Enhancing Security in Biometric System Using Blind Authentication Protocol

MOHAMMED AFNAN TK,
B.TECH IT, IV Year,
Aalim Muhammed Salegh College of Engineering,
Chennai-55.
tk_afnan@rediffmail.com

RAGHUL.C,
NAWAZ AHMED,
B.TECH IT, IV Year ,
Aalim Muhammed Salegh College Of Engineering,
Chennai-55.
rahuldhayare@gmail.com

***Abstract*—Biometric authentication system are used prevalently for its template security, retract ability and privacy. The Authentication process is reinforced by biometric cryptosystem. We propose a demonstrable secure and blind biometric authentication protocol which discloses only identity and not any other information to both client and server. To reduce the computational cost and enhance security we have used ElGamal. It is based on asymmetric encryption in which biometric authentication and security of public key cryptography is enhanced. Authentication protocol works on public network and provides template protection, ability to retract template protection and assuage the concern on privacy. In our approach the authentication in the encrypted domain does not affect the accuracy, while the encryption key bolsters security.**

Keywords*— Data Set, Cryptosystem, Privacy, Public key cryptography, Neural Network.

I. Introduction

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. There are several techniques that can be applied for verifying and confirming a user's identity. The technology used for identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice or handwriting is called Biometrics.

Advancements in technology has made possible to build rugged and reliable Biometric authentication system. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

The biometric traits of the same individual taken at different times are almost never identical. So the threshold τ is used since threshold value is used for matching the traits.

Verification Mode- The verification mode in the system validates a person's identity by comparing the captured biometric data and an identity with her own biometric template(s) stored in the system database.

Identification Mode- The identification mode in the system recognizes an individual by searching the templates of all the users in the database for a match.

II. Literature Survey

The literature review is based upon the various surveys of the biometrics system which is for secure authentication. The authentication mainly concentrates on template protection, retractable and trust issues. An ideal biometric template protection scheme should satisfy the properties of the basic biometric traits. In the common approach the original biometric template is not stored but a transformed version is stored and this would require decryption of the template while matching. Standard encryption techniques are not useful due to developments in computation which would increase the vulnerability of biometric systems.

A. Template protection

An ideal biometric template protection scheme should possess the following four properties

Diversity: The secure template must not allow cross-matching across databases, thereby ensuring the user's privacy.

Revocability: it should be straight forward to revoke a compromised template and reissue a new one based on the biometric data

Security: It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

Performance: The biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

The algorithms for template protection can be classified in two.

Features transformation: In the enrolment phase, a transformation function is applied to the biometric information and is stored in the database. In the authentication process, the same transformation function is applied to query features and the transformed query is directly matched against the transformed template. Feature transformation techniques can be further divided into two categories according to the property of the transformation function

Salting transformations: The biometric features are transformed using an invertible function defined by a user-specific key or password, which must be kept secret. The introduction of a secret key ensures revocability. In fact, in case a template is compromised, it's easy to revoke it and replace it with a new one generated by using a different user-specific key. By the way, if the user-specific key is compromised, the template is no longer secure, because the transformation is usually invertible.

Non-invertible transformation: The biometric template is secured by applying a non-invertible transformation function that is "easy to compute" but "hard to invert". Even if the key and/or the transformed template are known, it is computationally hard for an opponent to recover the original biometric template. Diversity and revocability can be achieved by using application-specific and user specific transformation functions. The main drawback of this approach is the trade-off between discriminality and non invertibility of the transformation function, which in general leads to a decrease of the recognition performances.

Biometric cryptosystems: In the biometric cryptosystems some public information about the biometric template, called helper data, is stored. The helper data does not reveal any significant information about the original biometric template but it is needed during matching to extract a cryptographic key from the query biometric features. Matching is performed indirectly by verifying the correctness of the extracted key. Biometric cryptosystems offer high security but are not designed to provide diversity and revocability.

Even, biometric cryptosystems can be split into two groups, depending on how the helper data is obtained

*Key-binding biometric cryptosystem.*The helper data is obtained by binding a key that is independent of the biometric features with the biometric template. It's computationally hard to decode the key or the template without any knowledge of the user's biometric data

Key generation biometric cryptosystems:The helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features. It's hard to develop a scheme that generates the same key for different templates of the same person and at the same time very different keys for different persons.

B. Cancellable biometrics

In Cancellable biometrics, during the enrolment, few images of the user are collected. The PIN number given by user is used by a random number generator to generate the random convolution kernel which is convolved for training images. The convolved training images are used to generate a single biometric filter which is stored on card. If the card is lost, the enrolment system generates a different convolution kernel to synthesize a different encrypted biometric filter. The attacker cannot cancel the template without knowing the user's PIN or the convolution kernel used. During the authentication the user will present his/her card and provide the PIN. That will generate the convolution kernel which will be used to convolve with the test images presented by the authentic user. The convolved test images are then cross-correlated with the encrypted biometric filters, and outputs are examined for authentication.

FUZZY VAULT: The fuzzy vault method is based on the polynomial reconstruction problem. First, secret S is encoded in some error-collection code. Then, S in a vault is locked by using a private unordered set k, and adding to random data, called chaff points, even when unordered set k is modified to k` such that k≈k`,S can be recovered from the vault. Using multiple minutiae location sets, they use canonical positions of minutia, as the elements of the set k. However, their system assumes that fingerprints are pre-aligned.This is not realistic assumption for fingerprint based authentication schemes. In a fuzzy vault system for fingerprint without error-collection steps, uses the Lagrange interpolation and the Cyclic Redundancy Check (CRC) for testing polynomial reconstruction. They use concatenated x and y coordinates of minutiae as [x|y], as the elements of the set k.

D. Zerobio authentication

In zerobio authentication, the basic building block consists of neural networks and homomorphic encryption. In neural networks for learning the weights back propagation method is used. Homomorphic encryption is used for encrypting unit values used in the neural networks. Hence neural network is robust against the fuzziness of the data. For registration of the user the element of feature vector are given as input to the neural network using back propagation algorithm where the optimal weights are identified and output is produced. After authentication user has to produce the weights and random number. The re extracted feature is given for registration; the user computes cipher text of hidden layer using weights and sends to the verifier. The verifier computes output value and then authenticates based on threshold value.The method is both efficient and generic; however, the server can estimate the weights at the hidden layer from multiple observations over authentications. Once the weights are known, the server can also compute the feature vector of the biometric, thus compromising both security and privacy. The system could also be compromised if an attacker gains access to the client computer, where the weight information is available in plain.

III. METHODOLOGY

All the above stated methods for the template protection have its own limitation which would compromise the security of the system. The Blind Authentication can be defined as a biometric authentication protocol that does not reveal any information about the biometric samples to the authenticating server. It also does not reveal any information regarding the classifier, employed by the server, to the user or client. The goal of the authentication could be achieved using any biometric trait with this authentication protocol, and also proves that the information exchanged between the client and the server does not reveal anything other than the identity of the client.

Blind Authentication addresses all the concerns such as the ability to use strong encryption addresses template protection 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. In this we have split the system into three modules.

A. Feature extraction

In the first module is for feature extraction. From the biometric trait the essential feature is extracted. For this feature extraction we are using Hilditch Thinning Algorithm.

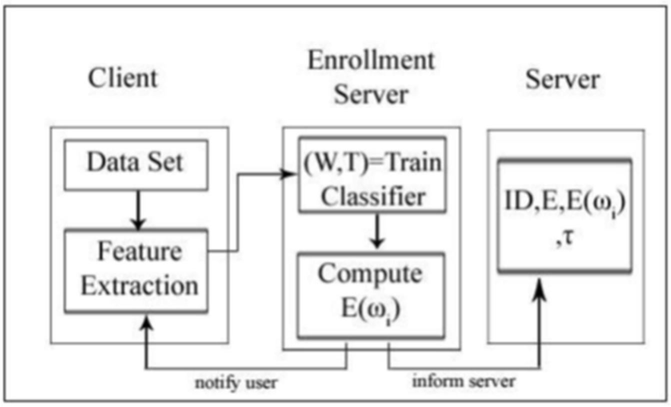
The process of Skeletonisation in this involves the thinning of the ridges using conditions involved in the algorithm. From the skeletonised image we point out the Bifurcation and Ridge end. These points are used as feature vector.

B. Enrollment

The second module is for Enrolment of a new user into the System. During the enrolment, the client sends encrypted form of her extracted feature vector E(x) of her biometric using her public key to the enrolment server. For the classification of the data, Neural network based classification could be used. In neural networks, artificial neural networks (ANN)are well-suited for training the data.

The neural network consists of processing elements called neurons which intern consists of a summing part and an output part. The summing part computes a weighted sum of the input vector and the output function determines the output signal. An ANN consists of multilayer where the first layer is the input layer, the last layer the output layer, and the rest is known as hidden layers. Each layer, has a predefined number of neurons, computes a weighted summation of the input given to it and generates an output signal, which becomes an input to the next layer. The basic unit in ANN is the Sigmoid Unit which is based on a smoothed, differential threshold function the sigmoid unit computes a linear combination of its inputs, and then applies a threshold to the result. Using the encrypted version of the feature vector received from the user the enrolment server computes the parameters (ω,τ) with the help of classifier. The encrypted parameter E (ω) and Threshold (τ) sent to the authentication server. A notification is sent back to the client about the enrolment.

Figure i: Enrollment



C. Authentication

The authentication [9] happens over two rounds of communication between the client and the server. To perform authentication, the client locks the biometric test sample using her public key and sends the locked ID to the server. The server computes the products of the locked ID with the locked classifier parameters and randomizes the results. These randomized products are sent back to the client.

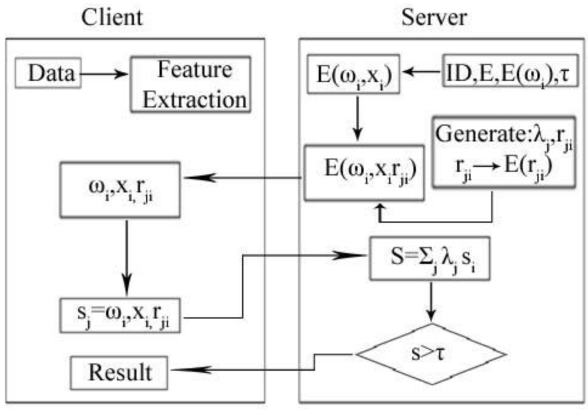


Figure ii: Authentication

During the second round, the client unlocks the randomized results and computes the sum of the products. The resulting randomized sum is sent to the server. The server de-randomizes the sum to obtain the final result, which is compared with a threshold (τ) for authentication.

In this system if a new user wants to enroll him first the user gives fingerprint from dataset. The feature is extracted from the fingerprint and is encrypted. The encrypted feature vector, id is sent to the enrolment server. The classifier computes the classifier parameter and the threshold value.

These values are sent to the server to inform about the new user. The user is notified that he is enrolled.

When an already existing user claims for an authentication, the feature vector is encrypted and sent to the server along with the identity of the user. The user's feature vector is encrypted since the server must not know the feature .For this purpose homomorphic encryption IS used which satisfies the following condition.

$E(X).E(Y)=E(X.Y)$

The product of the vector and the classifier parameter is calculated and randomized by the server. The randomized value is sent to the client. The first round of communication is done. In second round the client decrypts the value and then converts the product into sum and sent to server. The computed sum is de-randomized and compared with the threshold value. If condition is satisfied that $S > \tau$ then the user is authenticated otherwise rejected as an impostor.

IV. CONCLUSION AND FUTURE WORKS

This paper adopts the verification protocol for biometric system to improve the security and privacy. In this, the computation at the client side is reduced by the use of classifier which is present at server side. Interaction between the user and the server has been computationally reduced. The blind biometric authentication is extremely secure under a variety of attacks and can be used with a wide variety of biometric traits. The key exchange between client and server could be done using Homomorphic encryption schemes. The ElGamalhomomorphic encryption is adopted by us for the implementation of the system.

References

[1] 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, Jan. 2004

[2] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints," Proc. IEEE, vol. 85, pp. 1365–1388, Sept. 1997.

[3] Marco GRASSI, Marcos FAUNDEZ-ZANUY D.I.B.E.T. UniversitàPolitecnicadelle Marche, Ancona, Italy,EscolaUniversitàriaPolitècnica de Mataró (Adscrita a la UPC) Matarò, Spain "A protection scheme for enhancing biometric template security and discriminability".

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[5] E. B. Walter and J. Scheirer, "Cracking fuzzy vaults and biometric encryption" in Biometrics Symp., Maryland, 2007,