IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Signature Verification System

R. M. Samant[1], Mahendra Shilwant[2], Bhojraj Sarsambi[3], Mahesh Shelke[4]

Professor, IT Department, NBNSSOE Ambegoan, Pune, India [1]

Student, IT Department, NBNSSOE Ambegoan, Pune, India [2,3,4]

Abstract: Offline signature confirmation is one of most difficult region of personal authentication. Numerous strategies have been acquainted in literature to find whether a given signature is certifiable or phony. Signature is a vital part of distinguishing proof and validation of a object in this digitized world. Offline signature verification is a critical and troublesome procedure of signature verification. Signature is required by a specific client as a sender to presented himself in computerized world and also to make an impression on an element arranged at an alternate remote areas. With the goal that message can't be access to or modified by anybody other then whom the message to be intended to be accessed . As signature can be utilized as validation means by many organizations and association to secure there classified information and also for safeguard there protection because of which is less measure of information is accessible which is not adequate for acknowledgment of pattern utilized as a part of signature. This paper portrays a novel approach for signature verification and recognizable proof in a offline environment. In proposed work, A Signature picture is taken through some kind of sources like camera caught picture of signature or might be a transcribed signature then it will be actualized by executing picture through various techniques like signature acquisition, signature input ,signature thinning, boundary detection, feature extraction, signature recognition.

Keywords: Signature verification, Authentication, Signature acquisition, Feature extraction, Thinning.

I. INTRODUCTION

Despite endeavours toward the dematerialization of archives, the requirement for quick and exact paper-based record confirmation is as yet developing in our general public. The field of biometrics is an imperative range of study as it offers many focal points over more ordinarily utilized validation strategies, for example, picture ID cards, magnetic strip cards and so forth. These days, biometric innovations are progressively and all the more as often as possible being utilized to guarantee personality confirmation. Signatures regularly consolidate complex geometric pattern that make them a moderately secure means for approval for high security conditions. For chronicled reasons, the manually written Signatures keeps on being the most regularly acknowledged type of exchange affirmation, and in addition being utilized as a part of common law contracts, demonstrations of volition, or confirming one's personality. Some other offline signature verification applications incorporate the validation of bank checks, ID personal cards, administrative forms, formal agreements, acknowledgement of services received. Signature verification has been a point of serious research amid the previous quite a long while because of the critical part it plays in various territories, incorporating into money related applications. Considering the expansive number of signatures verified every day through visual examination by individuals, the development of a powerful and precise signature verification framework has numerous potential advantages for guaranteeing legitimacy of signature and diminishing extortion and different other crimes.. The objective of a signature verification framework is to have the capacity to check the character of an individual, in light of the investigation of his or her signature through a procedure that segregates a certifiable signature from a falsification. The check of human marks is especially worried with the change of the interface between people and PCs.

Contingent upon information obtaining system, there are two techniques for signature confirmation - Online or Dynamic and Offline or Static. Offline signature recognition is more troublesome than online as unique data are not accessible and it is hard to recuperate them from the disconnected pictures. In any case, necessity of gaining the signature on some uncommon game plan makes the online technique unacceptable for a large portion of the reasonable employments. Offline has the upside of utilizing it in an indistinguishable path from the current manual acknowledgment technique.

II. LITERATURE SURVEY

1 Online Signature Verification on Mobile Devices

This paper studies online signature verification on touch interface based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space. The algorithm was first tested on the well known MCYT-100 and SUSIG datasets. The

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

results show that the performance of the proposed technique is comparable and often superior to state-of-art algorithms despite its simplicity and efficiency.

2. Multimodal Biometric Template Authentication of Finger Vein and Signature Using Visual Cryptography
In this paper personal verification method using fingervein and signature is presented. Among many authentication systems finger-vein is promising as the foolproof method of automatic personal identification. Finger-vein and signature image is pre-processed and features are extracted using cross number concept and principle compound analysis. Fusion technique is used to fuse the finger vein and signature images. Then the visual cryptographic scheme is applied for the biometric template to generate the shares. The shares are stored in a separate database, and then the biometric image is revealed only when both the shares are simultaneously available.

3 Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing
The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm

4 Off-line signature verification and recognition: Neural Network Approach
This paper discusses signature verification and recognition using a new approach that depends on a neural network which enables the user to recognize whether a signature is original or a fraud. The user introduces into the computer the scanned images, modifies their quality by image enhancement and noise reduction techniques, to be followed by feature extraction and neural network training, and finally verifies the authenticity of the signature. The paper discusses the different stages of the process including: image pre-processing, feature extraction and pattern recognition through neural networks.

5 Signature Verification Using Neural Network
This scheme is based on the technique that applies preprocessing on the signature to get a binary image and then calculate the global and texture features points from it and maintain a feature vector. All calculations are done on the basis of these feature points. The feature vector obtained from the global and texture features is used to compare with the feature vector of incoming testing signature. Based on the values obtained, the network will decide the appropriateness of the signature. The suggested scheme discriminates between original and forged signatures using artificial neural network (ANN) for training and verification of signatures. The method takes care of simple and random forgeries and the skilled forgeries are also eliminated in greater extent. The objective of the work is to reduce two vital parameters, False Acceptance Rate (FAR) and False Rejection Rate (FRR). So the results are expressed in terms of FAR and FRR and subsequently comparative analysis has been made with standard existing techniques. Results obtained by our proposed algorithm are more efficient than most of the existing techniques.

III. MATHEMATICAL MODEL

Let ‗S' be the | signature to be verified as the final set
S = {……}
Identify the inputs as I
S = {U}, U= {U1, U2, U3, U4 …| ‗U' given user who give signature}
Identify the outputs as O
S = {V} V= {V1, V2, V3 …| ‗V' given verified signature}
Identify the functions as ‗F'
S = {…
F = {F1 (), F2(), F3(), F4(), F5(), F6(), F7()}
F1 (U) = Login to application, F2 (S) = Signature acquisition
F3 (S) = Signature input, F4 (S) = Thinning
F5 (S) = Boundary detection, F6 (S) =Feature recognition
F7 (V)=access application

IV. PREVIOUS WORK

This approach has problem in two steps. Initially a set of signatures are obtained from the subject and fed to the system. These signatures and preprocessed Then the preprocessed images are used to extract relevant geometric parameters that can distinguish signatures of different persons. These are used to train the system. The mean value of these features is

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

obtained. In the next step the scanned signature image to be verified is fed to the system. It is preprocessed to be suitable for extracting features. It is fed to the system and various features are extracted from them. These values are then compared with the mean features that were used to train the system. The Euclidian distance is calculated and a suitable threshold per user is chosen. Depending on whether the input signature satisfies the threshold condition the system either accepts or rejects the signature.

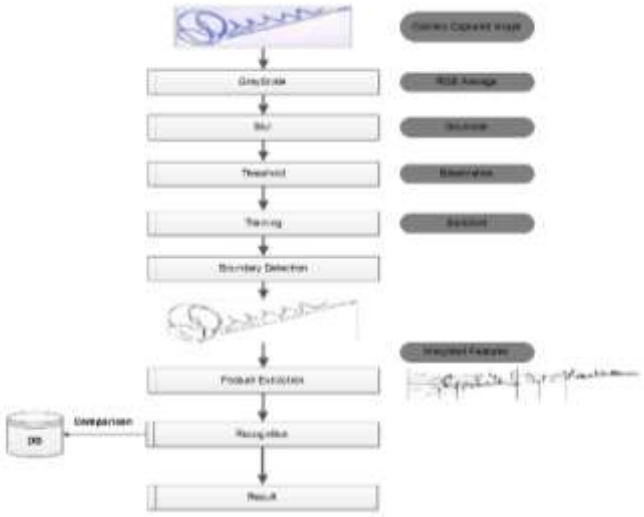
Disadvantage of existing system

High intra-class variability, Forgeries, Higher error rates than other traits, Affected by the physical and emotional state of the user, Large temporal variation

V. ALGORITHM DESCRIPTION

The structure of the proposed algorithm is straightforward. It works in two primary stages: feature extraction and feature matching. In the primary stage, the limits of the shapes from the information parallel pictures are followed. The removed contours are interpretation and scale-measure standardized, and a little arrangement of the in all likelihood beginning stages for both shapes are evaluated. In the second stage, the divergence measure is computed utilizing features extricated in the main stage. The beginning stages from both shapes are relegated into sets. Before assessing the disparity measure for a given combine of beginning stages, the revolution between these focuses is evaluated and one of the shapes is turned. The divergence between two shapes is figured for each match of beginning stages. The least general uniqueness is taken as the divergence measure between the two shapes.

VI. PROPOSED SYSTEM DIAGRAM



Signature aquisation:-

For offline signature verification system, images of the signatures are scanned using a digital scanner. Scanned images are stored digitally for offline processing.

THINNING

Diminishing is done to lessen the thickness contrasts by making the picture one pixel thick. To diminish the calculation time the diminishing procedure is finished. Diminishing is finished by utilizing the coupling point. This calculation is best for mark pictures since it save the mind boggling points of interest and different properties of the signature.

Feature Extraction

A perfect feature extraction method removes a negligible feature set that augments relational separation between mark cases of different people while limiting intrapersonal separate for those having a place with a similar individual. Features removed for disconnected mark confirmation can be extensively isolated into three principle classes

Global Features

Local Features

Geometric Features

Global features: The signature is viewed as a whole and features are extracted from all the pixels confining the signature image.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Local features: Local elements are separated from a bit or a restricted zone of the mark picture . These elements are figured to portray the geometrical and topological attributes of local fragments, for example, position, digression bearing, and bend. These elements are for the most part gotten from the dispersion of pixels of a signature, for example, local pixel thickness or inclination.
Geometric features: These features describe the characteristic geometry and topology of a signature and preserve their global as well as local properties.

VII. RELATED WORK

To enhance proficiency, Researchers are utilized distinctive strategies with the end goal of signature verification framework some of them are as per the following
1.The offline signature verification framework proposed in joins some factual classifiers. This signature verification framework comprised of three stages – the initial step is to transform the first signatures utilizing the character and four Gabor transform, the second step is to intercorrelate the investigated signature with the also transformed signatures of the learning database and after that in the third step verification of the realness of signatures by combining the choice identified with each transform.
2. A programmed disconnected signature verification framework introduced in is worked with a few measurable techniques. They utilized Hidden Markov Modeling (HMM) technique to assemble a reference display for every nearby component.
3. Another framework proposed in depended on worldwide, lattice and surface elements. For every one of the capabilities a unique two phase recognition OCON (one-class-one-network) classification structure was actualized .In the main stage, the classifier consolidated the choice aftereffects of the neural networks and the Euclidean separation acquired utilizing the three capabilities. The consequences of the primary stage classifier bolster a moment arrange outspread base function (RBF) neural network structure, which settled on a ultimate conclusion
4. A proposed framework in depends on a contour matching algorithm. They utilized the geometrical properties of the signature and considered the inescapable intrapersonal varieties for the client set. These are some of related work of signature verification however every one of these techniques are not equipped for handle the various types of fabrications in various conditions yet the scientists are growing more solid and competent techniques to distinguish various types of signature frauds.

VIII. CONCLUSION AND FUTURE WORK

The proposed work is to enhance the precision of the secured offline signature system. The signature pictures are pre-handled and components are separated from the signature utilizing cross number idea and standard compound examination at the same time. Hence the exploratory aftereffect of the proposed framework accomplishes secure verification result. Later on work distinctive combination system can be connected to improve the execution of the model and likewise the number of shares can be expanded to improve the check level.

REFERENCES

1. Banshidhar Majhi, Y. Santhosh Reddy and D. Prasanna Babu, 2006. Novel features for offline signature verification. Int. J. Comput. Commun Control, 1: 17-24. http://www.journalunivagora.ro/download/pdf/20.pdf.
2. Brault, J.J. and R. Plamondon, 1993. Segmanting handwritten signatures at their perceptually important points. IEEE Trans. Pattern Anal. Mach. Intel., 15: 953-957. http://doi.ieeecomputersociety. org/10.1109/34.232079.
3. Edson, J., R. Justino, F. Bortolozzi and R. Sabourin, 2005. "A comparison of SVM and HMM classifiers in the off-line signature verification. Pattern Recognit. Lett., 26: 1377-1385. http://dx.doi.org/10.1016/j.patrec. 2004.11.015.
4. Edson, J., R. Justino, F. Bortolozzi and R. Sabourin, 2001. An off-line signature verification using HMM for random, simple and skilled forgeries. In: 6th International Conference on Document Analysis and Recognition, September, pp: 1031-1034. http://doi.ieeecomputersociety.org/10.1109/ICDAR.2001.95394
5. Edson, J., R. Justino, F. Bortolozzi and R. Sabourin, 2002. The interpersonal and intrapersonal variability influences on off-line signature verification using HMM. Proceeding XV Brazilian Symposium Computer Graph and Image Processing, pp: 197-202. http://ieeexplore.ieee. org/iel5/8352/26315/01167143.pdf?arnumber=116 7143.
6. Edson, J., R. Justino, A. El Yacoubi, F. Bortolozzi and R. Sabourin, 2000. An off-line Signature Verification System Using HMM and Graphometric features. DAS, pp: 211-222. http://www.livia.etsmtl.ca/publications/2000/JustinoDAS.pdf.
7. Fang, B., C.H. Leung, Y.Y. Tang, K.W. Tse, P.C.K. Kwok and Y.K. Wong, 2003. Off-line signature verification by the tracking of feature and stroke positions. Patter Recognit., 36: 91-101. http://dx.doi.org/10.1016/S0031-3203(02)00061-4.
8. Migual, A.F., B.A. Jesus and M.T. Carlos, 2005. Off-line geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Tran. Pattern. Anal. Mach. Intel., 27: pp. 993-97http://dx.doi.org/10.1109/TPAMI.2005.125
9. Plamondon, R. and S.N. Srihari, 2000. Online and offline handwriting recognition: A comprehensive survey. IEEE Tran. Pattern Anal. Mach. Intel., 22: 63-84.http://doi.ieeecomputersociety.org/10.1109/34.824821.
10. Zimmer, A. and L.L. Ling, 2003. A hybrid on/off line handwritten signature verification system. In: 7th International Conference on Document Analysis and Recognition, 3-6 August 2003, Edinburgh, Scotland, UK. IEEE Computer Society 2003pp:424-428. http://doi.ieeecomputersociety.org/10.1109/ICDAR.2003.1227702.