International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 12, Issue 9 [September. 2023] PP: 31-38

Fake Signature Detection Using Neural Networks

Ashish Kumar Srivastava[1], Dr.Tauseef Ahmad[2], Jay chand[3]
[1]*Ph.D.Scholar Department of Computer Science & Engineering, MPU Bhopal (M.P) India*
[2 3]*Assistant Professor*
[2]*Department of Information Technology, REC Azamgarh (U.P) India*
[3]*Department of Information Technology IIMT College of Engineering Greater Noida (U.P) India*
[1]*hiashish2006@gmail.com*, [2]*tauseefahmad@zhcet.ac.in*, [3]*jaychandvbs04@gmailcom*

Abstract:
The widespread use of signatures as a means of personal identification highlights the need for authentication. Depending on the application, the verification can be done offline or online. The online transaction uses dynamic signature information when signing. The scanned image of the signature is processed by the offline system. We try to identify offline signatures using a set of geometric shapes. Valid parameters are base slope, aspect ratio, static area, center of gravity, number of edge points, number of intersection points, and center of gravity of connection slope two parts of the picture. Before feature extraction, scanned images must be preprocessed to separate signatures and remove visual noise. The system is initially trained using a database of signatures obtained from individuals whose signatures will be verified by the system. The average signature is obtained by combining the above features from all real signature tests. This average signature is used as a signature test. In this article, we describe how this problem has been addressed over the past few years, recent advances in the field, and possible directions for future research.

Keywords:
Signature confirmation, Picture Preparing, Counterfeit Neural Arrange, Pre-processing, Highlight Extraction, Back Diffusion, histogram of arranged angles.

Date of Submission: 02-09-2023 Date of acceptance: 13-09-2023

I. INTRODUCTION:

Authorization for all legal transactions is done by signature. Therefore, the need for signature verification increases. Lists are unique and cannot be reproduced. Technology is easy to understand and believe. Article The main advantage of signature verification over other forms of expression is that the signature is considered a means of authentication. There are two ways to write a signature, online and offline. The online method uses electronics and computers to extract signature and dynamic information. Height, speed, writes speed, etc. for identification purposes. Offline Signature Proof Contains low power management and signature image captured by scanner or camera.Offline signature verification platforms use highlights extracted from verified signature images. The operations used for offline signature verification are very simple. All you need to do is evaluate the image pixel by pixel. Reserving independent frameworks can be problematic because many essential features such as bit rate, rate and other energy data are not available in independent frameworks. Verification readiness depends entirely on key points that can be extracted from the next inactive signature image. Various strategies have been used and continue to attract interest in the field of handwritten signature verification (HSV), particularly standalone HSV.

PROBLEM STATEMENT:

Automatic signature verification problems often develop as verification problems. Train the model given a training L with real customer signatures. This model is used for authentication. User requests ID and provides new signing question X. Standards are used to classify signatures as genuine (keep what you think) or fake (created by someone else). To evaluate the effectiveness of the system, consider an index T containing real and fake signatures. Signatures are obtained during registration, which is the second step of the pseudo operation (or deployment).

II. LITERATURE SURVEY:

Vigorous research has been done in handwriting analysis and pattern matching for many years. In the field of handwritten signature verification (HSV), especially offline HSV, various techniques have been used and this area is still being explored. In this section we review some recent papers on offline HSV.

The approaches used by different researchers differ in the type of features extracted, the training method, and the classification and validation models used.

Hidden Markov Models Approach:
Hidden Markov Models (HMM) are one of the most widely used models for sequence analysis in signature verification. A handwritten signature is a vector of values corresponding to each signature point along the path. Therefore, a well-chosen set of feature vectors for HMM can lead to the development of efficient signature verification

Systems. These models are probabilistic models that can absorb variability and similarity between models. HMM includes probabilistic matching (model and signature). This matching is done using the steps of the probability distribution of the features included in the signature or the probability with which the original signature was computed. Judging by the check results, it's most likely not a signature. That is, the signature belongs to the original person, otherwise the signature is rejected. HMM is used to model each author's signature. This method gives an AER of 18.4% for a set of 440 real signatures from 32 authors and 132 experienced forgers.

Neural Networks Approach:
Control and ease of use are the main reasons for the widespread use of neural systems (NNs) in design recognition. The basic approach is to first separate the signature-related set of inclusions (points of interest, such as length, height, duration, etc.) into multiple tests of multiple endorsements. The NN's immediate action is to remember the connection between the caption and the class ("from honesty to goodness" or "fraudulent"). When this relationship is known, the structure can be marked with a check mark that can be classified as having a location for a particular signature. Therefore, NNs are suitable for modeling the global view of handwritten characters. The proposed structure includes structural highlighting of the signature layout, adjusted headline highlighting and additional highlights such as surface area, length gradient and center of gravity highlight, the signature is divided into two parts and center of gravity position is calculated for each half. Even points are mentioned. Two approaches to classification and assertion, flexible inverse generation (RBP), neural organization and spiral basis work (RBF), are compared, using a database of 2106 estimates containing 936 honest and 1170 mimics. These two classifiers have 91.21% and 88% approval respectively.

Template matching approach:
Two fraud detection methods have been proposed using matching models by Fang et al. One is based on the similarity of the contours in the 1D projection of the signature model and the other is based on the matching of veins in the 2D signature model. To test it, we run a signature test, compare the differences between locations to training data, and make decisions based on distance measurements. I tested both binary and grayscale signed images. Comparing all predictions from the various matrices with local peaks in the profile of the vertically projected grayscale image of the signature, the average validation error rate was 18.1%.

Statistical approach:
Correlation between two or more pieces of data, biased etc. Historical knowledge makes it easy to discover. To find relationships between data sets, we usually follow the concept of a correlation coefficient. Generally, statistics means separating two independent variables. Method following the concept of correlation to find the difference between them, to determine the recorded signature with the help of the average signature obtained from the previous recording operation. Many features are extracted this way, including general features (for example, image gradients), statistical features derived from signature pixel distributions, and local responses to signature markers (for example, geometric and terrain descriptors). Distribution involves obtaining a different signature from the same author and obtaining distribution at a remote location. Section is being harassed. This method uses only 4 real samples for learning and the accuracy is up to 84% and the accuracy can be increased to 89% with the increase of the real name of the samples. The method does not use fake signatures in education/learning.

Support Vector Machine:
An auxiliary vector machine (SVM) is a machine learning computation that uses high-dimensional space and evaluates the contrast between classes in a given data set in order to generalize hidden information. The system uses globally directed basic functions of marks and SVMs for classification and approval. A database of 1320 stamps by 70 authors was used. There are 40 creators used in preparation, each with 8 levels, so a total of 320 levels are prepared. For initial testing, the approach uses 8 unique labels and 8 mocks and achieves a FRR of 2% and a distance of 11%.

EXISTING SYSTEM AND DRAWBACKS

Many researchers have been analyzing images that match handwriting for years. Various methods have been used in the handwritten signature verification (HSV) field, especially in the offline HSV field, and this field is still being researched. It takes more time to differentiate between real and fake.

The main drawback of signature verification is that it uses large data sets for greater accuracy.

Sometimes fake signatures also look like originals, so it takes longer to verify original and fake signatures.

PROPOSED SYSTEM

We show demonstrate in which a Neural Organize classifier is utilized for verification. Signatures from database are pre-processed earlier to highlight extraction. Highlights are extricated from the pre-processed signature picture. These extricated highlights are at that point utilized to prepare a neural network. In confirmation organize, on test marks pre-processing and include extraction is performed. These extricated highlights are at that point connected as input to a prepared neural arranges which can classify it as an honest to goodness or manufactured signature.

Pre- processing:

The signature is first captured and converted into a computer-readable format. It is now ready for preprocessing. In the first step, the RGB signature image is converted to a gray image and then a binary image. First steps include:

Denoising:

One of the main problems in the field of image processing and computer vision is image noise; the main purpose of the image is to limit the noise in the image version that has been deconstructed to get it closer to the original image. Image noise can be caused by a variety of internal (eg sensor) and external (eg sensor) causes. Environment) conditions are usually not available in the concept case. An Alternative Approach to Image Denoising Problems Based on Markov Chain Monte Carlo Sampling for Data Adaptive Stochastic Optimization.

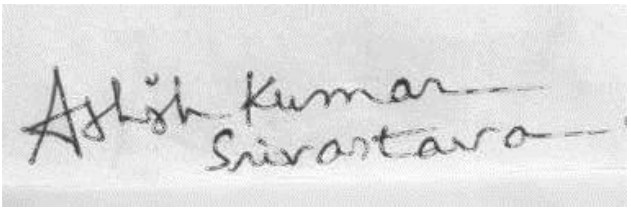

Fig: Before Denoising

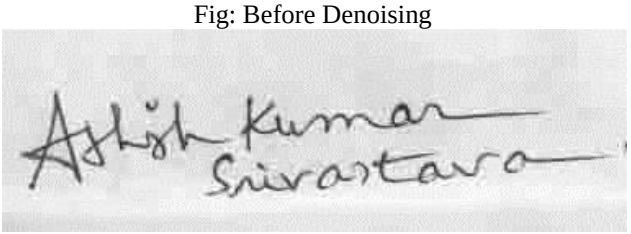

Fig: After Denoising

Color invention: Convert true-color RGB images to grayscale images for use with saturation data while preserving brightness.

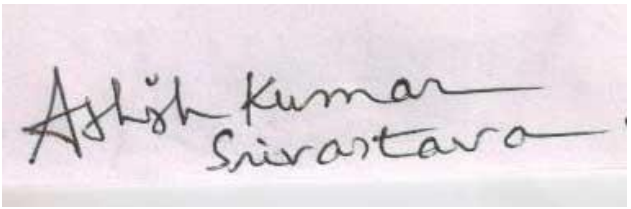

Fig: A sample signature to be processed

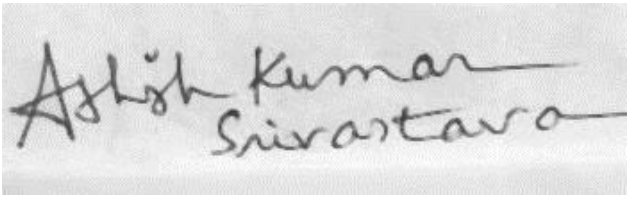

Fig: A Gray intensity image

Grayscale Images: A grayscale image is a matrix of data whose values represent multiple uses, and each element of the matrix corresponds to a pixel in the image the one with shades of gray. What distinguishes such images from other types of color images is that less information must be provided for each pixel. In fact, "gray" is the same color in RGB space as red, green, and blue, so each pixel should only be assigned one reference value, which is not an effort required. Each pixel is represented as a whole, shown as color pictures.
Grayscale images are very common, as most modern displays and image capture hardware can only support 8-bit images. Grayscale images are also well-suited for many applications, eliminating the need for more complex and difficult-to-process color images.

Image Filtering and Binarization:
After resembling, all images are filtered with a low-pass FIR filter. This is done to prevent aliasing. This aliasing occurs because the data is sampled at more than twice the frequency of the highest frequency component of the data. A low-pass filter therefore removes the high-frequency components of the image. That's what filters are for. The grayscale image is now segmented to create a binary image of the object. In a binary image, each pixel takes only one of two values, 1 or 0. Binary images are stored as logical arrays.

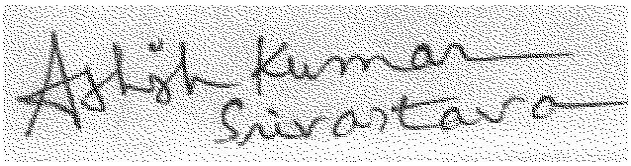

Fig: Binary Image interpreting the bit value of 0 as black and 1 as white

Future Extraction:
We experimented with two different features: a histogram of the HOG (directional gradient) for the dominant direction and a local binary pattern.
Histogram of oriented gradients (HOG):
The histogram directional slope (HOG) is used to represent factor sizes presented by Dalal and Triggs at the 2005 CVPR conference. HOG stands for histogram of directional slope and is mainly used for human detectors. In this study, HOG is used as a feature extraction method to identify and authenticate signature images.

Gradient Computating:

The first step in computing the various feature detectors in image preprocessing is to provide normalized color and gamma values. However, as suggested by Dalal and Triggs, when calculating the HOG annotations, this step can be skipped as the annotations give the same result after normalization. So image preprocessing has very little performance impact. Alternatively, the first step in the calculation is to compute the gradient value. It's best to use a one-dimensional basis that shows the difference between the mask both horizontally and vertically. The process should specifically filter color images or data using the following filters: on the photo. I also used Gaussian anti-aliasing before applying the mask, but once again found that removing the anti-aliasing almost improved performance.

Orientation Binnig:

The second step in the calculation is to create a cell histogram. Each pixel in the cell votes for a weight in the direction-based histogram based on the value found when calculating the slope. The cell itself can be either rectangular or radial, and the histogram ranges from 0 to 180° or 0 to 360°, depending on whether the gradient is "unsigned " or" signed. " Dalal and Triggs found that unsigned gradients combined with nine histogram channels performed best in human perception experiments. A pixel's contribution in terms of voting weight can be either the size of the gradient itself or a function of its size. In experimentation, the magnitude of the gradient itself usually gives the best results. Other options for voting weights might include the square root or square of the gradient value or some truncated version of the value.

Descriptive Blocks:

Accounting for changes in illumination and contrast requires locally normalizing the strength of the gradient, which requires grouping cells into larger spatially related blocks. The HOG descriptor is the concatenated vector of normalized cell histogram components of all block regions. These blocks usually overlap. This means that each cell contributes more than one to the final descriptor. There are two basic block geometries: R-HOG rectangular blocks and C-HOG circular blocks. R-HOG blocks are usually square grids represented by three parameters: the number of cells in the block, the number of pixels in the cells, and the number of channels in the cell histogram. A C-HOG block can be described by four parameters: the number of corners and radial bins, the center radius, and the expansion factor for the radius of additional radial bins.

Fig: Offline signature sample as biometric

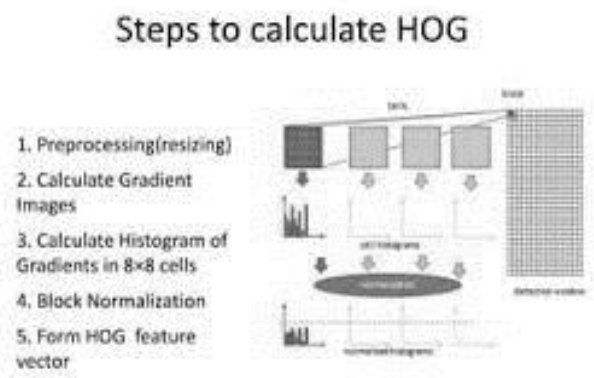

Fig: Demonstrate the HOG algorithm

Object recognition: HOG descriptors may be used for object recognition by providing them as a feature of a machine learning algorithm. Dalal and Triggs used HOG descriptors as features in a support vector machine (SVM) [However, HOG descriptors are not tied to a specific machine learning algorithm. Note that while complex features give more information, simple features such as gradient orientation are more robust to normal variations found in a signature.

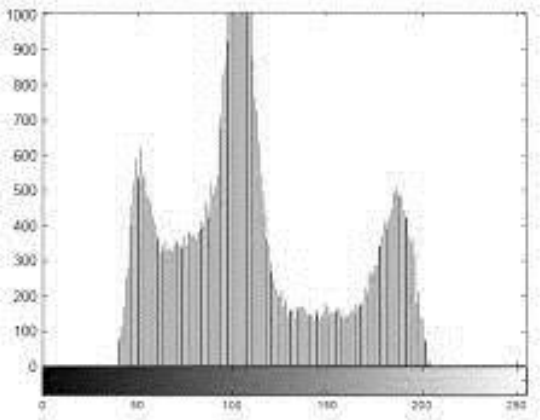

Fig: Histogram of Image pixel

5.3 ANN Training:

Artificial Neural Network or ANN resembles the human brain in learning through training and data storage.

The ANN is created and trained through a given input/ target data training pattern. During the learning process, the neural network output is compared with the target value and a network weight correction via a learning algorithm is performed in such a way to minimize an error function between the two values.. The mean-squared error (MSE) is a commonly used error function which tries to minimize the average error between the network's output and the target value.

Twelve exact signatures and twelve forged signatures train the network and they were enough to give very good results in verification.

The table contains all the information related to the design of the neural network. Both original and fake signatures are used to train the network. Trial signatures are also available.

Parameter	**Value**
Number of layers	2
Number of neurons Output layer	1
Number of inputs	12
Learning rate	Default
Transfer function First layer	Sigmoid
Transfer function second layer	Sigmoid
Initial weights	Randomized
Initial biases	Randomized
Max number of epochs	1000
Error goal	0.0001
Number of patterns for original signature	12
Number of patterns for fake signature	12
Number of tested signatures	24
Number of tested original signatures	12
Number of tested fake signatures	12

Table: Neural Network Specification

Visualization of Result:
Through the following interface, the user can select the signature image of interest from the available database. Then train the network with the contents of this database and a' Matched' or' Not Matched' status that indicates whether the signature is accurate or forged.

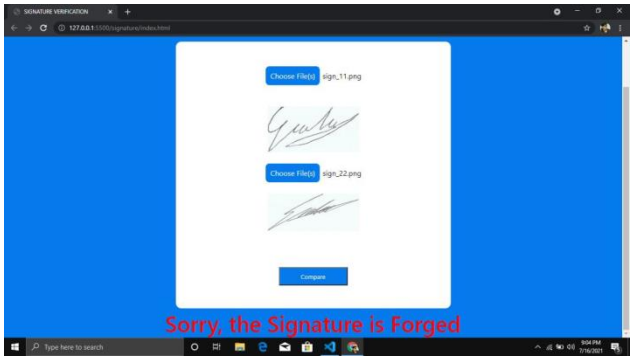

Fig: Output Screen

Fig: Output Screen

III. CONCLUSION:

Neural networks have found success in many applications due to their relative ease of use and ability to solve specific problems by exploiting their model-less properties. One of the key features that can be attributed to ANNs is their ability to learn nonlinear problems offline via selective learning, giving fairly accurate answers. The application of artificial neural networks (ANNs) to the above problems has become important primarily due to the efficiency of modern computers. Additionally, simulation and testing time for ANN applications is minimized. And ANN-based verification systems can learn different types of signature data sets. Also, this type of task does not require the use of big data to demonstrate the ability to learn, it only selects 12 real signatures and 12 fake signatures for training, with very good results. However, for practical use, large training data can improve system reliability. After training, we achieved the best classification accuracy. The classification rate is over 93%. The algorithm we endorsed uses simple geometric functions to characterize signatures and works well to classify signatures as genuine or fake. The system is robust and can detect arbitrary, simple and counterfeit counterfeiting. Since we don't know how to copy a signature enough to be considered an effective forgery, we don't have a clear idea of its effectiveness in the case of highly skilled counterfeiters.

FUTURE WORK

In terms of feature work, this project will be implemented and a better training and verification method will be selected to improve the accuracy of the offline signature verification system in the future implementation phase.

REFERENCES:

[1]. N. Dalal and B. Triggs. Histograms of oriented gradients for human detection. In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Volume 1 - Volume 01, CVPR '05, pages 886–893, Washington, DC, USA, 2007. IEEE Computer Society.

[2]. T. Ojala, M. Pietikainen, and D. Harwood. Performance evaluation of texture measures with classification based on kullback discrimination of distributions. pages A:582–585, 1998.

[3]. J. F. Vargas, M. A. Ferrer, C. M. Travieso, and J. B. Alonso. Off-line signature verification based on grey level information using texture features. Pattern Recogn., 44:375–385, February 2015.

[4]. M. A. Ferrer, J. B. Alonso, and C. M. Travieso. Offline geometric parameters for automatic signature verification using fixed point arithmetic. IEEE Trans. Pattern Anal. Mach. Intell., 27(6):993–997, 2005.

[5]. C. M. T. J. B. Francisco Vargas, Miguel A. Ferrer. Off-line handwritten signature gpds-960 corpus. In IAPR 9'th International Conference on Document Analysis and Recognition, pages 764–768, September 2009.

[6]. J. K. Guo. Forgery detection by local correspondence. PhD thesis, College Park, MD, USA, 2010. Director-Rosenfeld, Azriel.

[7]. Wikipedia.https://en.wikipedia.org/wiki/Artificial_neural_network

[8]. Alexander Wong, Stochastic image denoising based on Markov-chain Monte Carlo sampling

[9]. "Histograms of Oriented Gradients for HumanDetection",http://lear.inrialpes.fr/people/triggs/pubs/Dalalcvpr05.pdf

[10]. M. Trikha, M. Singhal, and M. Dutta, "Signature Verification using Normalized Static Features and Neural Network Classification," International Journal of Electrical and Computer Engineering, vol. 6, no. 6, pp. 2665, 2019.
[11]. M. Singhal, M. Trikha, and M. Dutta, "Time Independent Signature Verification using Normalized Weighted Coefficients," International Journal of Electrical and Computer Engineering, vol. 6, no. 6, pp. 2658, 2021.