An Advanced Efficient Secured Blind Authentication and Verification Crypto Protocol

S. Princy Suganthi Bai

Assistant Professor, Department of Computer Applications, Francis Xavier Engineering College, Tirunelveli, Tamil nadu, India.
vinodh_princy@yahoo.com

S. Selvakani Kandeeban

Professor and Head, Department of Computer Applications, Francis Xavier Engineering College, Tirunelveli, Tamil nadu, India.
sselvakani@hotmail.com

Abstract

The main objective of this application is to provide biometric verification protocol for the financial server with template protection and validity of trustable server. Most biometric systems assume that the template in the system is secure due to human supervision or physical protection. Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced once they are compromised. The main objective of this system is to provide secure and blind biometric authentication protocol to protect the biometric template data with high security and accuracy. The protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. The encryption also provides template protection, the ability to revoke enrolled templates, and alleviates the concern on privacy in widespread use of biometrics. The proposed approach makes the communication between the concern and its client in a trustable mode

Keywords: *Biometrics, cryptosystems, privacy, public key cryptography, security, support vector machines (SVMs).*

1. Introduction

The process of verifying a person's identity also called authentication. It plays an important role in various areas of everyday life. Reliable authentication [6] is becoming an increasingly important task in the Web-based world. A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of this scheme is to ensure that the rendered services are provided and accessed only by a legitimate server and user. In the presence of robust personal recognition schemes, these systems are helpless to the deceit of a fake. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological characteristics.

By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms [5] that make the systems both secure and cost-effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiable nature and user convenience.

Face recognition technology [9] is the best biometric technology. It is the most obvious individual identifier – the human face. Face recognition-system analysis the characteristics of a person's face images input through a web camera. Based on the input image, system measures the overall face structure, including distances between eyes, nose, mouth and chicks. With the use of these unique characteristics face recognition-system store face template into its database. The face recognition problem can be divided into two main stages: face verification (or authentication), and face identification (or recognition). The detection stage is the first stage; it includes identifying and locating a face in an image. The recognition stage is the second stage; it includes feature extraction saving and then matching.

2. Literature Survey

The previous work in the area of encryption-based security of biometric templates tends to model the problem as that of building a classification system that separates the genuine and impostor samples in the encrypted domain [1],[8],[9]. However, a strong encryption mechanism destroys any pattern in the data, which adversely affects the accuracy of verification. Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in our approach is that we are able to design the classifier in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/ privacy[3]."A template protection scheme with provable security and acceptable recognition performance has thus far remained elusive" at the existing work in light of this security-accuracy dilemma, and understand how this can be overcome by communication between the authenticating server and the client.

2.1 Existing System

Server is responsible to allow the client to access the service of the server with proper verification and there may be a possibility of hackers to catch over the biometric features. The traditional process may lead to misuse the biometric template. In the current system, by using the authentication algorithm biometric data are known explicitly. The certain traditional biometrics protection algorithm sometimes will degrade the performance of the recognition. Normally in the financial server, the server will only suspect the client and build up with proper identification algorithm. The client does not have guaranteed on the truthfulness of the server.

2.2 Proposed System

Providing highly end secured protocol for biometric template production and establishing trustable server with privileges. In the proposed system encryption won't affect the

performance of the recognition. The authentication protocol is blind in nature regarding to the algorithm and features. The Enrollment server properly captures the biometric data and stores it in the authentication server in crypto mode. The proposed approach addresses the following issues:

The ability to use strong encryption addresses template protection issues as well as privacy concerns. Non-repudiable authentication can be carried out even between non-trusting client and server using a trusted third party solution. It provides provable protection against replay and client – side attacks even if the keys of the user are compromised. As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked.

2.3 Project Description

Under an Efficient secured blind authentication and verification crypto protocol there are two modules. They are Enrollment module and verification module.

2.3.1. Enrollment Module

Role of User: In the Enrollment phase, the user has to supply the profile with complete description along with security key and sensor biometric based face image.

Role of Enrollment Server: The Enrollment server collects all the details supplied by the user and embeds the authenticate key behind the face image with the concept of the watermarking technique.

The Secured Key Embedding: The watermark, denoted by W= { w_i |i=1,…….L_w } is a key-based bit sequence. The key must be of size 40 bits length. According to the number of watermark bit chooses location randomly from the image. The embedding rules are formulated as

If w(i) = 1, The bit at the selected position I(x, y) must be odd. Otherwise make it as odd I (x, y) = I(x, y) +1. If w(i)=0, The bit at the selected position I(x, y) must be even. Otherwise make it as even I(x, y) =I(x, y) - 1.

Role of Authentication Server: The Authentication server is responsible for the fully secured biometric verification. Authentication server extract key from the face image using the extraction algorithm. The face feature is extracted using gabor filter as follows:

Gabor filter works as a band pass filter for the local spatial frequency distribution, achieving an optimal resolution in both spatial and frequency domains. The 2D Gabor filter $\psi_{f,\theta}(x,y)$ can be represented as a complex sinusoidal signal modulated by a Gaussian kernel function as follows

$$\psi_{f,\theta}(x,y) = \exp\left[-\frac{1}{2}\left\{\frac{x^2\theta_n}{\sigma^2 x}+\frac{y^2\theta_n}{\sigma^2 y}\right\}\right]\exp(2\pi f x_{\theta_n}) \tag{1}$$

$$\begin{pmatrix} x\theta_n \\ y_{\theta_n} \end{pmatrix} = \begin{pmatrix} \sin\theta_n & \cos\theta_n \\ -\cos\theta_n & \sin\theta_n \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \tag{2}$$

σ_x, σ_y are the standard deviations of the Gaussian envelope along the x and y dimensions, f is the central frequency of the sinusoidal plane wave, and θ is the orientation. The rotation of the x-y plane by an angle θ_n will result in a Gabor filter at the orientation θ_n. The angle θ_n is defined by

$$\theta n = \pi / p(n-1) \tag{3}$$

for n=1,2…….,p and p∈N, where p denotes the number of orientations. Design of Gabor filters is accomplished by tuning the filter with a specific band of spatial frequency and orientation by appropriately σ_x, σ_y , radial frequency f, and the orientation of the filter θ_n.

2.3.2 Verification Module

At the time of user login, the first level of verification is done on the basis of userid and password. The second level of biometric verification along with trusted server confirmation is done as follows.

- The face feature template is created for the logged user facial view.
- Authenticate key once again extracted from the registered face of the corresponding user.
- Using the extracted key the encrypted feature transformed to the decrypted form.
- The person is verified on the basis of template matching.
- If the person is valid one then the authenticate key send to the user for the trusted server confirmation.

The extraction of key is done at the time of biometric verification. The key extracted and that key is used to decrypt the face template features for the biometric verification. The extraction is done on the basis of

- If the bit at the selected position I(x,y) is even then the bit is 0
- If the bit at the selected position I(x,y) is odd then the bit is 1.

SVM Classifier [2] is a cross-platform graphical application that handles very large datasets well. Support Vector Machines are a useful technique for data classification. A classification task usually involves separating data into training and testing sets. Each instance in the training set contains one target value" (i.e. the class labels) and several attributes" (i.e. the features or observed variables). The goal of SVM is to produce a model based on the training data which predicts the target values of the test data given only the test data attributes. The goal of SVM is to produce a model which predicts target value of data instances in the testing set which are given only the attributes. Classification in SVM is examples of Supervised Learning Known labels help indicate whether the system is performing in a right way or not. This information points to a desired response, validating the accuracy of the system or be used to help the system learn to act correctly.

3. Architecture Diagram

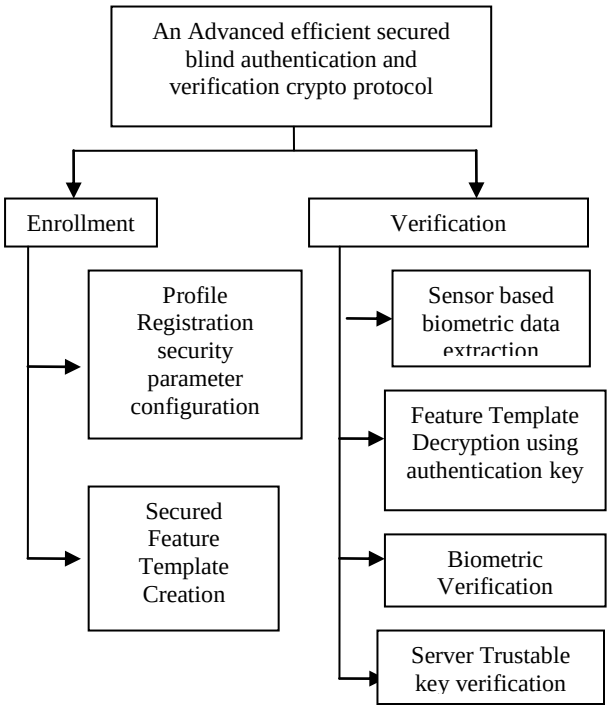

Figure 1. Verification and Enrollment

A step in SVM classification involves identification as which are intimately connected to the known classes. This is called feature selection or feature extraction. Feature selection and SVM classification together have a use even when prediction of unknown samples is not necessary. They can be used to identify key sets which are involved in whatever processes distinguish the classes [7].

SVM has been found to be successful when used for pattern classification problems. Applying the Support Vector approach to a particular practical problem involves resolving a number of questions based on the problem definition and the design involved with it.

4. Experiments and Results

It is a formal process to determine how well the system is working, how it has been accepted and whether adjustments are needed. It is also important to gather information for the maintenance. The system is implemented to satisfy all the requirements specified in the proposed system. The system is implemented as new form of the existing web site for the concern. This application provides great services to their share holders, insurance agent. This system is implemented with the help of the ASP.NET features. The forms are designed with web server controls in a user friendly nature. The data are properly maintained in the back end as Sql server 2005.

The implemented system works properly by giving all kinds of inputs as the user needs to give all the personal information for registration. The personal information

like first name, last name, date of birth, gender, username, password, retype password, email id, country, city, zip code, phone number and also give the key to embed into the image then the photo snap of the user is taken and enrolled successfully. The enrollment server make the size of the photo to image size of 64x64 dimensions and the key is embedded into the image and sent to the authentication server. Then the admin opens the authentication server and views the enrolled clients. The authentication servers extract the key from the image. Then the feature extraction takes place in the image. Then the feature extraction is encrypted with the key.

Next time the user login to the site. The user has to give the username and the password then the photo snap of the user is taken. The user photo also resizes to the 64x64 dimensions. The feature extraction takes place in this image. The authentication server takes the image which is embedding with the key when the user registers the details. The server separates the key from the image. Take the key and decrypt the feature extraction of the image at the registration time. Then the server compares the feature extraction of the image in the registration time and the login time. If both the feature extraction is same, then the user is allowed to go into the site or invalid person to go into the site. This application provides the output in proper format as authentication success or invalid person.

To verify the effectiveness of using SVMs as a classification model for biometrics verification problems, we tested it on two different modalities. The verification accuracies on each of the datasets are presented in the Table I.

Table I: Verification Accuracy on Data Sets

Dataset	No of Features	Accuracy
Face	20	98.68%
Oral dataset	20	96.54%

The first set of experiments used the face representation as features on the face dataset consisting of 20 users and gives the accuracy of 98.68%. For the second set of experiments used the oral datasets consisting of 10 users and gives the accuracy of 96.54%.

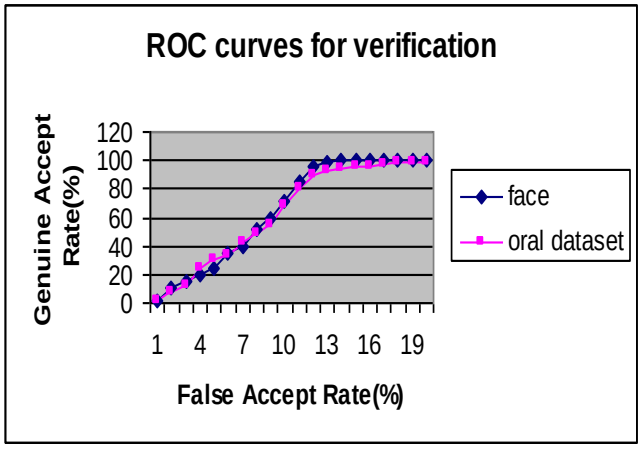

Figure 2. ROC curves for Verification

Figure 2 shows the *receiver operating characteristic* (ROC) plots for the biometrics using the fixed length representation. The primary objective of the experiments is to demonstrate that making the authentication secure does not decrease the accuracy. Hence we apply the technique to secure any fixed length representation of a biometric trait, which is classified using SVM.

5. Conclusion

The advantage of the proposed approach is that we are able to achieve classification of a strongly encrypted feature vector using generic classifiers such as SVMs. The authentication server need not know the specific biometric trait that is used by a particular user, which can even vary across users. Once a trusted enrollment server encrypts the classifier parameters for a specific biometric of a person, the authentication server is verifying the identity of a user with respect to that encryption. The real identity of the person is hence not revealed to the server, making the protocol, completely blind. This allows one to revoke enrolled templates by changing the encryption key, as well as use multiple keys across different servers to avoid being tracked, thus leading to better privacy. The proposed blind authentication is extremely secure under a variety of attacks and can be used with a wide variety of biometric traits. Protocols are designed to keep the interaction between the user and the server to a minimum computation.

6. Future Enhancements

As the verification can be done in real-time with the help of available hardware, the approach is practical in many applications. The use of smart cards to hold encryption keys enables applications such as biometric ATMs and access of services from public terminals. Possible extensions to this work include secure enrollment protocols and encryption methods to reduce computations. Efficient methods to do dynamic warping-based matching of variable length feature vectors can further enhance the utility of the approach. Biometrics' future will include e-commerce applications for extra security on the checkout page, and biometrics will guard against unauthorized access to cars and cell phones. In the future, biometric technology will further develop 3-D infrared facial recognition access control, real-time facial recognition passive surveillance, and visitor management authentication systems. Multi level recognition can be made in the authentication.

References

[1] S. Abe, Support Vector Machines for Pattern Classification. New York: Springer, 2005.

[2] Anastasios Texas, Constantine Kotropoulos, Ioannis Pitas," Using Support Vector Machines to Enhance the Performance of Elastic Graph Matching for Frontal Face Authentication", IEEE transactions on pattern analysis and machine intelligence, vol. 23, no. 7, 2001.

[3] S. Avidan and M. Butman, "Blind vision," in Proc. Eur. Conf. Computer Vision (ECCV), 2006, pp. 1–13.

[4] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in CVPR Biometrics Worshop, Jun. 2007, pp. 1–7.

[5] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[6] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar "A Secure Crypto-Biometric Verification Protocol" IEEE transactions on information forensics and security, vol. 5, no. 2, june 2010.

[7] Nello cristianini and John Shawe-Taylor," An Introduction to Support Vector Machines and other Kernel-based Learning Methods", Cambridge University press, 2000.

[8] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol.40, no. 3, pp. 614–634, Mar. 2001.

[9] W. Zhao, R. Chellappa, A. Rosenfeld and P.J. Phillips, Face Recognition: A Literature Survey, ACM Computing Surveys, pp. 399-458,2003.

Authors

S. Princy Suganthi Bai received the MCA degree from Kamaraj College, Tuticorin and M.Phil degree from Mother Teresa Women's University. Presently she is working as an Assistant Professor, MCA Department in Francis Xavier Engineering College. She has presented 1 paper in an International Conference and 1 paper in a National Conference. She is currently pursuing her Ph. D degree in Neural Network in Network Security.

S. Selvakani Kandeeban received the MCA degree from Manonmanium Sundaranar University and M.Phil degree from Madurai Kamaraj University. Presently she is working as an Professor & Head, MCA Dept in Francis Xavier Engineering College, Tirunelveli. Previously she was with Jaya College of Engineering and Technology as an Assistant Professor, MCA Department. She has presented 6 papers in National Conference and 1 paper in international conference. She has published 2 paper in National journal and 10 papers in International Journal. She is currently pursuing her PhD degree in Network Security.