Offline Signature Recognition and Verification using Neural Network

[1]Dhananjay Rakshe, [2]D. B. Kshirsagar
[1]Student, [2]Professor
[1]Department of Computer Engineering,
[1]SRES College of Engineering, Kopargaon, Maharashtra, India

***Abstract* - Computers have become common and are used in almost every field including financial transactions, so it's necessary to provide additional security measures. Considering consumers' expectations, these security measures must be reliable, cheap and un-intrusive to the authorized person. This technique of signature recognition has advantage over the other biometric techniques like voice, iris, fingerprint etc. as it is mostly used for daily routine procedures like document analysis, banking operations, access control, electronic funds transfer etc. Most importantly, people are less likely to object it because its easy. The technique described in this paper uses neural network which enables the user to recognize whether a signature is original or a fraud. Scanned images are introduced into the computer, their quality is modified with the help of image enhancement and noise reduction techniques, specific features are extracted and neural network is trained. The different stages of the process involve image preprocessing followed by feature extraction and pattern recognition through neural networks. This method will be more efficient and provide more accurate results than the existing techniques.**

***Index Terms* - Feature Extraction, Neural Network, Back Propagation Algorithm, Signature Verification.**

I. INTRODUCTION

In the business world we sign things such as accounts and other official documents. Personal signatures lend themselves well for biometric verification in state-of-the-art electronic devices. Unfortunately, one disadvantage of signature is that individuals don't perpetually sign documents in only identical manner. Just like the angle at that they sign could also be totally different owing to seating position or owing to hand placement on the writing surface. Also other affecting factors can be different inks used to make signature, variety of pens but these things can be eliminated with the help of image enhancement and noise reduction techniques.

In this era of automation, automatic person identification is a major challenge, not that it's a new problem to the society but with this significant development of internet; interactions are becoming more and more automatic and thus the problem of identity of individual has become more important. Handwritten signatures are most easy and preferable because they are used to carry out daily transactions, every individual's signature is unique, they are less controversial and people are less likely to object it.

There are many existing systems and studies based on different methods of verification and recognition. It mostly depends on what kind of features you're extracting and how the neural network is trained. Features like Eccentricity, orientation, kurtosis [1] have been used. False acceptance rate (FAR) and false rejection rate (FRR) are calculated and used as quality performance measures [2] to evaluate performance of the system. Extraction method based on grid features [3] had FRR of 10.8% and FAR of 13.5%. These systems extracted various static and dynamic features [4] and used them to train neural network.

According to the studies that were done on signatures and types of signatures, forged signatures [1] fall into following three categories:

Random: These signatures are not based on any knowledge of the original signature. Forger does not know how the original signature looks like or how it's made, Signature is usually random and can be easily identified as fake.

Simple: Based on an assumption of how the signature looks like by knowing the name of the signer. If the name is known, the possibilities are limited about how the signer would have made his sign. As most of the people have habit to write their name, the chances of faking a signature are increased.

Skilled: An imitation of the original signature, Forger knows exactly how the original signature looks like. Therefore, a perfect imitation can be made if the forger is good at copying.

It appears that the skilled signatures are the most difficult ones to detect as they can be very similar to the original signature and the error rate might be very small.

II. System Overview

The system mainly focuses on following areas-

- Image Pre-processing
- Feature Extraction
- Neural Network Training

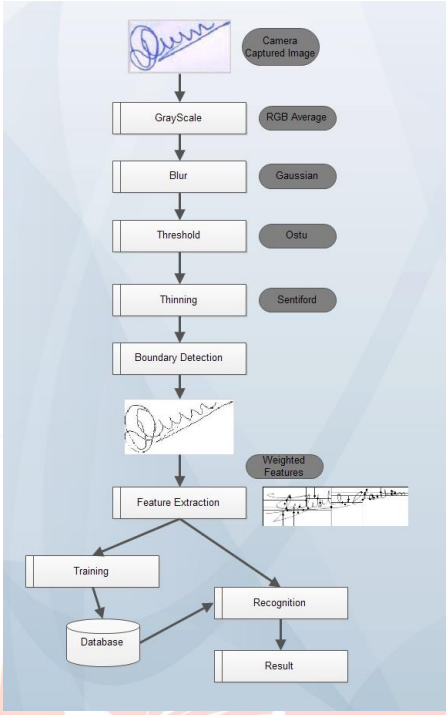

Figure 2.1: System Overview

Figure 2.1 shows the offline signature recognition and verification system. As illustrated in the design, Scanned signature is taken as an input (using camera or scanner) and is provided to the system for pre-processing. Image will be processed using different image enhancement and noise reduction techniques. These techniques involve converting input image into gray scale format, making it smoother to deal with sharpness, converting the image into black and white image, detecting boundaries to remove unnecessary portions of image and finally thinning the image. Reason behind using these techniques is to enhance the image to a suitable form so that it can be properly used. As different people make signatures in different ways, pens and ink used to create these signatures varies too. So it becomes essential to enhance the input image first. Next step involves extracting different types of features from the input image and storing them in the database for future use. These features are used for comparison with the features that will be extracted from input signatures while authenticating them. Meanwhile, they are also used to train the neural network. When the neural network is successfully trained, it can be used in recognition process to authenticate whether provided signature is authentic or a forgery.

III. Signature Recognition and Verification

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Image Preprocessing

Image pre-processing has a wide range of techniques that exists for the manipulation and modification of images. It is the first step in signature verification and recognition. This step ensures improved results and higher accuracy rates. Reasons about why image pre-processing is important are stated as follows:

- Level of similarity is achieved in the general features of an image, this helps enhancing the comparison between images.
- Signatures vary according to the tool that was used in writing; the type of pen/pencil, the ink, the pressure of the hand etc. These facts should be eliminated as they're not important in off-line signature recognition.
- Removal of defects, noise reduction and enhanced image.
- Quality of image information is improved.
- Simplicity in the process of feature extraction on which the matching mainly depends.

Image pre-processing techniques used:

RGB average: RGB average algorithm is used to convert an image into gray scale format. This method separates Red, Green and Blue values from 24 bit image and gray scale component is calculated by taking average. Every original pixel value is then replaced with its gray scale component.

Otsu (threshold): Pixel intensity ranges from 0 to 255. User defined threshold is used to compare pixels and accordingly black or white values are assigned to them depending on the background required to achieve pure black and white image.

Stentiford (thinning): Thinning is the most important part and can be done successfully using Stentiford algorithm. To do so, first signature image is gray scaled and binarized. Then the pixel locations that can be erased are found and erased.

Feature Extraction

Objective of this phase is to extract the features [5] of the test image that will be compared to the features of training image for verification purpose. Feature extraction technique is based on selecting 60 feature points from the geometric center of the signature and comparing them with the already trained feature points. This method can take care of skilled, simple and random forgeries. Also we can reduce the two vital parameters- False Acceptance Rate (FAR) and False Rejection Rate (FRR) which are normally used in any signature verification scheme.

Feature Extraction: The geometric features are based on two sets of points in two-dimensional plane. Vertical splitting of the image provides thirty feature points (v1, v2,, v30) and the horizontal splitting provides thirty feature points (h1, h2,.,h30). These feature points are obtained relative to a central geometric point of the image. Image is scanned from left to right and total number of black pixels is calculated. Similarly the image is scanned from top to bottom and total number of black pixels is calculated. Then image is divided into two halves w.r.t. the number of black pixels on two lines vertically and horizontally which intersects at a point called the geometric center. By referring this point we can extract 60 feature points: 30 vertical and 30 horizontal feature points of each signature image.

The geometric features are based on two sets of points in two-dimensional plane. Each set having thirty feature points which represents the stroke distribution of signature pixels in image. Total sixty feature points can be calculated with the help of geometric center. They can be retrieved with 2 main steps namely Vertical Splitting and Horizontal Splitting.

The procedure for finding vertical feature points is stated as follows.

1) Use a vertical line passing through the geometric center (v0) to divide the image into two halves: Left part and Right part.
2) Find the geometric centers v1 and v2 for the left part and the right part respectively.
3) Use horizontal lines to split left and right parts through v1 and v2 to divide them into four parts: Top left, Bottom-left and Top-right, Bottom- right parts from which we obtain v3, v4 and v5, v6.
4) We again split each part of the image through their geometric centers to obtain feature points v7,., v14.
5) Then we split each of the parts once again to obtain all the thirty vertical feature points (as shown in Fig. 3.1).

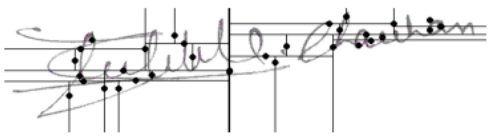

Figure 3.1: Vertical Splitting of Signature Image

To find horizontal feature points:

1) Use a horizontal line passing through the geometric center (h0) to divide the image into two halves: Top part and Bottom part.
2) Find geometric centers h1 and h2 for top part and bottom part respectively.
3) Use vertical lines passing through h1 and h2 to divide the two parts into four parts: Left-top, Right-top and Left-bottom, Right- bottom parts from which we obtain h3, h4 and h5, h6.
4) We again split each part of the image through their geometric centers to obtain feature points h7,., h14.
5) Then we split each of the parts once again to obtain all the thirty vertical feature points (as shown in Fig. 3.2).

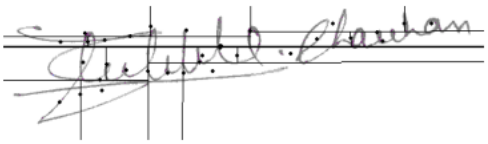

Figure 3.2: Horizontal Splitting of Signature Image

These extracted features can be provided as an input to the neural network for training purpose.

Neural Network Training

Neural networks are known for being a very accurate and efficient technique for pattern recognition in general. We can see the idea and structure of neural networks, their types, and how they contribute to pattern recognition.

A neural network is one application of artificial intelligence, where it's trained to think like a human being or even better. A neural network is an information processing paradigm that is inspired by the way biological nervous systems like brain processes the information. The key element is the structure of the information processing system. It constitutes of a large number of processing elements (neurons) that are highly interconnected and work in unison to solve specific problems.

Neural networks - like human beings - depend on the idea of learning in order to achieve any task. They learn through training on a large number of data, which enables them to create a pattern with time, that they will use later. They are very helpful in detecting patterns that are complicated and hard to derive by humans or by simple techniques. Just like the case of signature recognition, it's hard to tell whether a signature is original or forged, especially if it is carried out by a skilled forger. So it requires more advanced techniques to detect the differences needed to achieve a decision on its authenticity. Neural networks do not follow a set of instructions, they learn case by case.

Neural networks are highly reliable when trained using a large amount of data. They're useful in applications where security is highly valued. We can use multilayer Perceptions MLPs neural network. The structure of this neural network depends on the multilayer feed forward, where all the nodes in any layer have connections to all the nodes in the next layer and so on, but these nodes do not have any connections with the previous layers. It can be modified to function as a back-propagation neural network with the help of Back-Propagation algorithm. The implementation of back-propagation learning updates the network weights and biases in the direction in which the performance function decreases most rapidly, the negative of the gradient. The equation for one iteration can be written as follows-

$$X_{k-1} = X_k - \alpha_k Y_k \qquad (1)$$

Where Xk is a vector of current weights and biases, Yk is the current gradient and αk is the learning rate. The gradient is computed and the weights are updated, after each input to the network.

The network can be trained using the set of data available in the database as an input to input layer, which includes the images and their extracted 60 features points. The output layer consists of a single node that calculates the weighted sum of the connections coming to the output layer. The total number of the neurons in the hidden layer is double of the neurons in the input layers so that the network can learn the technique of recognition based on these previously mentioned features.

The final output from MLPs networks is a confidence value indicating the likelihood that the test signature was performed by the same person that provided the reference signatures used in training. The confidence value is compared to a threshold and the test signature is verified. If the confidence value exceeds this threshold it is accepted or otherwise it is rejected. Then the classification rate or the error can be calculated in percentage rate.

Recognition

The following steps provide details on how the recognition process operates:

- During the training of neural network it learns how to work on signatures and their features and then compares the features of the given signature with those of the signatures in the database.
- The differences between the extracted features from the new signature and those in the database are calculated.
- Signature with minimum differences is then returned with its corresponding tag and a number showing the percentage of similarity.
- Similarity percentage can be used to decide whether the signature is original or not.
- If the percentage of similarity ranges between 85-100%, the signature is considered original. This is based on the natural signature recognition method, which assumes that there are natural differences in the signature of a single person.
- If the similarity percentage ranges between 75-85%, the signature is considered relatively suspicious.
- If the similarity percentage is lower than 75%, the signature is considered highly suspicious.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

Image Pre-processing is necessary in order to obtain an enhanced image in a suitable form for further processing. Image is passed down as an input to algorithms like Gray scale conversion, threshold, thinning to enhance it and remove any noise. Then the image is provided as an input to the next module which is feature extraction.

Results of image enhancement and noise reduction techniques can be seen in following screen shots. Fig. 4.1 illustrates threshold image i. e. pure black and white signature and Fig. 4.2 shows a thinned signature where all the unnecessary pixels are erased. Fig. 4.3 represents features extracted from the processed signature image.

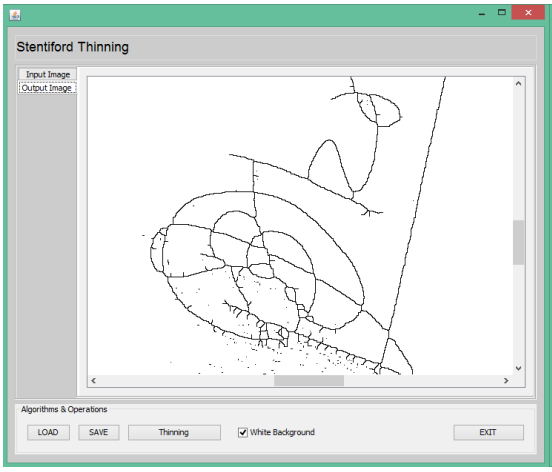

Figure 4.1: Threshold Signature

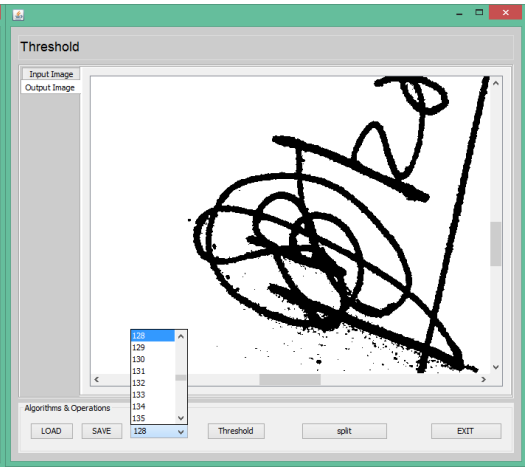

Figure 4.2: Thinned signature

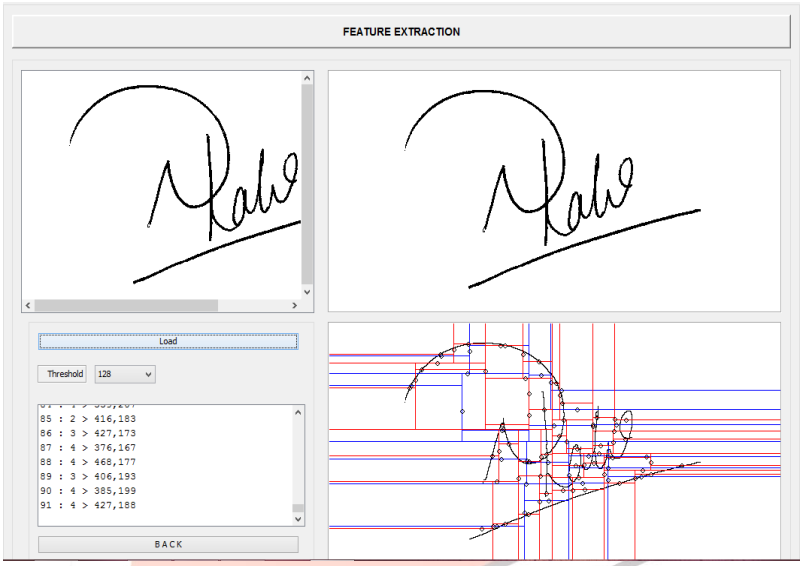

Figure 4.3: Features Extracted from Input Signature

In feature extraction module, instead of 60 feature points, we extracted total 92 feature points from each input signature pattern. As we are extracting more feature points than usual, it is essential for a user to create his/her signature with utmost care to avoid rejection of original signature.

The Database used consists of total 2000 signature samples. It is further divided into training dataset and testing dataset. 10 original samples and 10 forgery samples are taken from 100 persons each. 7 original and 7 forgery samples of each person are used for training of neural network so the training dataset consists of total 1400 samples. Remaining 3 original and 3 forgery samples are used for testing so the testing dataset consists of total 600 samples. We can try variations in the training and testing dataset contents to evaluate systems performance in different situations; for example: 60% of signatures for training and remaining 40% for testing.

Accuracy of the system has been calculated in the form of percentage using quality performance measures namely FAR (False Acceptance Rate), FRR (False Rejection Rate) and CCR (Correct Classification Rate). Results obtained are described as follows.

Table 4.1: Result of Trained Neural Network with New Samples from Database

Samples Presented	Genuine	Forged	FAR	FRR	CCR
300 Genuine	233	67	15%	22.34%	81.3%
300 Forged	45	255			

V. CONCLUSION

This paper presents a method for offline signature recognition and verification. Camera captured or scanned signatures can be provided in the form of image to this system. Various image enhancement and noise reduction techniques can be used to enhance the image to a suitable form for further processing. The Algorithm based on the 60 feature points is used which is more efficient and can provide more accurate results than the existing techniques and can survive against the skilled forgeries. With a database of total 2000 signature samples, accuracy of 81% has been achieved for the testing dataset. Security is one of the most critical issues when it comes to signature recognition especially if used by banks. One fraud signature can result into big financial losses, damaged reputation etc. so a system like this one is necessary.

VI. ACKNOWLEDGMENT

I would like to express my profound gratitude and deep regard to my Project Guide Prof. D. B. Kshirsagar, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His suggestions were of immense help throughout my project work. Working under him was an extremely knowledgeable experience for me.

REFERENCES

[1] Suhail M. Odeh and Manal Khalil, "Off-line signature verification and recognition: Neural Network Approach", 978-1-61284-922-5/11/$26.00 IEEE 2011

[2] Rimpi Suman and Dinesh Kumar, "Punjabi Offline Signature Verification System Using Neural Network", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-3, Issue-2, December 2013

[3] Devshri Satyarthi, Y.P.S. Maravi, Poonam Sharma and R.K. Gupta, Comparative Study of Offline Signature Verification Techniques, International Journal of Advancements in Research Technology, Volume 2, Issue2, February-2013

[4] Vaishali M. Deshmukh and Sachin A. Murab, "Signature Recognition Verification Using ANN", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-6, November 2012

[5] Vahid Malekian, Alireza Aghae, Mahdie Rezaeian and Mahmood Alian, "Rapid Off-line Signature Verification Based on Signature Envelope and Adaptive Density Partitioning". 978-1-4673-6206-1/13/$31.00 IEEE 2013

[6] Cemil OZ, Fikret Ercal and Zafer Demir, "Signature Recognition and Verification with ANN",

[7] Manoj Kumar, "Signature Verification Using Neural Network," International Journal on Computer Science and Engineering (IJCSE) 2012

[8] Pradeep Kumar, Shekhar Singh, Ashwani Garg and Nishant Prabhat, "Hand Written Signature Recognition Verification using Neural Network", international Journal of Advanced Research in Computer Science and Software Engineering volume 3, Issue 3, March 2013

[9] Debasish Jena, Banshidhar Majhi and Sanjay Kumar Jena, "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method", Journal of Computer Science 4 (2): 111-116, 2008

[10] Swati Srivastava, Suneeta Agarwal, "Offline Signature Verification using Grid based Feature Extraction", International Conference on Computer Communication Technology (ICCCT)-2011