.
5. "Off-Line Persian Signature Identification and Verification based on Image Registration and Fusion", Journal of Multimedia, vol. 4, pp. 137-144, 2009. S. Ghandali and M. EbrahimiMoghaddam.
6. Mohammed Maaz, Md Akif Ahmed, Md Maqsood, & Dr Shridevi Soma. (2023). Development Of Service Deployment Models In Private Cloud. Journal of Scientific Research and Technology, 1(9), 1–12. https://doi.org/10.61808/jsrt74
7. Mr. Praveen Hipparge, & Dr.Shivkumar S. Jawaligi. (2023). Design Problems in Cognitive Radio Networks for Spectrum Sensing. Journal of Scientific Research and Technology, 1(8), 64–69. https://doi.org/10.61808/jsrt72

8. Griechisch E, Malik MI, and Liwicki M: Online Signature Verification using Accelerometer and Gyroscope Proceedings of the 16th Biennial Conference of the International Graphonomics Society, January 2013, pp. 143-146. El-Sayed A. El-Dahshan, Heba Mohsen.
9. Antariksh Sharma, Prof. Vibhakar Mansotra, & Kuljeet Singh. (2023). Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning. Journal of Scientific Research and Technology, 1(6), 174–187.
10. Mrinalini kakroo, & Vibhakar mansotra. (2023). Automatic Segmentation of liver Tumor using Deep Learning. Journal of Scientific Research and Technology, 1(5), 100–113.
11. Biometric Authentication Using Online Signatures by A. Kholmatov and B. Yanikoglu. Pages 373–380 in Berlin and Heidelberg: Springer Berlin Heidelberg, 2004.
12. Riaz Ahmad, KiranBibi, Saeeda, Naz, and Saeeda. DeepSignature: a refined transfer learning-based solution for verifying signatures 38113–38122 in Multimedia Tools and Applications 81.26 (2022).
13. Dr. Rekha Patil, Bhavana Y, Bhavani Rathod, & Naina Gupta. (2023). Rental And Loan System In Agriculture Using Blockchain Technology. Journal of Scientific Research and Technology, 1(3), 1–14.
14. Hassina Kouser, & Prof. Vibhakar Mansotra. (2023). Deep Learning-Based Segmentation Of Brain Tumor. Journal of Scientific Research and Technology, 1(5), 78–91.
15. Using image invariants and dynamic features, Abdullah I. AlShoshan's computer science department at Qassim University verified handwritten signatures in 2006 (CGIV'06). 14 August 2006, $20.00, ISBN 0-7695-2606-3 IEEE.
16. Dr. Rekha J Patil, Indira Mulage, & Nishant Patil. (2023). Smart Agriculture Using IoT and Machine Learning. Journal of Scientific Research and Technology, 1(3), 47–59.
17. Gaurav Prajapati, Avinash, Lav Kumar, & Smt. Rekha S Patil. (2023). Road Accident Prediction Using Machine Learning. Journal of Scientific Research and Technology, 1(2), 48–59.
18. Offline Signature Recognition and Forgery Detection Using Deep Learning, Jivesh Poddara, Vinanti Parikha, and Santosh Kumar Bhartia [11] April 6 - 9, 2020.