A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF FINAL YEAR PROJECT

ON

SIGNATURE VERIFICATION USING GRID BASED FEATURE EXTRACTION

BY,

BINAY KARALI

110EI0040

Under the Guidance of

Prof. Sukadev Meher

Department of Electronics and Communication Engineering

National Institute Of Technology

Rourkela

2013-2014

ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA

ROURKELA – 769008; www.nitrkl.ac.in

CERTIFICATE

This is to certify that the thesis titled "**Signature Verification using grid based feature extraction**" submitted by Binay Karali (110EI0040) in partial fulfillment of Bachelor of Technology in Electronics and Instrumentation Engineering at National Institute of Technology, Rourkela is an authentic work carried out by him under my supervision and guidance.

Prof Sukadev Meher
Department of Electronics and Communication Engineering
National Institute of Technology, Rourkela

DECLARATION:

I, hereby declare that the project work entitled "**Signature Verification using grid based feature extraction**" is a record of our original work done under **Prof. Sukadev Meher** in National Institute of Technology, Rourkela. Throughout this documentation wherever contributions of others are involved, every endeavor was made to acknowledge this clearly with due reference to literature. This work is being submitted in the partial fulfillment of the requirements for the degree of Bachelor of Technology in Electronics and Communication Engineering at National Institute of Technology, Rourkela for the academic session 2010– 2014.

……

Binay Karali,

110EI0040

Department of Electronics & Communication Engineering,

National Institute of Technology, Rourkela.

Acknowledgement

I would like to express my gratitude to my thesis guide **Dr.Sukadev Meher** for his guidance, advice and constant support throughout my thesis work. I would like to thank him for being my advisor here at National Institute of Technology, Rourkela.
I would like to thank all faculty members and staff of the Department of Electronics and Communication Engineering, N.I.T. Rourkela for their generous help in various ways for the work to go on.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I've enjoyed their companionship so much during my stay at NIT, Rourkela.

I am especially indebted to my parents for their love, sacrifice, and support. They are my first teachers after I came to this world and have set great examples for me about how to live, study, and work.

BINAY KARALI

110EI0040

CONTENTS

LIST OF FIGURES AND TABLES:

ABSTRACT

Signature does not depend on physical features like that of iris detection, gait, fingerprint, facial features; instead it's a completely behavioral attribute of an individual.

The field of signature verification is broadly classified into two parts i.e. online and offline. Online signature verification deals with signatures obtained from digital tablets or any such device where in addition to spatial features of the signature; time, pressure etc. information is also available.

Offline signature verification deals with only verifying the signature through its scanned copy of signature sample, hence it lacks dynamic information which makes offline verification difficult which is still used in our daily lives as in banks, offices etc.

The sole purpose of this research paper is to develop an efficient signature authentication system which is still an important part of biometric identification methods.

Here we work with offline signature verification which uses feature extracted from grid matrix placed over the signature image. In order to verify the signature we compare test and reference sample features using appropriate algorithm to correctly verify the identity of a person through his signature. This technique can be applied for various applications viz. bank cheque verification, official purposes, passport verification etc.

The sensitivity of signature verification system can be dynamically altered by changing the threshold depending upon the level of security required. Here we are mainly interested in evaluating our system with respect to skilled forgeries because normal free hand forgeries can be easily detected by any signature verification system.

Chapter 1

Introduction

1.1 Introduction

From a lay man's point of view, we can easily recognize a person through his way of speaking, voice, facial characteristics but thing is limited to only a number of persons in our vicinity. The problem with recognition comes when the person to be identified doesn't lie in your vicinity. This is where comes the requirement of an efficient system which can easily and effectively verify a person's identity.

The security requirements of today's world has provoked a need for an efficient system for verifying a person's identity. Biometrics has recently gained too much popularity in identification of individuals, as it effectively deals with it by utilizing distinctive features of individuals.

A biometric technique ought to either confirm or identify. In verification mode, it ought to be able to authenticate the person's identity based of his/her claimed identity. In lieu, in identification mode, it searches for the person's identity (among enrollment knowledge in a database) without the subjects having to claim their identity .Depending on the personal traits thought about, types of biometric can be defined: physiological or behavioral.

The former is based on the measurement of biological traits of users, like, for instance, fingerprint, face, hand geometry, retina, and iris. The latter consider behavioral traits of users, such as voice or handwritten signature.

There has been lots of research on online signature verification but that of on offline signature is not much. Online signature verification is not a trivial pattern recognition issue when it comes to expert forgeries. Online signature has dynamic features hence verification for online signatures is simpler than that for offline signatures, since the latter lacks dynamic knowledge and they must rely basically on picture features only. Also, the performance of the systems is not directly comparable due to this difference. Historically some authors have worked on simple forgeries while others have handled the verification of expert forgeries. Our present work deals with the verification of expert forgeries.

1.2 Identification

Identification is performed by checking for a person's identity along with the whole database. Basically we compare the test sample for each subject with whole of the database i.e. with samples from all subjects in the database.

1.3 Verification

Verification is the process of comparing reference/test sample with samples from the same subject only, which is not the case in identification. This process basically deals with person's identity verification and not searching for person's identity in an ensemble of data from user.

1.4 Advantages of a biometrics system

Biometric system is a behavioral attribute and does vary from person to person. So clearly if we use it as a measure for verification of identity, it can give satisfactory results far much better than other systems.

1.5 Disadvantages of a biometric system

Biometric system also has some of disadvantages that can be given as:

- The finger prints of those people, working in processing industries are often affected. Therefore those companies shouldn't use the finger print mode of authentication.
- Voice of a person may change with increasing age or suppose a person is affected by common cold or any flu, then there is significant change in his voice. So the system must be adaptive enough to take care of this alterations.
- When people are affected with eye problems as that of cataract, conjunctivitis, problems may arise in the system.

Despite these disadvantages, biometric systems are nowadays used widely in much kind of industries. If one can gain desired accuracy, than no other thing can take its place.

Chapter 2
Problem Statement

2.1 Problem Statement

Signature check methods may use numerous distinctive qualities of a singular's signature in place for ID of that single person. The points of interest of utilizing such a verification systems are

(i) Signatures are generally acknowledged all over the place as a type of distinguishing proof and confirmation.

(ii) Information obliged is not that delicate.

(iii) Forging of one's signature doesn't mean a long-life misfortune of that one's character.

The fundamental thought is to ask into a mark confirmation system which is not exorbitant to make, is solid regardless of the fact that the distinct is under diverse feelings, easy to understand as far as design, & strong against fakers.

In signature check requisition, the marks are prepared to concentrate offers that are utilized for confirmation. There's stages called selection & confirmation. In deciding the execution of the check system the decision of characteristics takes fundamental part & it is basic. The characteristics are chosen focused around positive paradigms.

Mainly, the characteristics must be little to be put away in a savvy card & needn't bother with complex strategies. There's sorts of characteristics that approving a mark. They are static & element characteristics.

Static characteristics are those, which are concentrated from marks that are recorded as a picture although element characteristics are concentrated from marks that are procured in genuine time. The characteristics are of sorts, capacity based & parameter based characteristics.

Function based characteristic cases incorporate position, weight, inclination point, pen slant and speed. Despite the fact that the execution of such characteristics is excessively exact in confirming marks, they are not suitable for this situation due to the many-sided quality of its matching calculation. Consequently, parameter based characteristics are not utilized habitually unless until its a solid necessity.

It is paramount to consider outside components when researching a mark check system. These days signature confirmation provisions are utilized within our everyday lives and are laid open to human feelings. The framework needs to give solid precision in confirming a singular's signature even in circumstances when client is under diverse circumstances.

Chapter 3
Signature Verification

3.1 Signature Verification:

Signature verification is a common behavioral biometric used in identification of human beings for purposes of verifying their identity. Signatures are useful for identifying a specific person because each person's signature is highly one-of-a-kind, if the dynamic properties of the signature are thought about in addition to the static features of the signature. It's true that expert forgers can truly replicate the signature, but it's highly unlikely to forge dynamic features of a signature which is used in online signature verification.

3.2 Types of Signature verification

Signature verification is part into two as per the accessible information in the data.

Offline (Static): The signature is obtained from a confirmation framework is the snap of a mark and is valuable in programmed check of marks found on bank checks and archives.

Online (Dynamic): Signatures that are caught by information procurement gadgets like weight-touchy tablets that concentrate element characteristics of a signature notwithstanding its shape (static), and might be utilized as a part of constant requisitions like Visa transactions, security of little individual gadgets, approval for getting to of workstation clients which have delicate information or projects, and validation of people for access to labs, working environment and so forth.

3.3 Why Online Signature Verification?

Offline signatures are generally available, due to checking equipment or paper foundation, and hold less one of a kind data since just the filtered duplicate of the mark is the info to the framework. While authentic marks of the same individual may marginally change, the contrasts between an imitation and a bona fide marks may be troublesome, which make programmed disconnected from the net mark confirmation an extremely testing example distinguishment and matching issue. Moreover, the contrasts in pen widths and capricious change in signature's perspective degree are different troubles of the issue. It is worth to recognize the way that even proficient criminological analysts perform at something like 70% of right signature grouping rate (real or forgery).unlike logged off, On-line marks are more interesting and troublesome to fashion than their partners are, since notwithstanding the static data, element characteristics like pen slant, weight, and catch time of each one point on the mark trajectory are accessible to be included in the arrangement assignment. Subsequently, on-line signature confirmation is more dependable than the logged off however it

requires more intricate calculations and likewise exorbitant gears for its execution.

3.4 Why sudden urge for offline signature verification?

As we did observe that online signature has both static as well as dynamic features of a signature, which makes it difficult for the observer to reproduce.

Even a good forger may replicate the signature exactly but it is too difficult for him to reproduce exact dynamic features. But as offline signature only rely on image of the signature we need to develop an efficient method for offline signature verification in order to verify these signatures, since these are more prone to forgery.

3.5 Performance Evaluation of Signature vs. System:

For evaluation of performance of a signature verification system, there are two important factors: the false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures. These two are inversely proportional to each other and hence lowering of one leads to increasing of another. We need to trade-off between these two depending upon our application. Generally we establish Equal Error Rate (EER) which is used as a measure for signature verification system, a point where FAR equals FRR.

Forgery means that an individual is attempting to make false signatures of any other individual to become authenticated. There are three types of forgeries:

(1) ***Random Forgery:*** In this type of forgery an individual creates an signature just by knowing the name of the person in the signature.

(2) ***Unskilled Forgery****:* The signer creates a signature after observing the signature without any prior experience.

(3) ***Skilled Forgery:*** The signer, who may be a professional replicates a signature after observing the signature carefully and practicing the original signature prior to signing.
There have been several studies on on-line signature verification algorithms. On-line signature verification systems differ on various issues like data acquisition, preprocessing, and dissimilarity calculation.

The proposed method has proven to give results on Database (Set 1) and FAR of 13.5% and FRR of 10.8% for Database (Set 2) which is better than many existing verification techniques.

Chapter 4
General System Overview

4.1 General System Overview:

A dynamic signature verification method gets its input from knowledge acquisition tool like a digital tablet or other, dynamic input tool. The signature is then represented as time-varying signals. The verification method focuses on how the signature is being written than how the signature was written. This provides a better means to grasp the individuality of the writer but fails to recognize the writing itself.

But in case of offline signature we get the image of signature from a scanner or camera or any such image capturing device which basically gives us only static features of a signature.

4.2 Signature verification procedure:

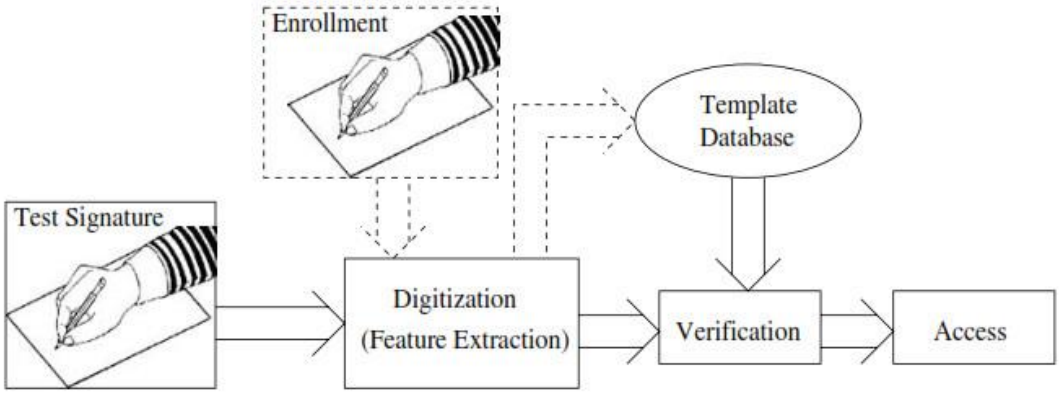


Fig.1 Signature verification system

Input:

For an off-line signature verification system, input is static. This input is normally captured through a tablet or like camera based tracking of pen tip while an individual performs a signature. This input is digitized and fed for processing. First of all pre-processing is done on the input received and then some features are extracted from the captured online data on the basis of which the signature is validated.

Output:

The output obtained from an online signature verification system is a decision if the person providing the signature is authorized or not.

Chapter 5
Preprocessing

5.1 Preprocessing:

In order for confirmation of a signature correctly, preprocessing of acquired signature is always necessary. The acquired signature in offline signature may contain extra dots which arise as a result of dust in lens of capturing device, all these are unwanted. This extra dots can be efficiently removed byusage of median filters on the captured signature image.
Preprocessing includes some more operations like resizing, binarization and thinning & rotation normalization. The foremost step in preprocessing is to resize the signature to a standard size so that all the signatures have same normalized size, so that it makes our task easy afterwards to compare reference and test samples.

There are some common preprocessing steps, aimed to improve the performance of a verification process. These include size normalization, smoothing of the trajectory & re-sampling of the signature knowledge.
Low resolution tablet or low sampling rates tablets may give signatures that have jaggedness which is often removed using smoothing techniques. In the systems where tablets of different active areas are used, signature size normalization is a often used as preprocessing method.
Comparing of signatures having the same shape but of different sizes would lead to low similarity scores. Size normalization is applied to remove that affect.

The resized image needs to be thinned so as to get a single pixel run of the image of signature. If at all we don't perform it wouldn't be that big a problem, but still it is done so that we effectively get the most essential details of the signature. Thinning is basically done so that it reduces the load on feature extraction module by discarding the unnecessary pixels in the signature image. Finally after preprocessing we get an image which can be used efficiently for feature extraction.

Fig.2 Genuine signature samples:

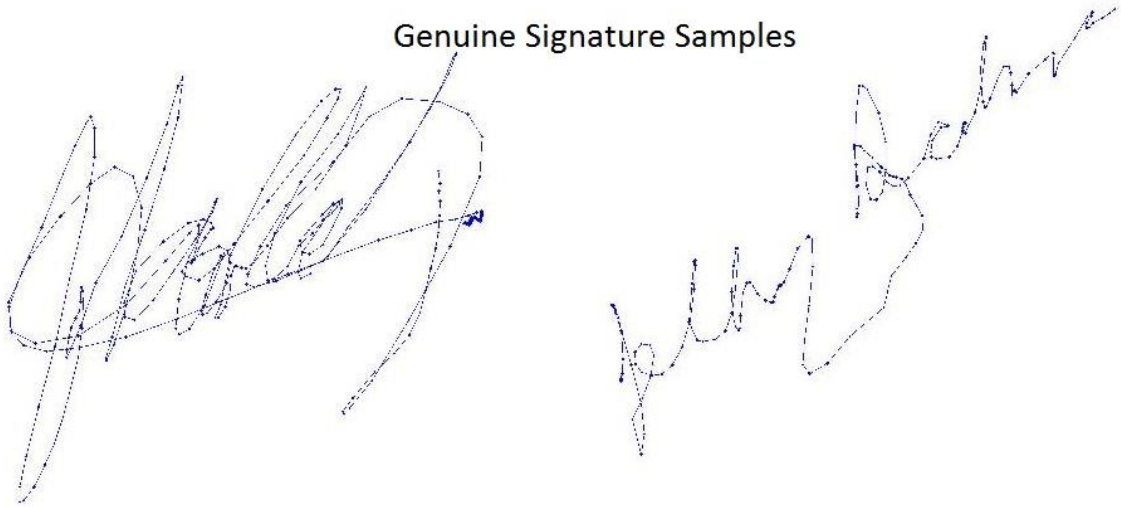


Fig.3 Skilled Forgery Samples:

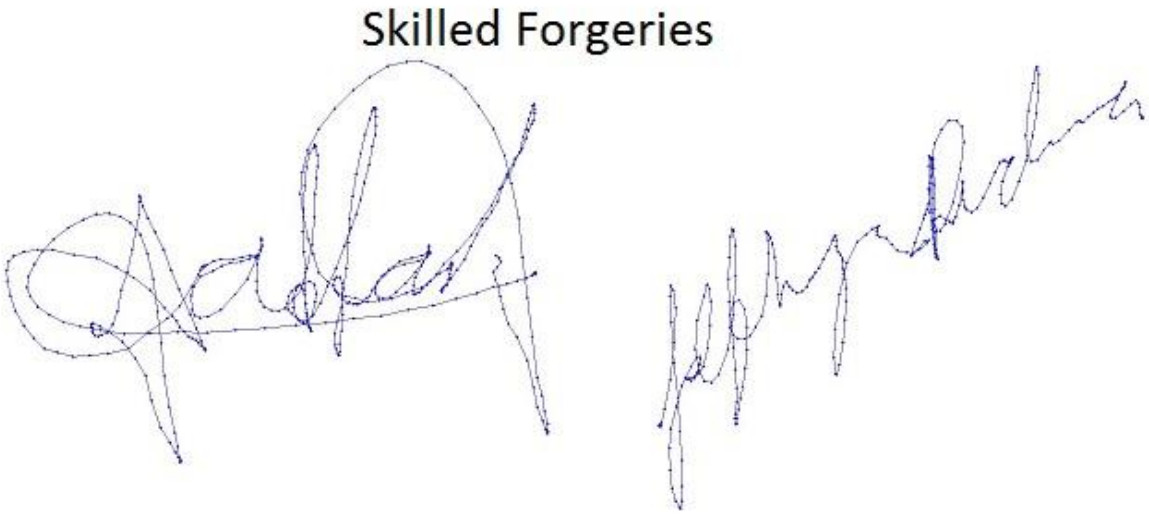


Fig 4 Resized genuine samples:

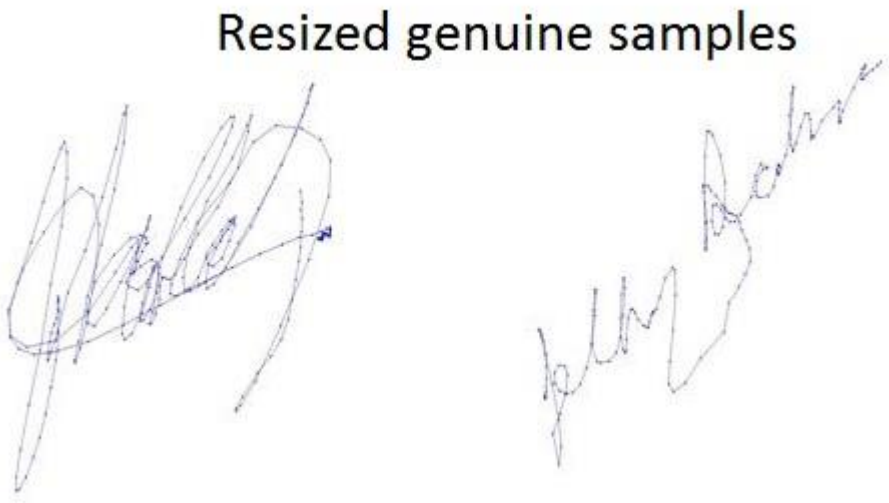


Fig 5 Binarized Samples:

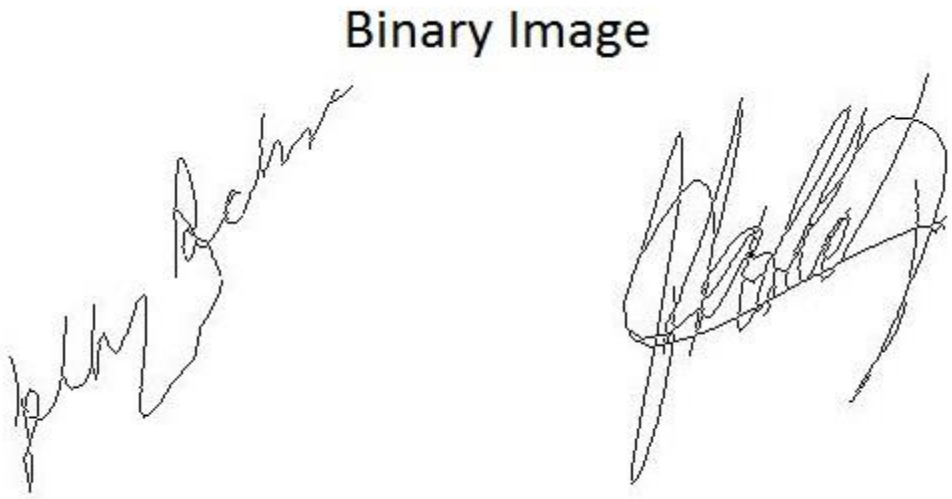


Fig 6 Thinned signature samples:

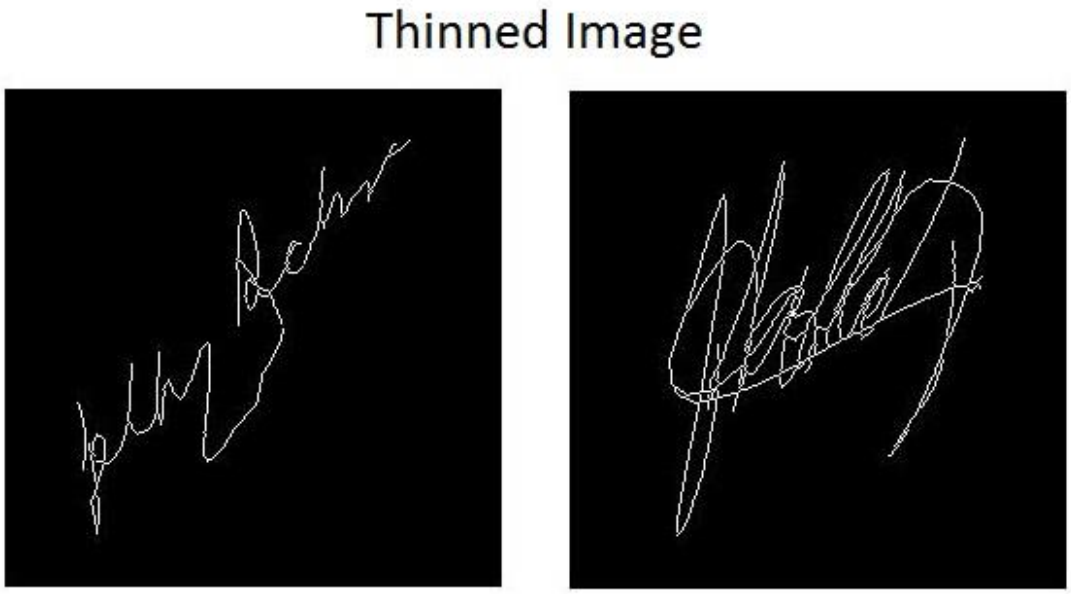
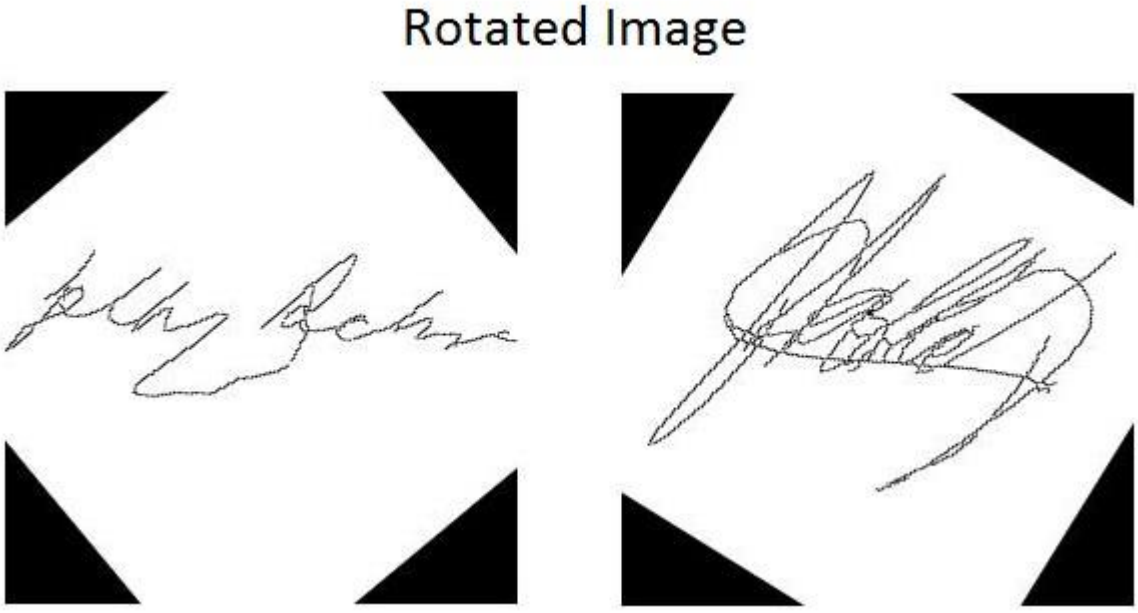


Fig 7 Rotated signature samples:



5.2 Skew Correction:

The projection parallel to the true alignment of the lines will likely have the the maximum variance, since when parallel, each given ray projected through the picture will hit either no black pixels (as it passes between text lines) or lots of black pixels (while passing through lots of characters in sequence).

There are several often used methods for detecting skew in a page, some depend on detecting connected parts (for lots of purposes, they are roughly equivalent to characters) & finding the average angles connecting their centroids. The method they employed was to project the page at several angles, & decide the variance in the number of black pixels per projected line.

Here we use Histogram curve method of best fitting in order to eliminate skew. This process can be skipped by attaching a horizontal sheet of paper of particular dimension (e.g. 2cm X 7 cm) in case of online signatures , so that a user signs within the box and skew is avoided.

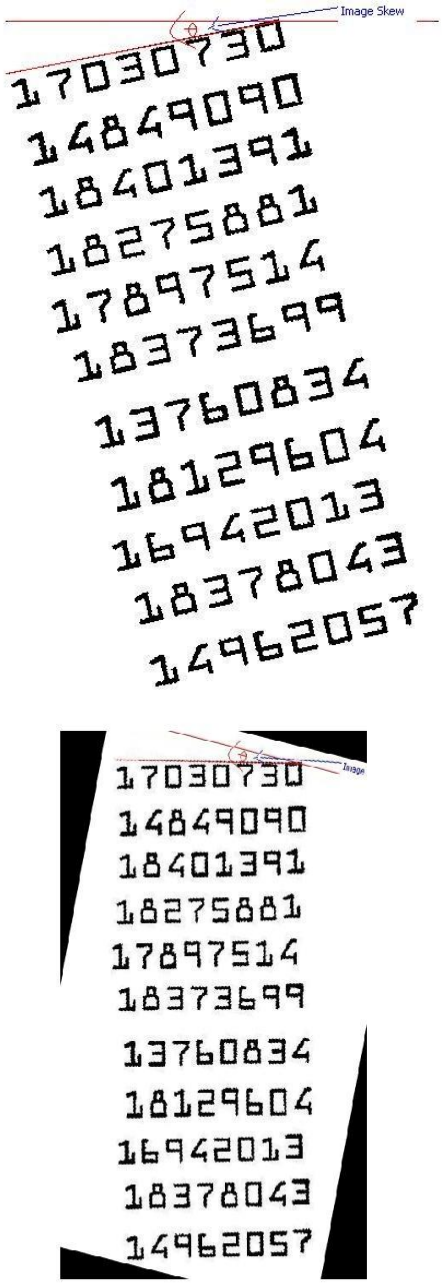


Fig 8 Skew corrected images

Chapter 6
Feature Extraction

6.1 Feature Extraction:

Characteristic extraction stage is maybe the most pivotal phase of a mark check framework. Characteristics could be considered worldwide or nearby, where worldwide characteristics speak to properties of a signature all in all and neighborhood ones relate to properties particular to a testing point. The worldwide characteristics samples are signature limit box, length of trajectory or normal marking speed, and speed or speed between two sequential focuses in a mark are nearby characteristics.

6.2 Feature Types for Signature Authentication:

It is especially essential to actualize personality confirmation methodology which gives high degree in execution and still worthy by a greater part of clients. A mark could be verified utilizing either static (off-line) or dynamic (on-line) check.

• Static (off-line): The signature is composed either on a bit of paper and afterward checked or straightforwardly on the machine utilizing gadgets, for example, the advanced cushion. The state of the signature is then contrasted and the enlisted (reference) signature. The trouble with this method is that a great counterfeiter will have the capacity to duplicate the state of the mark.

• Dynamic (on-line): The client's signature is gained progressively in real time. By utilizing this element information, further characteristic, for example, quickening, speed, and prompt trajectory plot and removals might be concentrated.

Data extracted from tablet is in the form of a matrix.

The objective of this phase is to extract the features of the test image that will be compared to the features of training image for verification purpose.
There are two types of features: (i) Function features and (ii) Parameter features.
Function features include position, velocity, pressure etc. and are used in online verification techniques.
Parameter features are further divided into global parameters and local parameters.
Global parameters include Fourier transform, wavelet transform etc. Local parameters are further divided into component-oriented and pixel-oriented.
Component-oriented features include contour based, geometric based, slant based etc. Pixel-oriented features include grid based, intensity based etc. Here we are going to use grid based feature extraction.

6.3 Steps:

(1) After preprocessing we have a signature of size 100x200(pixels). At that point we make a network of m x n where, over a preprocessed signature as demonstrated in In this paper, we have taken m=10 and n=20. In this way, a mark picture is partitioned into 200 square cells where each one cell is having 100 pixels. We have done such division of the mark picture with the goal that more productive and compelling correlations is possible which can undoubtedly discover the imitations.

(2) Next we figure out the cells of a column of a matrix that are the mark content. Recognize that signature substance is figured regarding dark pixels, hence just those cells ought to be acknowledged which are having 3 or more dark pixels. Rehash the procedure for all lines of a network. Subsequently we have each one of those cell positions which are some piece of the mark picture. Presently we make a network of size m x n comparing to the matrix of size m x n i.e. one cell of a network compares to one component of a framework. The network component is equivalent to 1 if the cell of same position in the lattice is the piece of signature, generally the grid component will be 0. Consequently, as a consequence of this step, we have a grid having components 0 or 1 as needs be.

(3) We compute the amount of dark pixels in cells of a line holding mark content. Rehash the procedure for all lines. At that point we put the qualities of m columns in a cluster. Additionally, the same procedure could be connected to segments. Consequently we get an alternate cluster having n components comparing to every section.

(4)Next we figure out the limit box encasing the signature by discovering the dark pixel in each one corner of the examined, diminished, binary picture. Here this characteristic is joined in order to add to the given characteristics. Here it serves as a worldwide characteristic which gives a more hearty list of capabilities.

In this way we have extricated three characteristics:

(1) a m x n grid as portrayed above comparing to a m x n lattice.

(2)an show of size m where first component is the amount of dark pixels in first line of a network, second component is the amount of dark pixels in second column etc,

(3) A show of size n where the first component is the amount of dark pixels in first section of the network, second component is the amount of dark pixels in second segment etc.

(4) Signature boundary box.

These features are further used in verification process. Our main motive is now to compare reference with test sample and then classify it to be genuine or forged one.

Chapter 7
Classifier Implementation

7.1 Signature Verification:

The purpose of verification phase is to compare the test image with training image using extracted features and to decide whether the test image is original signature of the writer or forgery.

7.2 Verification steps:

(a) Calculation of Column Matching Score (CMS) :

(i) Let M1 and M2 be the lattices of reference picture and test picture individually. At that point we analyze the segments of the framework M2 with M1. Every section is having m components. On the off chance that at any rate β, where $\beta \geq 6$, components are same then that section is said to be matched and afterward expand the segment tally C1 (say) by one.

(ii) Let A1 and A2 be the exhibits of reference picture and test picture separately holding number of dark pixels in every segment. Analyze for the accompanying condition around relating clusters of mark picture:

$$\sigma ref - \alpha < \sigma test < \sigma ref + \alpha$$

where, σref is the component of reference show A1, σtest is the comparing component of the test exhibit A2 and α is the middle of the road element which is the permitted variety in number of pixels. Mediocre element is a changing esteem as it fluctuates for distinctive sections relying upon the mark content in that segment. Mediocre variable might be a

$$\alpha = \frac{p\ X\ \sigma Ref}{100}$$

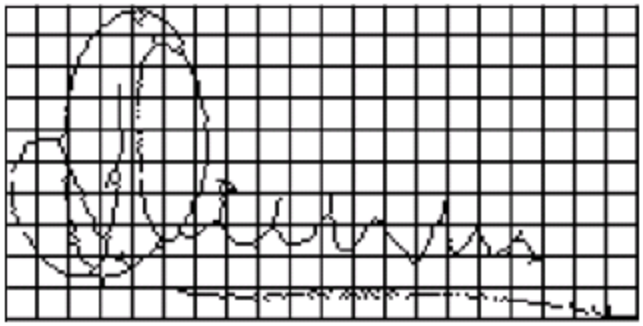


Fig 9 Grid over pre-processed signature

0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Fig 10 Matrix corresponding to above grid

where, p is percentage of black pixels in a column of a grid and σ_{ref} is the number of black pixels in that column. p can be obtained as:

$$p=(N \text{ X } \sigma_{ref})/100$$

where, N is total area of the cells having black pixels in that column and can be calculated as:

$$N = (\text{width X height}) \text{ X } c$$

where, c is the amount of cells which are a piece of the signature in that segment of a framework, width is the separation between two focuses in the flat projection and must hold more than 3 pixels in a cell, stature is the separation between two focuses in the vertical projection and must hold more than 3 pixels in a cell. In the event that condition (1) fulfills then that segment is worthy and increment the counter C2 (say) by one.

(iii) If C1 = n and C2 = n, then CMS is found to be 100%.

(iv) Boundary box zone ought to additionally exist in a middle of as far as possible. It may rely on our requisition. However all in all we take

$$0.98 area_{ref} < area_{test} < 1.2 area_{ref}$$

Signatures up to 60% CMS and if limit box exists in specified reach, are acknowledged for further preparing. In the event that CMS is underneath 60% then the test signature will be considered for further processing.

(b) Calculate Row Matching Score (RMS)

If CMS ≥ 60% then only we may calculate Row Matching Score (RMS). It is obtained in a similar fashion as that of CMS. All comparisons have to be done row wise. For RMS, $\beta \geq 14$. Calculate C1 and C2 for this case.

(c) Then we calculate the average of CMS and RMS.

(d) Threshold

Here the limit is the security level which the client needs to accomplish in the target provision. In the event that the client needs 100% security then include will be 100 and if the normal of the CMS and RMS is 100% then the mark will be acknowledged. On the off chance that the client needs 90% security then include will be 90 and if the normal is more terrific or equivalent to 95% then the mark will be acknowledged. Limit reach is from 100 to 65 i.e. most minimal security level for which comes about might be acquired in the proposed framework, is 65. On the off chance that normal is underneath 65% then that mark will be considered produce. Since the proposed method works for a breach of security levels, it could be utilized as a part of different provisions in which diverse level of security is needed for distinctive requisitions.

FAR (False Acceptance Rate): The false acknowledgement proportion is given by the amount of fake marks acknowledged by the framework as for the aggregate number of examinations made and is given by:

$$FAR = \frac{No.of\ Forgeries\ accepted}{No.of\ Forgeries\ tested}$$

FRR (False Rejection Rate): The false rejection rate is the aggregate number of real signature dismissed by the framework concerning the aggregate number of correlations made and is given by:

$$FRR = \frac{No.of\ Forgeries\ accepted}{No.of\ Forgeries\ tested}$$

FAR and FRR are the two parameters used for measuring the performance of any signature verification method. The purpose of verification is to reduce FAR and FRR.

We have ascertained FAR and FRR to assess the execution of the proposed framework. Distinctive qualities of limit are required to plot FAR versus FRR diagram. Here limit is the security level which could be set as per the target requisition.

FAR and FRR are contrarily corresponding to one another and expanding of one prompts diminishing of an alternate. Thus there requirements to be a bargain between these two. EER (Equal Error Rate) is the point where FAR and FRR get equivalent. Frequently it is utilized as a measure of signature verification system.

Chapter 8

Results and Conclusion

8.1 Comparison with Existing Methods:

We have contrasted the proposed strategy and the current three systems viz. Offline Signature Verification and Identification utilizing Distance Statistics which utilized the same standard Database B, Novel Features for Offline Signature Verification, and Offline Signature confirmation utilizing Local Radon Transform & SVM. It might be watched that the proposed calculation with matrix based characteristic extraction showed signs of improvement brings about terms of FAR and FRR.

TABLE 1: COMPARISON WITH EXISTING TECHNIQUES:

Technique	FAR(%)	FRR(%)
Offline Signature Verification and Identification using Distance Statistics [1]	34.91(Set1) 33.80(Set2)	28.33(Set1) 30.93(Set2)
Novel Features for Offline Signature Verification [2]	16.36	14.58
Offline Signature verification using Local Radon Transform & SVM[3]	22.0	19.0

TABLE 2: Signature verification results for set-1:

Threshold	**FAR(%)**	**FRR(%)**
95	**0**	**32**
90	**5.1**	**16**
80	**7.9**	**11**
75	**17**	**4**
70	**20**	**1.1**
65	**29**	**0**
Average	**12.6**	**10.2**

8.2 Performance Evaluation:

The execution of biometric check frameworks is regularly portrayed focused around terms, the false acknowledge rate (FAR) and a relating false reject rate (FRR). A false acknowledgement happens when the framework permits a falsifier's sign is acknowledged. A false reject proportion speaks to a legitimate client is rejected from getting access to the framework.

These two lapses are straightforwardly related, where a change in one of the rates will contrarily influence the other. A typical elective to depict the execution of framework is to figure the equivalent failure rate (EER). EER compares to the point where the false acknowledge and false reject rates are equivalent. With a specific end goal to outwardly remark the execution of a biometric framework, beneficiary working trademark (ROC) bends are drawn.

Biometric frameworks produce matching scores that speak to how comparable (or divergent) the info is contrasted and the put away format. This score is contrasted with a limit with settle on the choice of dismissing or tolerating the client. The limit quality might be changed so as to acquire different FAR and FRR fusions.

The ROC bend speaks to how the FAR progressions as for the FRR and the other way around.

A ROC bend sample is indicated. These bends can likewise be plotted by utilizing the bona fide acknowledge rate versus the false acknowledge rate. The certified acknowledge rate is gotten by basically one short the FRR.

FAR is conversely related to FRR.

Fig 11 Typical FAR vs FRR plot:

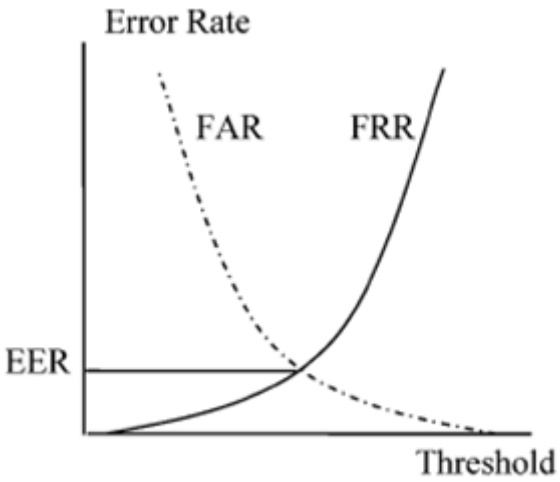
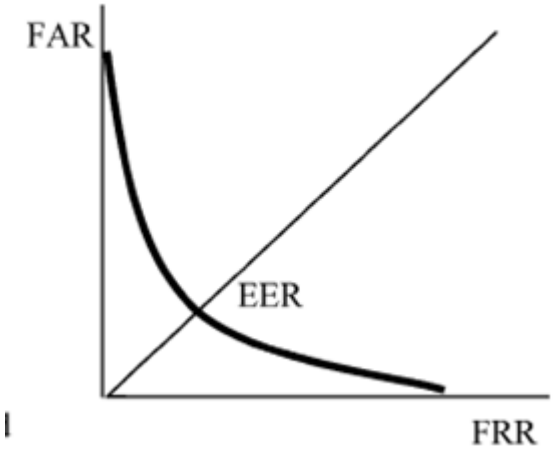


Fig 12 Typical plot to show EER:



8.3 Conclusion and Future Work:

In this paper, we have talked about an offline signature verification method utilizing grid based characteristic extraction. The preprocessed signature i.e. resized, binarized, diminished and pivot standardized mark is divided into lattice of size 10x20 cells where each one cell is having 100 pixels. Grid relating to network is structured and clusters holding number of dark pixels in columns and sections framed. For confirmation, these two characteristics for preparing and test pictures have been thought about both row and column and the test signature is then arranged in like manner.

Classifier hasn't been implemented yet and the results shown here are that of previous works in this field.

Bibliography

REFERENCES:

[1] 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, pp.1339-1360, 2004.

[2] Banshider Majhi, Y Santhosh Reddy, D Prasanna Babu, ‘‘Novel Features for Offline Signature Verification’’ ,International Journal of Computers,Communications & Control, Vol. I, No. 1, pp. 17-24, 2006.

[3] Vahid Kiani, Reza Pourreza, Hamid Reza Pourezza, “Offline Signature Verification Using Local Radon Transform and Support Vector Machines”, International Journal of Image Processing (IJIP), Vol.3, No.5, pp.184-194, 2010.

[4] Swati Srivastava, Suneeta Agarwal. “Offline Signature Verification using Grid based Feature Extraction” , International Conference on Computer & Communication Technology (ICCCT)-2011

[5] MEENAKSHI K. KALERA, SARGUR SRIHARI and AIHUA XU” OFFLINE SIGNATURE VERIFICATION AND IDENTIFICATIONUSING DISTANCE STATISTICS”, International Journal of Pattern Recognition and Artificial Intelligence Vol. 18, No. 7 (2004) 1339-1360.

[6] Sayantan Roy, Sushila Maheshkar. “Offline Signature Verification using Grid based and Centroid based Approach”
International Journal of Computer Applications (0975 – 8887) Volume 86 – No 8, January 2014

[7] Reliable On-Line Human Signature Verification Systems
Luan L. Lee, Toby Berger, and Erez Aviczer
IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 18, NO. 6, JUNE 1996.

[8] Automatic Signature Verification: The State of the Art
Donato Impedovo and Giuseppe Pirlo, Member, IEEE
IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 38, NO. 5, SEPTEMBER 2008