International Journal of Technology and Engineering System (IJTES)
Vol 6. No.3 – Jan-March 2014 Pp. 230-234

available at : www.ijcns.com
ISSN: 0976-1345

ACCESSING RESTRICTED WEB SERVICES USING MOBILE PHONES WITH FACE AND SIGNATURE RECOGNITION

Princy.K[1] and R.Muthuvenkatakrishnan[2]
Department of CSE
PRIST University.,
Thanjavur-613 403.
Email:jk.princy@yahoo.com[1] , muthubrillia@gmail.com[2]

ABSTRACT

In this paper an application has been proposed that allows a mobile phone to capture signature signals and recognize face to authenticate a user for accessing restricted web services such as banking service etc. The captured features are later recognized during a standard web session. The face is recognized using Eigen face-based facial recognition and in this the relative distance between eyes, nose, mouth etc., are calculated. The signature verification is done using HMM (Hidden Markov Model) based on score function. This signature verification system is adapted for a handheld device based on certain signature features. The experiment uses a single fast normalized cross-correlation matcher and simple sum rule fusion technique based on face and signature traits of a user to improve the accuracy rate. The proposed architecture can be used in a personal computer (PC), thus allowing a multiplatform (PC, personal digital assistant (PDA), mobile phone, etc.) biometric web access.

Keywords: Biometrics, Smart phones, Web service, HMM, Eigenface.

1.INTRODUCTION.

Biometric person recognition.This is the use of unique human characteristics (i.e., biometrics) to recognize the user. Biometrics can be divided into two categories based upon the underlying characteristic they are using: 1. Physiological which is based on direct measurements of a part of the human body (e.g., iris, fingerprint, face, hand shape, etc.), and 2. behavioural, which is based on measurements and data derived from an action performed by the user and, thus, indirectly measuring some characteristics of the human body (e.g., voice, keystroke dynamics, signature-handwriting, gait, etc.)[1].

The Application used nowadays needs a lot of authentication which bring the manner to restrict the access to a system, allowing the entrance only to those persons who know a specific code, own a card or have determined physic marks. The more complex is the system, the most difficult is to be attacked, although it will be more expensive and will require more software and hardware resources. When a new authentication system is implanted, it is essential a judgement between simplicity, price and efficiency, as well as social acceptability.

Disadvantages of password and tokens. The password method is the cheapest and simplest technology, because it only requires elementary software resources.On the other hand, this system is easily attackable, since it is quite simple to obtain the data from a person, either extracting the information to the person itself using deceits, or attacking the software of the system.

The Smart Cards are very useful since they can be easily combined with other authentication systems, serving as storage system. Self-containment of smart card makes it resistant to attack as it does not need to depend upon potentially vulnerable external resources. But its small size and bend requirements (which are designed to protect the card physically), limits the memory and processing resources. And used like the only identification system, is not excessively trustworthy, since it can be easily stolen, lost or simply forgotten at home. Besides, sometimes they are combined with cryptography methods, which makes them more difficult (more expensive) to implement.

Advantages of biometrics. The advantage that Biometrics presents is that the information is unique for each individual and that it can identify the individual in spite of variations in the time (it does not matter if the first biometric sample was taken year ago).The pillars of e-learning security are: authentication, privacy (data confidentiality) authorization (access control), data integrity and non-repudiation. Biometric is a technique that can

provide all this requirements with quite lot reliability.

Web Services. A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

The proposed architecture is highly versatile. User terminal can be any device capable of capturing face signals and online signatures. It is also highly scalable, since we can use powerful servers capable of managing several transactions in parallel, not only HTTP-based but using any other secured or unsecured protocols. Several applications that can use the proposed architecture are e-banking, e-commerce, Login, POS (Point-of-Sale), Physical Access Control, Medical records management, e-Government, and Electronic data security.

Mobile Banking. Mobile banking has become very attractive and useful facility from customers and services provider point of view. However, this domain has evidenced many security threats. Attackers target this domain for financial or other benefits. In spite of many security measures being taken by mobile service providers and application providers, still there are vulnerabilities that may be exploited by adversaries. The threats include intruding from a remote place and physical theft[2].

Mobile banking domain uses small hand held devices including mobile phones that have limited resources such as energy, storage and processing power. This is also one of the reasons for their vulnerability. The security mechanisms that are used in PC world are not suitable to mobile world due to the difference intheir capacity in having resources. This warrants having different security measures for mobile banking.

Multibiometrics. Biometric systems based on single source of information are called unimodal systems. Although some unimodal systems (e.g. Face, Iris, Palm, Fingerprint) have got considerable improvement in reliability and accuracy, they have suffered from enrolment problems due to non-universality of biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data[3].Hence, single biometric may not be able to achieve the desired performance requirement in real world applications.

One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision achieved through fusion. Studies havedemonstrated that multimodal biometric systems can achieve better performance compared with unimodalsystems.The Multi-biometric systems can incorporate information from multiple modalities, instances, sensors, samples.

Our approach is named as Input Pattern Based Authentication Method. This makes use of biometric feature to ensure security in mobile transactions. It prevents financial frauds being witnessed in mobile banking domain. Tough screens are provided with many mobiles. Users use their fingers or a stylus pen for the purpose of giving input to the mobile device.

2.ARCHITECTURE.

A general biometric system consists of the following four modules.

1) Sensor module (or biometric reader): This is the interface between man and machine; therefore, the system performance depends strongly on it.

2) Feature-extraction module: The data provided by the sensor must first be validated from thepoint of view of quality, refusing it when the quality is too poor, and, second, extracting the features that represent,in the best possible way, the identity of the individual.

3) Matcher and decision-making module: The extracted featuresare compared with the stored templates to generate a score to determine whether to grant or deny access to the system.

4) Database system: This is the repository of the biometric information. During the enrollment phase, the templates are stored along with some additional personal information, such as name, address, etc.

The main modules of the proposed architecture are

1) **Client Tier**.

On the client side, the biometric acquisitionsoftware is deployed. Since there are no standard software solutions for web browsers to capture biometric data, this part should be distributed “ad hoc” for each type of platform. For this reason, our architecture proposes to leave only the data-capturing module on the client side, with the rest of the modules at the server side. This means that the applications developed need no special memory or processing requirements, since the main computer load falls on the execution of a web navigator and standard mobile devices (e.g., touch screen, microphone, camera, etc.) are used to capture the biometrics; then, our proposal can be run in, practically, any current mid-range to high-range mobile devices.

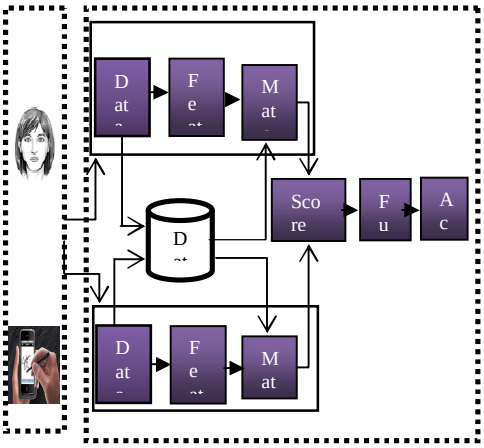

Fig: 1Client-server archi of face and signature modal

1) Embedded browser.in charge of the navigation and accessing to the web service;

2) Biometric capturer.in charge of calling and managing themobilecapture devices;

3) Biometricuploader.in charge of sending the biometric data to the server and managing this uploading. This modularity allows that we can switch between the executionof components without breaking the web session, whichis important for a secure and standard web access. Besides, the modularity allows the easy exchange of functionalities between components, as it happens in the applications implemented.

2) Server Tier:

The server side contains the main parts ofthe functionality of the proposed architecture. The components at this tier are the following.

1) Web server. This is responsible to collect the data sent by the data-capturing software on the client side, and passing it to the security module. Its mission is also to ensure that incoming data are consistent and come from reliable sources. Some examples of tasks carried out in this module are checking access lists, user names, algorithms for checking the validity of HTTP sessions, countermeasure detection of attacks by automated systems, etc.

2)Data processing module. This is in charge of collectingthe data received by the web server and storing for subsequent processing by other components of the system. Itconsists of following three modules.

a) Module for data collection and storage: Its functionis to extract data from HTTP variables and to pass the data to the validation module.

3)Validationmodule. This is responsible for verifying that the data received are correct, checking, for example, that required fields are populated and have the expected format. Its output is sent to the storage module.c) Storage module: This packages and stores the data in the system database.

4)Extractionmodule. Thiscollectsrawbiometricdataand prepares them for processing by the verification engine.It has the following modules.

a) Feature-extraction module: This is based on biometricdata supplied by the server-side capturing engine, and it generates the feature vectors.

b) Temporal normalization module: This is an optionalmodule used to obtain fixed-size temporal sequences of feature vectors.

c) Features-normalization module: In addition to obtainingthe features vector or sequence of feature vectors, it is usual to perform further geometric (i.e., zoom, rotation, or translation) or statistical (i.e., z-norm, min–max, etc.) transformations.

5)Databasesystem. Thiscontains information from theusers of the system (i.e., users database subsystem) andtheir biometric templates (i.e., users templates subsystem).

6) Verification engine. This module decides whether the access to the system is granted or denied to the user. It consists of the following modules.

a) Matcher module: This compares the information received against the template of the client stored in the database, thereby generating a numeric comparison score.

b) Score-normalization module: This is to improve thesystem performance or to use a universal decision threshold.

c) Decision module: From the comparison of the score with a decision threshold, this determines whether the user is accepted or rejected and is, thus, granted or denied access to the system or protected services.

7) Output module. This transmits the output back to theclient.

3.SYSTEM DESCRIPTION.

3.1 Face recognition

The task of facial recognition is discriminating input signals (image data) into several classes (persons). The input signals are highly noisy (e.g. the noise is caused by differing lighting conditions, pose etc.)[5], yet the input images are not completely random and in spite of their differences there are patterns which occur in any input signal. Such patterns, which can be observed in all signals could be - in the domain of facial recognition - the presence of some objects (eyes, nose, mouth) in any face as well as relative distances between these objects.

These characteristic features are called eigenfaces in the facial recognition domain (or principal components generally). They can be extracted out of original image data by means of a mathematical tool called Principal Component Analysis (PCA). By means of PCA one can transform each original image of the training set into

a corresponding eigenface. An important feature of PCA is that one can reconstruct any original image from the training set by combining the eigenfaces[6]. Figure 1: shows the example for face recognition using eigenfaces algorithm.

The algorithm for the facial recognition using eigenfaces uses the original images of the training set are transformed into a set of eigenfaces E. Afterwards, the weights are calculated for each image of the training set and stored in the set W.

Upon observing an unknown image X, the weights are calculated for that particular image and stored in the vector W_X. Afterwards, W_X is compared with the weights of images, of which one knows for certain that they are faces (the weights of the training set W).

One way to do it would be to regard each weight vector as a point in space and calculate an average distance D between the weight vectors from W_X and the weight vector of the unknown image W_X. If this average distance exceeds some threshold value , then the weight vector of the unknown image W_X lies too "far apart" from the weights of the faces. In this case, the unknown X is considered to not a face. Otherwise (if X is actually a face), its weight vector W_X is stored for later classification. The optimal threshold value has to be determined empirically.

Calculation of eigenfaces with PCA. In this section, the original scheme for determination of the eigenfaces using PCA will be presented.

Mathematically calculations. Let a face image *I(x,y)* be a two dimensional N by N array of (8-bit) intensity values. An image may also be considered as a vector of dimension N^2, so that a typical image of size 256 by 256 becomes a vector of dimension 65,536 or equivalently a point in a 65,536-dimensional space. An ensemble of images, then, maps to a collection of points in this huge space. Principal component analysis would find the vectors that best account for the distribution of the face images within this entire space.

Step 1: Prepare the data. Let the training set of face images be $T_1, T_2, T_3, \ldots T_M$.

Step 2: Subtract the mean. This training data set has to be mean adjusted before calculating the covariance matrix or eigenvectors.The average face is calculated as $\Psi = (1/M) \Sigma_1^M T_i$ Each image in the data set differs from the average face by the vector $\Phi = T_i - \Psi$.This is actually mean adjusted data.

Step 3: Calculate the covariance matrix. The covariance matrix is

$$\mathbf{C = (1/M)\ \Sigma_1^M \Phi_i \Phi_i^T (1)}$$

where $A = [\Phi_1, \Phi_2, \ldots \Phi_M]$.

Step 4: Calculate the eigenvectors and eigenvalues of the covariance matrix. The matrix C is a N^2 by N^2 matrix and would generate N^2 eigenvectors and eigenvalues. With image sizes like 256 by 256, or even lower than that, such a calculation would be impractical to implement. A computationally feasible method was suggested to find out the eigenvectors. If the number of images in the training set is less than the no of pixels in an image (i.e $M < N^2$), then we can solve an M by M matrix instead of solving a N^2 by N^2 matrix. Consider the covariance matrix as A^TA instead of AA^T. Now the eigenvector $v_i$can calculated as follows, $A^TAv_i = \mu_i v_i$**(2)**

Whereμ_i is the eigenvalue. Here the size of covariance matrix would be M by M.Thus we can have m eigenvectors instead of N^2. Premultiplying equation 2 by A, we have

$AA^TAv_{i=}\ \mu_i Av_i$(3)

The right hand side gives us the M eigenfaces of the order N^2 by 1.All such vectors would make the imagespace of dimensionality M.

Face Space. As the accurate reconstruction of the face is not required, we can now reduce the dimensionality to M' instead of M. This is done by selecting the M' eigenfaces which have the largest associated Eigenvalues. These eigenfaces now span a M'-dimensional subspace instead of N^2.

Recognition.A new image T is transformed into its eigenface components (projected into 'face space') by a simple operation,

$w_k = u_k^T (T - \psi)$(4)

here k = 1,2,….M'. The weights obtained as above form a vector $\Omega^T = [w_1, w_2, w_3, \ldots w_{M'}]$ that describes the contribution of each eigenface in representing the input face image. The vector may then be used in a standard pattern recognition algorithm to find out which of a number of predefined face class, if any, best describes the face.The face class can be calculated by averaging the weight vectors for the images of one individual. The face classes to be made depend on the classification to be made like a face class can be made of all the images where subject has the spectacles. With this face class, classification can be made if the subject has spectacles or not. The Euclidean distance of the weight vector of the new image from the face class weight vector can be calculated as follows,

$\varepsilon_k = || \Omega - \Omega_k ||$(5)

where $\Omega_k$is a vector describing the kth face class. The face is classified as belonging to class k when the distance $\varepsilon_k$is below some threshold value $\theta\varepsilon$. Otherwise the face is classified as unknown. Also it can be found whether an image is a face image or not by simply finding the squared distance between the mean adjusted input image and its projection onto the face space.

$\varepsilon^2 = || \Phi - \Phi_f ||$(6)

whereΦ_f is the face space and $\Phi = T_i - \Psi$is the mean adjusted input.

= A

Figure 2: example of face recognition using eigenface algorithm

With this we can classify the image as known face image, unknown face image and not a face image.

3.2 Signature verification

Two main types of dynamic signature verification systems exist.1.Feature-based systems model the signature as a holistic multidimensional vector composed of global features and 2.Function-based systems extract time functions from the signature signal (pen coordinates, pressure, etc.) and perform signature matching via elastic or statistical techniques like Dynamic Time Warping (DTW) or Hidden Markov Models (HMM)[7]. The typical architecture of an automatic signature verification system is depicted in Fig. 2.

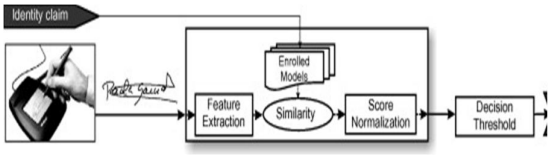

Fig. 3 Architecture of the proposed on-line signature verification system.

The system uses a set of time sequences and Hidden Markov Model. This paper deals with on-line signature verification. On-line refers here to the use of the time functions of the dynamic signing process.

Feature extraction

Basic functions. The signature representation considered in this work is based on the followingfive time sequences: horizontal xn and vertical yn position trajectories, azimuthn and altitude _n of the pen with respect to the tablet, and pressure signalpn. The value n = 1, . . . ,N is the discrete time index given by the acquisitiondevice and N is the time duration of the signature in sampling units. As a result, the basic functionset consists of xn, yn and pn.

Geometric normalization.A signature acquisition process on a restricted size frame is assumed (Fierrez-Aguilar et al., 2004). As a result, users are supposed to be consistent in size andwriting dynamics. Moreover, a geometric normalization consisting of positionnormalization followed by rotation alignment is applied.

Position normalization.consists in aligning the center of mass of the different signatures. Rotation normalization consists in aligning the average path tangent angle. of the different signatures, where the upper dot notation denotes first order time derivative.

Extended normalisation. After geometric normalization, 4 extended sequences are derived from the basic function set. Previous results with other dynamic sequences have shown good levels of performance. In the present work, four dynamic sequences have been used as extended functions, namely

- Path-tangent angle.
- Path velocity magnitude.
- Log curvature radius
- Total acceleration magnitude.

are respectively the tangential and centripetal acceleration components of 5 the pen motion.In all cases, (discrete) time derivatives have been computed by using the second-order regression.

Time derivatives. First order time derivatives of complete instantaneous function-based feature sets are highly effective as discriminative parameters regarding verification with other behavioral traits (Soong and Rosenberg, 1988), so we have decided to incorporate time derivatives in our system. Because of the discrete nature of the above-mentioned functions, first order time derivatives are calculated by using a second order regression (Young et al., 2002).

Signal normalization: A final signal normalization, oriented to obtain zero mean and unit standard
deviation function values is performed.

Signature modeling

Background on Hidden Markov Models. Hidden Markov Models were introduced in the pattern recognition field as a robust method to model the variability of discrete time random signals where time or context information is available (Rabiner, 1989). Some previous works using HMMs for signature verification include (Yang et al., 1995; Kashi et al., 1997; Dolfing et al., 1998). Basically, the HMM represents a doubly stochastic process governed by an underlying Markov chain with finite number of states and a set of random functions each of which is associated with the output observation of one state (Yang et al., 1995). At discrete instants of time n, the process is in one of the states and generates an observation symbol according to the random function corresponding to that current state. The model is hidden in the sense that the underlying state which generates each symbol cannot be deduced from simple symbol observation. Formally, a HMM is described as follows:

- H, which is the number of hidden states.
- The state transition matrix.
- The initial state distribution.

Twenty-five dynamic features are extracted at eachpoint of the signature. Signatures are modeled

by a continuous left-to-right HMM [10], by using, in each state, a continuous multivariate Gaussian mixture density. The number of states in the HMM modeling the signatures of a given person is determined individually according to the total number of all the sampled points available when summing all the genuine signatures that are used to train the corresponding HMM. Matching is done using the decision score.

3.3 Fusion

Levels of Fusion in Multi-biometric system:

The fundamental issue in the information fusion system is to identify the type of the information before it get consolidate [3]. The information can be consolidating at different levels in biometric system, starting from the acquisition of the data to the decision making module. There are four different possible levels of fusion.

- sensor level fusion
- fusion at the feature extraction level,
- fusion at the matching score level,
- fusion at the decision level.

Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as logistic regression may be used to combine the scores reported by the two sensors. These techniques attempt to minimize the FRR for a given FAR. Figure 1 illustrates the matching score level of fusion for combining face and signature biometric systems.

For sum rule matcher scores are simply added, with no prior normalization. Scores are neither rescaled, nor weighted to account for differences in matcher accuracy.

This technique works with following steps:

In the first step probability density functions are modelled separately for genuine and impostor distribution by each. For each matcher the Likelihood ratios are computed from these models. Transformation is performed to their likelihood ratios to normalize scores. Lastly, Normalized scores are simply multiplied.

4.CONCLUSION AND FUTURE ENHANCEMENT

In this paper, the problem of using biometric user authentication during a standard web session when a mobile phone is used has been successfully approached. We have focused on the technological problem of capturing the biometric with the mobile phone, sending it to the web server and after user authentication allowing or rejecting the user's continuation with the web session in the same way this had been performed using password authentication.

The performance of single modality based biometric recognition has been suffering from the different noisy data, non-universality of biometric data, and susceptibility of spoofing. The multimodal biometric system can improve the performance of the system. In this paper shows that face and signature based bimodal biometric system can improve the accuracy rate about 10%, than single face signature based biometric system. The rate can also be improved using advanced pattern recognition techniques, which will be studied in future.

Although biometrics is considered the most effective and safe method (is very difficult to falsify), we have to bear in mind its disadvantages, for example, that since it is a relative new technology, it is not still integrated in PC, so IT departments need to make a conscious decision before making the purchase and change its structure.

REFERENCES

[1] Carlos Vivaracho-Pascual and Juan Pascual-Gaspar ,"On the Use of Mobile Phones and Biometrics forAccessing Restricted WebServices", part c: applications and reviews, vol. 42, no. 2, march 2012.

[2] K.Sujana, Md.Murtuza Ahmed Khan "Preventing Spoofing Attacks in Mobile Banking Based on UserInput Pattern - Based Authentication",Volume 7, Issue 3 (Nov. - Dec. 2012), PP 15-19 Page.

[3]kazim.m., rode y.s., dabhades.b., al-dawlan.n.h., mane a.vmanzar.r. and kale k.v." multimodal biometric system using face and signature: a score level fusion approach",volume 4, issue 1, 2012, pp.-99-103.

[4]A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics(International Series on Biometrics). Secaucus, NJ: Springer-Verlag,2006.

[5] T. Hazen, E. Weinstein, and A. Park, "Towards robust person recognitionon handheld devices using face and speaker identification technologies,"inProc. Int. Conf. Multimodal Interfaces, 2003, pp. 289–292.

[6] "On Optimising Local Feature Face Recognitionfor Mobile Devices" Mauricio Villegas and Roberto Paredes.

[7] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Towardsmobile authentication using dynamic signature verification: Usefulfeatures and performance evaluation," in Proc. 19th Int. Conf. PatternRecogn., Dec. 2008, pp. 1–5.