INCORPORATION OF MULTIMODAL SUBSTANTIATION VIA CROSS DISCOVERY & ANDROID BASED GRAPHICAL PROTOTYPE STUDY

Dr.N.Pughazendi [1],R.Sathishkumar[2] , S.Subburaj[3], B.Mukunth[4]
Professor [1,] Assistant Professor[2,3,]UG Scholar [4]
Department of Computer Science Engineering, Panimalar Engineering College Chennai
pughazendi@yahoo.com[1], mukunthbalaji1@gmail.com[2] ,satz.lic@gmail.com[3,] subburajs87@gmail.com[4]

ABSTRACT

Abstract- within the Existing System, web banking applications became a lot of and a lot of complicated, it's unsecured one. within the projected SYSTEM, web banking once registering the applying for the token, a signature or a collection of them is scanned and keep within the internal memory of the token. we have a tendency to projected a brand new framework for corroborative the written signature victimization jointly the CT and therefore the feature unsimilarity live. The verification step is performed victimization solely the feature unsimilarity live for evaluating signature's likeness. within the MODIFICATION method, we have a tendency to ar implementing Multimodal based mostly user verification system. thus we have a tendency to ar combining automaton based mostly Pattern Authentication System with signature verification. Neural network & Back Propagation algorithmic program is employed for signature Verification, once successful authentication of signature verification, automaton based mostly Graphical word is verified. User are going to be registering with 2 pictures and with its Pixels. User must choose an equivalent Set of pictures and same picture element Values for Authentication. User is etch as long as each signature and automaton based mostly Graphical word is matched.

Key words: web banking, signature verification, Android based mostly graphical word.

I INTRODUCTION

THE growing interest toward identity authentication is today targeted upon the best severity level criteria for a whole automation of security systems. Among biometric systems, the written signature verification is one amongst the foremost wide used since it's recognized as a legal means that for individual verification in body and monetary establishments. it's conjointly one amongst the foremost complicated biometric applications as a result of the verification relies on the analysis of the written activity action. the most perplexity is that, on one hand, the activity facet of handwriting is characteristically specific to every author and, on the opposite hand, the relevance of machine-driven system lies on its generalized relevancy to any or all writers. Moreover, a high similarity between 2 signatures doesn't essentially mean that they need been written by an equivalent person. In fact, this case will occur once the signature had been skilfully reproduced by another person. Conversely, an occasional similarity between 2 signatures doesn't essentially mean that it comes from 2 completely different writers thanks to the intra-writer variability. The signature analysis will, therefore, develop into a particularly complicated drawback requiring completely different disciplines to be concerned. within the rhetorical domain, the acceptableness of writer's handwriting individuality as scientific testimony had been subjected to many ruling in courts few decades past. A rigorous study provided in explains this scientific validation in courts victimization some macro and micro-features from a written document. it's been established that 2 writers may be distinguished and thus known through the handwriting with a ninety eight confidence which the boldness level might be close to 100 percent once considering finer options.

Some challenges of the sensible and rhetorical processes of automatic signature verification were unnoticed in previous written Signature Verification Systems till the previous few years like the big variety of users, the restricted variety of reference signatures out there per author and therefore the dependency of the model on the owner. Thus, an excellent effort has been undertaken to additional refine HSVS and, today high level of accuracy is earned through varied off-line written signature verification systems which might be conducted consistent with 2 verification procedures referred to as writer-dependent (WD) and writer-independent (WI).The classical WD consists of making a reference model for every author, generated as a results of his/her nonheritable samples, and therefore the questioned signature of the claimed author is compared to his/her own model throughout the verification stage. the most disadvantage of this approach is that the have to be compelled to generate a model for every new author that isn't appropriate because of the big variety of users. The second approach, utilized by rhetorical consultants relies on the duality remodel that permits a multi-class drawback to be remodeled into bi-class one, i.e. real or forgery category. a lot of exactly, feature vectors generated between pairs of handwriting patterns ar remodeled into the unsimilarity vectors to be used for coaching one classifier, then, the classifier is employed to match a questioned handwriting pattern to at least one or a lot of references.

The advantage of this approach is to alleviate the difficulties of planning a WI system with restricted variety of reference handwriting patterns from an outsized variety of users. Usually, building one model may be achieved employing a binary classifier trained on real signatures against counterexamples like forgery or random signatures. throughout the verification step, a questioned signature is initial remodeled by duality procedure, which is able to be submitted to the binary category ifier that attributes the questioned signature to the accepted or rejected class. the most aim of the project is that we have a tendency to implementing Multimodal based mostly user verification system. thus we have a tendency to ar combining automaton based mostly Pattern. The Authentication System with signature verification. Neural network &amp; Back Propagation algorithmic program is employed for signature. The signature is verified once successful authentication of the signature. The automaton based mostly Graphical word is verified. The User are going to be registering with 2 pictures and with its Pixels. User must choose an equivalent Set of pictures and same picture element Values for Authentication. User is echt as long as each signature and automaton based mostly Graphical word are matched.

II DRAWBACK

The signature analysis can, therefore, be born-again into a awfully sophisticated draw back requiring fully completely different disciplines to agonize. The user revocation and re-registration with constant identity may cause the user impersonation attack, once degree authentication theme distributes the static secret tokens. Therefore, springing up with degree economical approach to tackle of user revocation whereas supporting strong user trait becomes a tough drawback.

III LITERATURE SURVEY

In 2015[1] Luiz G. Hafemann presented in the Int.Conf. Appln.titled as “Offline Handwritten Signature Verification -Literature Review”

In this paper, the area of Handwritten Signature Verification has been broadly researched in the last decades and still remains as an open research problem. This report focuses on offline signature verification, characterized by the usage of static (scanned) images of signatures, where the objective is to discriminate if a given signature is genuine(produced by the claimed individual), or a forgery (produced by an impostor). We present an overview of how the problem has been handled by several researchers in the past few decades and the recent advancements in the field.

In 2011[2] Mustafa BerkayYilmaz presented in the IEEE Int.Conf. titled as “Offline Signature Verification Using Classifier Combination of HOG and LBP Features”. In this paper, we present an offline signature verification system basedon a signature’s local histogram features. The signature is divided into zones using both the Cartesian and polarcoordinate systems and two different histogram features arecalculated for each zone: histogram of oriented gradients(HOG) and histogram of local binary patterns (LBP).The classification is performed using Support Vector Machines (SVMs), where two different approaches for training are investigated, namely global and user-dependentSVMs. User-dependent SVMs, trained separately for eachuser, learn to differentiate a user’s signature from others,whereas a single global SVM trained with difference vectors of query and reference signatures’ features of all users,learns how to weight dissimilarities. The global SVM classifier is trained using genuine and forgery signatures ofsubjects that are excluded from the test set, while userdependent SVMs are separately trained for each subject using genuine and random forgeries.The fusion of all classifiers (global and user-dependentclassifiers trained with each feature type), achieves a15.41% equal error rate in skilled forgery test, in the GPDS-160 signature database without using any skilled forgeries in training.

In 2008[3] DonatoImpedovo and Giuseppe Pirlo presented in the IEEE Int.Conf., titled as “Automatic Signature Verification:The State of the Art”.

In recent years, along with the extraordinary diffusion of the Internet and a growing need for personal verification in many daily applications, automatic signature verification is being considered with renewed interest. This paper presents the state of the art in automatic signature verification. It addresses the most valuable results obtained so far and highlights the most profitable directions of research to date. It includes a comprehensive bibliography of more than 300 selected references as an aid for researchers working in the field.

In 2001[4] Sargur N. Srihari presented in the IEEE Int.Conf, titled as “:Establishing Handwriting Individuality Using Pattern Recognition Techniques”.

We undertook a study to objectively validate the hypothesis that handwriting is individualistic. Handwriting samples of one thousand five hundred individuals, representative of the US population with respect to gender age, ethnic groups, etc., were obtained. Analyzing differences in handwriting was done by using computer algorithms for extracting features from scanned images of handwriting. Attributes characteristic of the handwriting were obtained, e.g., line separation, slant, character shapes, etc. These attributes, which are a subset of attributes used by expert document examiners, were used to quantitatively establish individuality by using machine learning approaches. Using global attributes of handwriting and very few characters in the writing, the ability to determine the writer with a high degree of confidence was established. The work is a step towards providing scientific support for admitting handwriting evidence in court. The mathematical approach and the resulting software also have the promise of aiding the expert document examiner.

In 2013[4]Youbao Tang presented in the IEEE Int.Conf. Titled as "Offline text-independent writer identification using stroke fragment and contour based features"

This paper proposes a novel approach for offline text-independent writer identification. The proposed approach extracts two new features: Stroke Fragment Histogram (SFH) and Local Contour Pattern Histogram (LCPH). For SFH extraction, a handwriting image is firstly segmented into many stroke fragments (SFs) by using the proposed fragment segmentation method based on sliding window. Then all SFs extracted from training dataset are clustered to generate a codebook by using the Kohonen SOM 2D clustering algorithm. All SFs extracted from test datasets are adopted to compute SFHs by the proposed feature extraction method based on codebook. For LCPH extraction, the contour of an input handwriting image is firstly obtained Then a LCPH is formed to characterize the writer's individuality by tracking every contour point. For feature matching, the chi-square distance is employed to measure the similarity between SFHs and LCPHs. After feature matching, both similarities are fused for final decision by simple weighted sum. Three public handwriting datasets are used to evaluate the proposed approach and the experimental results show that the proposed approach can get the best performance compared with the state-of-the-art text-independent writer identification algorithms in all of these datasets.

In 2015[5] Osama Mohamed Elrajubi presented in the IEEE Int.Conf. Titled as "Angle features extraction of handwritten signatures"

The selection of the signatures' features is crucial for the success of any signature verification system. The features of signature can be divided into global features and local features. Local features represent a segment or limited region of the signature image. Although, they require more computations; they are much more accurate than global features. In this paper, feature extraction using angle features has been studied and implemented in system of handwritten signature verification in many methods which differ in the way of determining the width and the height of each part, and differ in determining the number of parts in dividing signature image. The efficiency of the system for each method has been tested on a local database. The local database of 880 signatures taken from 40 persons has been developed in this study.

In 2012[6]D. Impedovo,G. Pirlo, presented in the IEEE Int.Conf. Titled as "Handwritten Signature Verification: New Advancements and Open Issues"

Recently, research in handwritten signature verification has been considered with renewed interest. In fact, in the age of e-society, handwritten signature still represents an extraordinary means for personal verification and the possibility of using automatic signature verification in a range of applications is becoming a reality. This paper focuses on some of the most remarkable aspects the field and highlights some recent research directions. A list of selected publications is also provided for interested researchers.

In 2007 [7]Marius Bulacu presented in the IEEE Int Conf. Titled as
"Text-Independent Writer Identification and Verification Using Textural and Allographic Features"

The identification of a person on the basis of scanned images of handwriting is a useful biometric modality with application in forensic and historic document analysis and constitutes an exemplary study area within the research field of behavioral biometrics. We developed new and very effective techniques for automatic writer identification and verification that use probability distribution functions (PDFs) extracted from the handwriting images to characterize writer individuality. A defining property of our methods is that they are designed to be independent of the textual content of the handwritten samples. Our methods operate at two levels of analysis: the texture level and the character-shape (allograph) level. At the texture level, we use contour-based joint directional PDFs that encode orientation and curvature information to give an intimate characterization of individual handwriting style. In our analysis at the allgraph level, the writer is considered to be characterized by a stochastic pattern generator of ink-trace fragments, or graphemes. The PDF of these simple shapes in a given handwriting sample is characteristic for the writer and is computed using a common shape codebook obtained by grapheme clustering. Combining multiple features (directional, grapheme, and run-length PDFs) yields increased writer identification and verification performance. The proposed methods are applicable to free-style handwriting (both cursive and isolated) and have practical feasibility, under the assumption that a few text lines of handwritten material are available in order to obtain reliable probability estimates.

In 2016 [8] Nan Lipresented in the IEEE Int Conf.Titled as "Online Signature Verification Based on Biometric Features"

Since current signatures are generally not verified carefully, frauds by forging others signature always happen. This paper tried to authenticate user automatically with electronic signatures on mobile device. We collected coordinates, pressure, contact area and other biometric data when users sign their name on touch screen smart phone. Then we used four different classification algorithms, Support Vector Machine, Logistic Regression, AdaBoost and Random Forest to build a specific signature verification model for each user, and compared the verification accuracy of these algorithms. The experimental result on 42 persons' dataset shows that these four algorithms have satisfactory performance on Chinese signature verification, and Adaboost has the best performance with error rate of 2.375%.

IV SYSTEM STUDY

Existing System

In The Existing System Internet Banking Applications Have Become More and More Complex, It Is Unsecure One.

Disadvantages

- Unreliable
- Less Data Transmission Rate
- Less Effective
- Less Security

Proposed System

In the proposed system, internet banking when registering the application for the token, a signature or a set of them is scanned and stored in the internal memory of the token. We proposed a new framework for verifying the handwritten signature using conjointly the ct and the feature dissimilarity measure. The verification step is performed using only the feature dissimilarity measure for evaluating signature's resemblance.

Modification Process

In the modification process, we are implementing multimodal based user verification system. So we are combining android based pattern authentication system with signature verification. Neural network & back propagation algorithm is used for signature verification, after successful authentication of signature verification, android based graphical password is verified. User will be registering with two images and with its pixels. User has to select the same set of images and same pixel values for authentication. User is authenticated only if both signature and android based graphical password are matched.

Advantages:

- Reliable
- High data transmission rate
- More effective
- High security

V ARCHITECTURE DIAGRAM

The user enters his user name and password to authenticate in the system. Once the password is correct, the user has to write his signature using the mouse which is explained in Figure 1. The server verifies the user's signature and checks the signature is matching or not. Once the signature is verified, the second Authentication is done in the mobile by entering the password. If both the password and the signature match each other then we can use net banking.

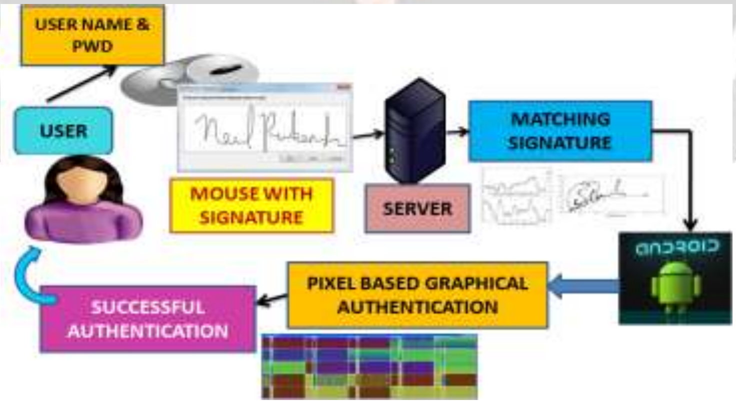

Figure No1: Architecture Diagram

VI MODULES

User Registration

In this module we are going to create a User application by which the User is allowed to access the data from the Server which is explained in Figure 2.

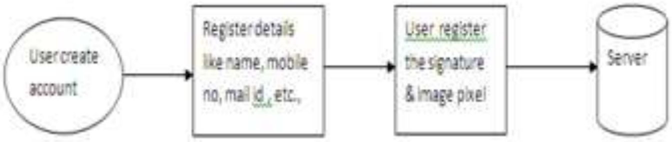
User create account
Register details like name, mobile no, mail id , etc.,
User register the signature & image pixel
Server

Figure No2: User Registration Process

Here first the User wants to create an account and then only they are allowed to access the application. To access the Application, the Client wants to the register their details with Application Server. They have to provide their information like Name, Password, Date Of birth, Mobile Number and etc. his information will store in the database of the Application Server. The User is allowed to the access the application only by their provided Interface. User register will the signature, finger print and also register the two images with its pixels. In this phase, the we'll train the system according to identify the User's Finger by using the finger print device, so the user have give the finger print to train the system to identify the correct finger print to valid the user.

Server

The Server Application can be created using Java/ Dot Net Programming Languages. The Server will monitor the Mobile Client's accessing information and Respond to Client's Requested Information. The Server will not allow the Unauthorized User from entering into the Network. So that we can provide the network from legitimate user's activities. Also the Server will identify the Malicious Nodes activities which is explained in Fig 3.

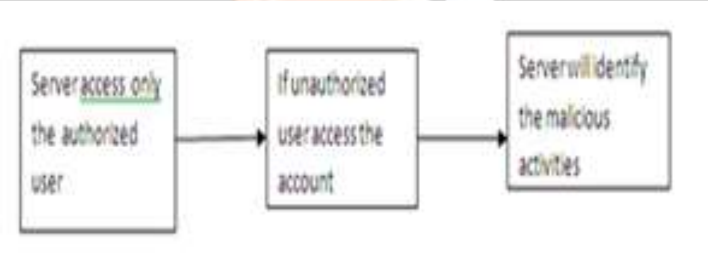
Server access only the authorized user
If unauthorized user access the account
Server will identify the malicious activities

Figure No3: Server Process

Signature Training

In this phase, the we'll train the system according to identify the User's Signature by using the mouse so the user have to gives 20 times of signature to train the system, here we are not using signature device which cost effective instead we use mouse signature to valid the user which is explained in figure 4.

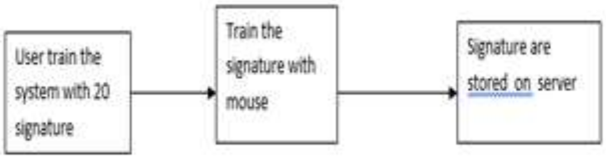
User train the system with 20 signature
Train the signature with mouse
Signature are stored on server

Figure No 4: Signature training process

Android – Graphical Password

In this module, can build image verifications against specific elements for pixel-by-pixel visual verifications in tests. The image verification feature is based on an element's visual rendering rather than the properties or attributes of that element.

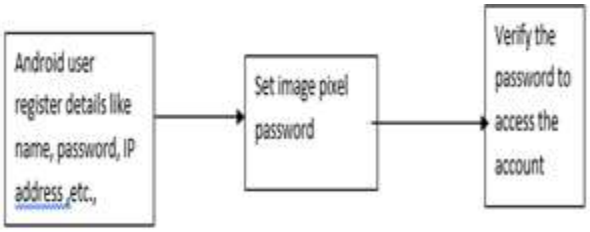
Android user register details like name, password, IP address ,etc.,
Set image pixel password
Verify the password to access the account

Figure No4: Android Graphical Password Process

An application with rich graphic rendering can leverage this functionality to automate some of its test scenarios that have always needed manual visual inspection to verify.

The image verification in test Studio allows you to refine your verification area down to the pixel level within an element and also assign error tolerance for the matching.

Multi Modal Authentication & Transaction

In this module, we can design and implementation of multimodal authentication. Verify the finger print , signature and pixel based images afterwards only success the transaction.

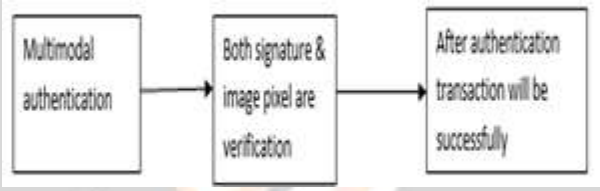
Multimodal authentication
Both signature & image pixel are verification
After authentication transaction will be successfully

Figure No5: Multi modal Authentication & Transaction Process

.

VII CONCLUSION

We proposed in this paper a new framework for verifying the handwritten signature using conjointly the CT and the feature dissimilarity measure. The writer-independent concept is combined with one-class verification using a reduced number of genuine references. Moreover, the system does not need any robust classifier such as SVM or Neural Networks to be trained on dissimilarities. The verification step is performed using only the feature dissimilarity measure for evaluating signature's resemblance. A unique WI decision threshold deduced from the stability parameter is required to verify signatures independently of datasets. The proposed system doesn't refer to any simple or skilled forgery model and can be developed with a reduced number of reference signatures. Experimental results have shown the possibility of developing a global system that can be deployed in many institutions. The Future work targets at further improving resultant system accuracy by fine tuning the selection of individual features (coefficients) that enhance the variation between genuine and forgery signatures. Also, improving the performance by selecting correlated genuine signatures as the training samples. Moreover, looking for better methods for selecting coefficients that represent intra personal features and hence could improve system performance. Furthermore, to compare performance of this system to performance of other systems when using same online handwritten signatures databases.

Reference

[1] D. Impedovo, G. Pirlo, and R. Plamondon, "Handwritten signature verification: New advancements and open issues," in Proc. 13th Int. Conf.Frontiers Handwriting Recognit., Bari, Italy, Sep. 2012, pp. 367–372.

[2] S. N. Srihari, S. H. Cha, H. Arora, and S. Lee, "Individuality of handwriting," J. Forensic Sci., vol. 47, no. 4, pp. 1–17, Jul. 2002.

[3] D. Rivard, E. Granger, and R. Sabourin, "Multi-feature extraction and selection in writer-independent off-line signature verification," Int. J.Document Anal. Recognit., vol. 16, no. 1, pp. 83–103, Mar. 2013.[4] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers," Pattern Recognit., vol. 43, no. 1, pp. 387–396, Jan. 2010.

[5] S. N. Srihari, A. Xu, and M. K. Kalera, “Learning strategies and classification methods for off-line signature verification,” in Proc. 9th Int.Workshop Frontiers Handwriting Recognit., Tokyo, Japan, Oct. 2004, pp. 161–166.

[6] S.-H. Cha and S. N. Srihari, “Writer identification: Statistical analysis and dichotomizer,” in Advances in Pattern Recognition. Berlin, Germany: Springer, 2000, pp. 123–132.

[7] C. Santos, E. J. R. Justino, F. Bortolozzi, and R. Sabourin, “An offline signature verification method based on the questioned document expert’s approach and a neural network classifier,” in Proc. 9th Int.Workshop Frontiers Handwriting Recognit., Tokyo, Japan, Oct. 2004, pp. 498–502.

[8] A. Bensefia, T. Paquet, and L. Heutte, “A writer identification and verification system,” Pattern Recognit. Lett., vol. 26, no. 13, pp. 2080–2092, 2005.