A COMPARATIVE STUDY OF BIOMETRIC AUTHENTICATION BASED ON HANDWRITTEN SIGNATURES

Rajdeep Das[1],Sangeeta Dhar[2], Sabarni Das[3],Saurav Dutta[4],Subra Mukherjee[5]

[1, 2, 3, 4, 5]*Dept. of Electronics and Communication, Don Bosco College of Engineering and technology, Assam Don Bosco University Guwahati, India*

rajdeepdas1591991@gmail.com, dhar.sangeeta087@gmail.com, dassabarni2@gmail.com, saurav.dutta08@gmail.com, subra_mukherjee@yahoo.in

Abstract

With the increasing concerns for security, automated systems for authorization and authentication have become enormously important in every sector today. There are many methods for personal identification such as smart cards, PIN (personal Identification Number), passwords, etc. Regardless of the efficiency and accuracy of these systems, these systems can be always be stolen, lost, forgotten, cracked, hacked, etc. And it is for this reason biometric based authentication system have gained a lot of importance worldwide. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological (face, iris, retina, voice, palm prints, hand geometry) or behavioral characteristic (signature, voice, keystroke pattern) that the person possesses. This system is more accurate as these characteristics are unique for a particular person and vary almost negligibly over time. In this paper we have presented a comparative study of recent advances in biometric authentication based on mainly offline Hand-written signatures.

Keywords:- *Biometrics, online and offline signature verification, authentication, feature extraction, region of interest (ROI), Artificial Neural Network.*

----------***----------

1. INTRODUCTION

1.1 Biometrics

The term *biometric* comes from the Greek word "*bios*" (life) and "*metrikos*" (measure). The biometry defines some of the body characteristics like face, gait, voice, signature, finger print, handwriting, iris, DNA etc. Since today, a wide variety of applications require reliable verification schemes to confirm the identity of an individual, recognizing humans based on their body characteristics and behavior became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometric cannot be borrowed, stolen, or forgotten, and forging one is also very difficult. Biometrics can be categorized as behavioral and physiological. Handwritten signature belongs to behavioral biometric. In most of the places the verification is done either by a person who is familiar to the signature or by matching it against a few signature templates manually. Handwritten signature verification can be classified into offline signature recognition system and online signature recognition system. The use of signatures has been one of the most opportune methods for the recognition and verification of human beings. A signature may be termed a behavioral biometric, as it can be modified depending on many essentials features such as frame of mind, exhaustion, etc. The first signature recognition technique was the Optical Character recognition (OCR) which allowed the scanning of the written text and translates it into basic text documents, which are easily accessible in digital forms [1]. The online techniques depend on the dynamic characteristics such as speed of writing, pen pressure and order of strokes etc. The offline signature verification schemes are necessary to determine genuineness of a person's signature. There are some crest and toughs in a person's signature and it remains same and thereby used to measure the genuineness. This technique is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening. Some of the well known biometric features used for authentication are tabulated below:

Table 1: The following table shows the most well known biometric features used for authentication.

Biometric Trait	Description
Fingerprint	Finger lines, pore structure
Signature	Various features based on writing of a person

Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	Iris pattern
Retina	Eye background (pattern of the vein structure)
Hand geometry	Measurement of fingers and palm
Finger geometry	Finger measurement
vein structure of back of hand	Vein structure of the back of the hand
ear form	Dimensions of the visible ear
Voice	Tone or timbre
DNA	DNA code as the carrier of human hereditary
Odor	Chemical composition of the one's odor

1.2 Signature Types and Techniques

Signature is a behavioral biometric. The signature verification can be classified into two types, online signature scheme and offline signature schemes. Online signature schemes the data is received through sensors [2]. The data obtained is usually active data which includes the speed, acceleration, pressure, tip pressure, gradient etc. As such ones signature may change over time depending upon his her mood, health, etc. The computerize image is available in offline signature verification so the offline signature verification is important than online signature verification. Broadly speaking, signatures can be classified as: **Simple Signatures, Cursive Signatures and Graphical Signatures**. *Simple signatures* are the ones where the person just writes his or her name. *Cursive Signatures* are the ones that are written in a cursive way. The signatures can be classified as *Graphical* when cursive signatures depict geometric patterns.

Also with the recent technological developments, the fraud cases are also increasing day by day. The forgery has now been a major problem where the forger copies the original signature very easily.

The various types of forgery are [1, 3]:
Random Forgery: Are formed without any knowledge of the signer's name or signature shape.

Simple Forgery: Produce by people knowing the name of the signer's but without any example of the signature.

Skilled Forgery: Are produce by people looking at the original signature image and try to imitate it as closely as possible. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening. There are two types of signature verification methods:

Online Verification: This technique is mainly concerned with the dynamic characteristics of a signature. The characteristics include the writing speed, pressure points, strokes, acceleration as well as the static characteristics of signatures [3]. Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or building [1].

Offline Verification: This technique on the other hand includes the static characteristics. It depends on the feature extraction techniques. Off-line verification just deals with signature images acquired by a scanner or a digital camera. In an off-line signature verification system, a signature is acquired as an image. This image represents a personal style of human handwriting, extensively described by the graphometry [3].

2. RELATED WORK

Enhanced security is considered to be the greatest benefit of biometric technologies, followed by accuracy. Other benefits are its unique feature of not being shared/copied/lost, it reduces paperwork, and it is convenient. The signature verification is the behavioral biometry which has numerous applications in financial institutions or any other sector where transaction is involved. Also it finds wide application in person identification, forensic sciences, etc. It is because of this wide level of acceptance and potential applications that it has drawn the attention of researchers worldwide. Numerous work have been done is area. However we try to present a comparative analysis of the most recent ones.

The following table presents a comparative study of the different methods used for signature identification along with their recognition rate based on previous literature reviews.

Table 2: A comparative analysis of signature verification methods

Reference	DATA PRE-PROCESSING	FEATURE EXTRACTION	MATCHING AND CLASSIFIER	RECOGNITION RATE
6	Removal of noises using filters and thinning. ROI is extracted.	Signature height-width ratios, occupancy ratio, distance ratio calculation at boundary and signature image clustering.	Decision system	Varied from 10% to 80% depending on signature features extracted from different people and cluster.
12	-	RCWF and DTCWT was used.	Canberra Distance method.	90.6% using proposed method and 61.45% using DWT.
3	ROI extraction, binarization, noise elimination, skeletonization and isolated pixel removal.	Signature height-width ratio, area, end point number of the signature, maximum horizontal histogram and maximum vertical histogram.	SIFT feature matching and LVQ (Linear Vector Quantization) as classifier.	96.98%-99.03%
2	Denoising, binarization, thinning and skew removal.	Pixel density and angle feature.	Neural Network.	80(in sec) for pixel density method, 85(in sec) for angle feature and 95(in sec) for both methods mixed.
4	Normalization to gray scale values and with respect to height and width, noise removal.	Feature vector, projection, localization of point density and spatial frequency distribution. Calculation of correlation, mean and deviation.	Decision system based on correlation, mean and deviation values.	-
14	No preprocessing	Standard deviation of both x and y acceleration, average pressure, time taken, length and other 26 features.	Euclidean classifier.	FRR maximum=11.57% FRR minimum=0.66% FAR maximum=27.02% FAR minimum=0.72%
15	Noise filter, binarization and thinning .	Image gradient analysis (global), height- width ratio (statistical), geometrical and topological features.	Template matching approach, neural network approach, hidden Markov model approach, statistical approach and other approaches were taken for a comparative study.	-
16	Image enhancement by removal of noise and	Area, Euler number, extent and solidity.	Feed forward neural network.	-

	blurring.			
1	Background elimination, width normalization and thinning.	Global features like height width ratios, mask features like angle of signature and grid feature.	C sharp and Neural network.	100% for signatures that the network was trained for.
17	Binarization, region props tool.	Vertical and horizontal projection profile.	Testing is done in MATLAB using image processing.	-
10	DWT, resizing, skeletonization and exact signature area.	Angle features	MATLAB and comparison algorithm.	EER=7.2 corresponding to optimal threshold of 0.256 at a point where FAR=FRR.
7	Rotation normalization followed by interpolation	Global, statistical, geometrical and topological features.	CEDAR FOX system. Bayes classifier	FAR=23.18%, FRR= 20.62% and EER=21.90%.
11	Binarization, thinning and bounding box.	Center of mass, aspect ratio, tri surface feature and transition feature.	Error back propagation training algorithm and Neural network.	Classification rate is 82.66% and 100% success rate.
10	Noise removal and binarization.	Total area, convex area and mean orientation.	ANN	99.5%
18	Gabor wavelet transform	Statistical features.	Support vector machine.	94.47%
8	Color normalized and scaled into a standard format.	Global features like area, height and width.	Euclidean distance model.	89%
5	Noise reduction, binarization, clutter removal and thinning.	Euclidian distances from vertical and horizontal sectioning of the signature.	Four Feed forward ANNs are used.	FAR=15% And FRR=25% for vertical sectioning, 30% and 13 % for horizontal sectioning and 10 and 15% when 4 ANNs are used.
19	Normalization, angle of least second, smoothing and thinning.	Raw binary pixel intensities.	Graph matching and Hungarian method.	EER of 26.7% and 5.6% for skilled and random forgeries respectively.

2.1 Scheme of Implementation

This paper discusses the methodology for offline verification methods. As compared to on-line signature verification systems, on-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case [3]. The design of any signature verification system generally requires the solution of five sub-problems:

data acquisition, pre-processing, feature extraction, algorithm matching.

2.1.1 Data Acquisition:

Before moving further in the offline verification, the basic step to be followed is the data acquisition. The signature of an individual varies with state of mind and physical state. So, it is necessary to collect the data from the person at different time. This requires specifying the resolution, image type and format to be used in scanning each image. To this effect, a number of existing offline signature databases was studied. So in any offline signature verification system, the first step is to extract these signatures from papers using scanners [3].

Priya Metri, Ashwinder Kaur [4] they collected ten signatures of one person and stored it in the database which they were going to use in training of their software and not for actual matching. The database created in paper [5] showed seven signatures from each individual on A4 size paper which was divided into eighteen blocks each of width 5.5cm and height 3.5cm. Both the signatures used in training and testing were scanned at the same resolution. Samples from ten individuals were collected which gave a database of seventy signatures. Five out of the seven were used for the training of the ANNs and the rest two were used for testing. Infact in any offline method the first step is to create a database of handwritten signatures, comprising of several signatures from each person so as to overcome the various challenges in the later post processing stages.

2.1.2 Segmentation and Preprocessing:

This is one of the preliminary stages of signature identification. This is generally done to extract the region of interest from the image, i.e, the region containing the signature of the individual and remove irrelevant background. Image segmentation is the process of partitioning a digital image into multiple segments (set of pixels). It is the decomposition of a gray level or color image into homogeneous regions. Here every pixel in an image is assigned a label such that pixels with the same label share certain visual characteristics.

A signature image is first segmented (vertical and horizontal) and then data is extracted from individual blocks. The data is then compared with the test signature. In [6], signature verification is done by feature extraction is based on horizontal and vertical segmentation of the signature.

Vertical Segmentation: After pre-processing first the image is put inside a rectangle or bounding box so that it is properly fitted inside it. Scanning is started from left most upper point. Here vertical scanning is performed and if any peak or crest in the image is found then a line is drawn through it. Similar process is performed by scanning from left most lower point and going upwards while scanning. In this way total image is divided in vertical segments.

Horizontal Segmentation: Horizontal segmentation is done on each vertical segment. Here scanning is done from upper left point and down to lower left point. In each case scanning is moved from left to right to find any peak or crest. If found a horizontal line is drawn through it. Similar operation is performed for right most upper point to lower point in each vertical segment. After vertical and horizontal segmentation, signature is divided to small blocks. Data can be extracted from individual blocks.

Not only this, segmentation of the ROI is very important for further processing stages.

2.1.3 Feature Extraction of an Image:

Feature extraction is an essential step to image processing. When the input data to an algorithm is too large to be processed, then the input data will be transformed into a reduced representation set of features (also named features vector). Transforming the input data into the set of features is called feature extraction. Many data analysis software packages provide for feature extraction and dimension reduction. Common numerical programming environments such as MATLAB, SciLab etc. are used for feature extraction of an image.

There are numerous methods for feature extraction proposed by the researchers which are discussed in brief. The features for offline technique can be classified into following categories [7]:
1) *Global features*: It can be extracted from each of the pixels present in the rectangle containing signature. It is easily extractable, immune to noise and depends on the alignment of the signature.
2) *Statistical features*: It is extracted from the distribution of the pixels in the signature image. This technique includes the extraction of high pressure factors with respect to vertically segmented zones and the aspect ratio.
3) *Geometrical or topological features*: Describe the characteristic geometry and topology of a signature and thereby preserve the signatures global and local properties. This feature has a high tolerance to writing style and angle variations.

Samit Biswas, Tai-hoon Kim, Debnath Bhattacharyya, Pallavi Patil, Archana Patil [6,8] proposed a method to verify signature based on clustering technique. Clusters technique divides the set of data points into non-overlapping groups or clusters. The various stages of feature extraction they discussed about are:

- ***Signature height width ratio*:** The ratio is obtained by dividing signature height to signature width. The height is the maximum length of the column in an image and similarly the width is the row of maximum length. This ratio may differ from person to person, but the ratio is constant for an individual.

- ***Signature occupancy ratio***: It is the ratio of number of pixels which belong to the signature to the total pixels in the signature image.
- ***Distance ratio calculation at the boundary*:** It is calculated as the ratio of the leftmost pixel its distance from bottom boundary to the bottom left most pixel, the distance from right boundary.
- ***Signature image clustering:*** They created a separate cluster for set of sample signatures for each person. Here they used K-Nearest Neighbors' (KNN) clustering Technique for verifying a test signature belongs which cluster.
- ***Centroid:*** It is related to the centre of the image considering the vertical alignment as x axis and horizontal alignment as y axis.

The paper presented by Rahul Verma and D.S.Rao [9] discussed about the extraction using pixel density and the energy density of each segment which is calculated by taking the number of white pixels present in a segment. Based on the chain code (direction of connecting pixel) the pixels is observed and direction vector of each pixel is noted. They also included the angle feature where each subdivided cell is then resized and partitioned into sub-cells and finally calculated the angle of each pixel.

A recent work by Prashanth C. R. and K. B. Raja [10] described verification based on angle features. They found that in the angular features, the two phases are of major concern. Initially the preprocessed signature is undergone horizontal and vertical splitting. The skeleton of the signature image is scanned from left to right and top to bottom to calculate the total number of black pixels. The image is divided into two halves with respect to the number of black pixels by two lines, vertically and horizontally which intersects at a point called the centre of signature or geometric centre.

2.1.4 Matching Algorithm:

Here an algorithm is defined such that it takes all the extracted features and then matches it with the templates already created in the system and provide its result to the decision system. Algorithm should be developed in a manner where its computational complexity is very less and little changes in the signature should be detected and accordingly modifications should be made so that the system returns an accurate and reliable result.

Various techniques have been used by researchers for verification of signature in offline model. Two of the most widely used methods are using Artificial Neural Network and Hidden Markov Model. In paper [1,11] the authors proposed a system based on Neural Network. For the training of dataset ANN has been used. The features that had been extracted from signature images were fed as an input to an Artificial Neural Network using feed forward back propagation. In order to train the neural network, a set of training signature images were required, and the varieties were predefined. During training, the connection weights of the neural network were initialized with some random values. The training samples in the training set were input to the neural network classifier in random order and the connection weights were adjusted according to the error back-propagation learning rule. Feed forward back propagation neural network classifier is used to verify the signatures. Database has been split into two parts, to perform the training and testing components.

Another technique used is Hidden Markov Model Approach: [12] it is one of the most widely used models for sequence analysis in signature verification. The matching is done by steps of probability distribution of features involved in the signatures or the probability of how the original signature is calculated. If the results show a higher probability than the test signatures probability, then the signatures is of the original person, otherwise the signatures are rejected.

2.2 Performance Measures

In context, the performance of a biometric measure is usually defined in terms of

- False accept rate (FAR), or *fraud rate*: what percentage of times an invalid user is accepted by the system.
- False rejection rate (FRR) or *insult rate*: the percentage of times a valid user is rejected by the system
- Failure to enroll rate (FTE or FER).

In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameters. One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER). The lower the EER, the more accurate the system is considered to be.

3. DISCUSSION

Though the literature consist of a huge number of work on signature authentication using handwritten signature yet there still remain many challenges open to be resolved. As it is concerned with authentication or recognition of person, it is very sensitive and so the features extraction should be done very precisely so that they uniquely define one's signature. Also as signature authentication mainly finds application in transactions of financial institution, so the matching algorithm should be very accurate and both FAR and FRR should be extremely low. We have presented a brief study of various methods and algorithms employed for offline signature authentication.

After a study of number of works done on signature verification, it was found that a large number of systems

employ limited number of features for extraction mainly done to reduce the algorithm size and make it run faster. The data is acquired as a scanned image and it undergoes various enhancement techniques leading to increase in memory size of the program. Instead, a good quality scanner can be used so that few enhancement techniques are enough to make the data available for segmentation. Moreover, a set of signature can be taken from an individual at various instances so that little variation can be neglected. Along with the existing features available for feature extraction, new features like number of pens up and pen down, unique characters and ending pattern of the last stroke can also be taken.

CONCLUSIONS

There are always concerns about adapting to new technologies. Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. Many business applications (e.g. banking) will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. The main benefit of using a biometric authentication factor instead of a physical token is that biometrics can't easily be lost, stolen, hacked, duplicated, or shared. The future of biometrics looks increasingly bright with the demand for security rising daily. Educational institutions, private companies and governments all have important roles in improving the technology and promoting its use through better education, knowledge dissemination, increased usability, standards, and proven reliability.

REFERENCES

[1] O.C. Abikoye, M.A. Mabayoje, R. Ajibade, "Offline Signature Recognition & Verification using Neural Network" , International Journal of Computer Applications(0975-8887), Vol.35-No.2, December 2011

[2] Rahul Verma, D.S. Rao, "Offline Signature Verification and Identification Using Angle feature and Pixel Density Feature And Both Method Together" , International Journal of Soft Computing and Engineering(IJSCE) ISSN: 2331-2307 , Vol. 2, Issue-4, April 2013.

[3] Meera V. Kanawade & Kataria S, "Signature verification & recognition-case study", International Journal of Electronics, Communication & Instrumentation Engineering Research And development(IJECIERD), ISSN: 2249-684X, Vol. 3, Issue 1, March 2013.

[4] Priya Metri, Ashwinder Kaur, "Handwritten Signature Verification using Instance Based Learning", International Journal of Computer Trends and Technology-March to April Issue 2011.

[5] Manasjyoti Bhuyan, Kandarpa Kumar Sharma and Hirendra Das, "Signature Recognition & Verifivation using Hybrid Features & Clustered Artificial Neural Network (ANN)s" , International Journal of Electrical and Computer Engineering 5:2 2010

[6] Samit Biswas, Tai-hoon Kim, Debnath Bhattacharyya, "Features extraction and Verification of Signature Image using Clustering Technique" , International Journal of Smart Home, Vol.4, No.3, July,2010

[7] Meenakshi K. Kalera, Sargur Srihari and Aihua Xu, "Offline Signature Verification and Identification Using Distance Statistics" , International Journal of Pattern Recognition and Artificial Intelligence, Vol.18, No.7(2004) 1339-1360.

[8] Ms Pallavi Patil & Ms. Archana Patil, "Offline Signature Recognition Using Global Features" , International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459 Volume 3, Issue 1, January 2013.

[9] Prashanth C. R. and K.B. Raja," Offline Signature Verification Based on Angular Features" , International Journal of Modeling and Optimization, Vol. 2, No.4, August 2012.

[10] Vibha Pandey, Sanjivani Shantaiya, "A novel Approach for Signature Verification using Artificial Neural Network", International Journal of Engineering and Advanced Technology(IJEAT), ISSN: 2249-8958, Vol. 1, Issue-6, August 2012.

[11] Pradeep Kumar, Shekhar Singh, Ashwani Garg, Nishant Prabhat, "Handwritten Signature Recognition & Verification using Neural Network" , International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, March 2013

[12] Shirdhonkar, Manesh Kokare, "Off-line handwritten Signature Identification Using Rotated Complex Wavelet Filters", IJCSI International Journal of Computer Science Issues, Vol.8, Issue 1, January 2011.

[13] Hassan Soliman, Abdelnasser Saber Mohamed, Ahmed Atwan, "Feature Level Fusion of Palm Veins and Signature Biometrics", International Journal of video & image Processing and Network Security IJVIPNS-IJENS Vol:12 No: 01 28.

[14] Saad Tariq, Saqib Sarwar, Waqar Hussain, "Classification of Features into Strong and Weak Features for an Intelligent Online Signature Verification System" , Proceedings of the 1st International Workshop on Automated Forensic Handwriting Analysis(AFHA) 2011.

[15] Meenakshi S Arya, Vandana S Inamdar, "A Preliminary Study on Various Off-line Handwritten Signature Verification Approaches", International Journal of Computer Applications(0975-8887), Vol.1-0- No. 9.

[16] Ms. Vibha Pandey, Ms. Sanjivani Shantaiya, "Signature Verification using Morphological Features Based on Artificial Neural Network", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 7, July 2012

[17] Kritika Raghuwanshi, Niketa Dubey, Riju Nema, Rishabh Sharma, "Signature Verification through MATLAB Using Image Processing", International Journal of Emerging Trends and Computer Science(IJETECS), Vol.2, Issue 4, April 2013

[18] Amit Sharma, Poonam Sharma, Ashutosh Sharma, "Rotation Invariant Offline Signature Recognition", International Journal of Engineering Sciences Research-IJESR, ISSN: 2230-8504, Vol.3, Issue 5, September-October 2012.

[19] Ibrahim S. I. ABUHAIBA, "Offline Signature Verification Using Graph" Matching, Turk J Elec Engin, VOL.15, NO.1 2007.