NABS: Novel Approaches for Biometric Systems

Abstract:

Research on biometrics has noticeably increased. However, no single bodily or behavioral feature is able to satisfy acceptability, speed, and reliability constraints of authentication in real applications. The present trend is therefore toward multimodal systems. In this paper, we deal with some core issues related to the design of these systems and propose a novel modular framework, namely, novel approaches for biometric systems (NABS) that we have implemented to address them. NABS proposal encompasses two possible architectures based on the comparative speeds of the involved biometries. It also provides a novel solution for the data normalization problem, with the new quasi-linear sigmoid (QLS) normalization function. This function can overcome a number of common limitations, according to the presented experimental comparisons.
A further contribution is the system response reliability (SRR) index to measure response confidence. Its theoretical definition allows taking into account the gallery composition at hand in assigning a system reliability measure on a single-response basis. The unified experimental setting aims at evaluating such aspects both separately and together, using face, ear, and fingerprint as test biometries. The results provide a positive feedback for the overall theoretical framework developed herein. Since NABS is designed to allow both a flexible choice of the adopted architecture, and a variable compositions and/or substitution of its optional modules, i.e., QLS and SRR, it can support different operational settings.

Existing System:

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. 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. Over the years a number of attempts have been made to address the problem of template protection and privacy concerns and despite all efforts, puts it, "a template protection scheme with provable security and acceptable recognition performance has thus far remained elusive". In this section, we will look 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. Detailed reviews of the work on template protection can be found.

Disadvantage of existing system:

1. The first class of feature transformation approaches known as Salting offers security using a transformation function seeded by a user specific key. The strength of the approach lies in the strength of the key. A classifier is then designed in the encrypted feature space. Although the standard cryptographic encryption such as AES or RSA offers secure transformation functions.

2. The second category of approaches identified as noninvertible transform applies a trait specific noninvertible function on the biometric template so as to secure it. The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set.

3. The third and fourth classes are both variations of Biometric cryptosystems. They try to integrate the advantages of both biometrics and cryptography to enhance the overall security and privacy of an authentication system. Such systems are primarily aimed at using the biometric as a protection for a secret key (key binding approach or use the biometric data to directly generate a secret key (key generation approach. The authentication is done using the key, which is unlocked/generated by the biometric.

Proposed System:

Blind authentication is able to achieve both strong encryption-based security as well as accuracy of a powerful classifiers such as support vector machines (SVMs) and neural networks. While the proposed approach has similarities to the blind vision scheme for image retrieval, it is far more efficient for the verification task. Blind Authentication addresses all the concerns mentioned

1) The ability to use strong encryption addresses template protection issues as well as privacy concerns.

2) Non-repudiable authentication can be carried out even between non-trusting client and server using a trusted third party solution.

3) It provides provable protection against replay and client side attacks even if the keys of the user are compromised.

4) As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked.

The framework is generic in the sense that it can classify any feature vector, making it applicable to multiple biometrics. Moreover, as the authentication process requires someone to send an encrypted version of the biometric, the nonrepudiable nature of the authentication is fully preserved, assuming that spoof attacks are prevented. The proposed approach does not fall into any of the categories. This work opens a new direction of research to look at privacy preserving biometric authentication.

Advantage:

The proposed approach is that we are able to achieve classification of a strongly encrypted feature vector using generic classifiers such as neural networks and SVMs 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 with no resort to computationally expensive protocols such as secure multiparty computation (SMC). 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.

Hardware Requirements

- SYSTEM : Pentium IV 2.4 GHz
- HARD DISK : 40 GB
- FLOPPY DRIVE : 1.44 MB
- MONITOR : 15 VGA colour
- MOUSE : Logitech.
- RAM : 256 MB
- KEYBOARD : 110 keys enhanced.

Software Requirements

- Operating system :- Windows XP Professional
- Front End :- Microsoft Visual Studio .Net 2008
- Coding Language : - C# 2008.
- Database :- SQL Server 2005

Modules:

Client side

1. Authentication module
2. Blind encryption
3. Encrypted data forwarding

Server side

1. Blind decryption
2. Biometric verification
3. Result forwarding

Module Description:

Client side modules:

1. Authentication module:

This module is to register the new users and previously registered users can enter into our project. The Register user only can enter into Proposed Process in our Project. The Other user can view Existing Of our Project

2. Blind encryption:

Blind in the sense that it reveals only the identity, and no additional information about the user or the biometric Data. In this module bio metric data encrypted using blind authentication method .the user doesn't know any information about key

3. Encrypted data forwarding

Data forwarding is a process of transferring data in a secure network. In this module blind encrypted data forwarded to server side.

Server side modules:

1. Blind decryption:

In this module client side encrypted bio metric data decrypted using key. Here used Asymmetric key blind decryption process the server didn't know any information about both encryption and decryption keys

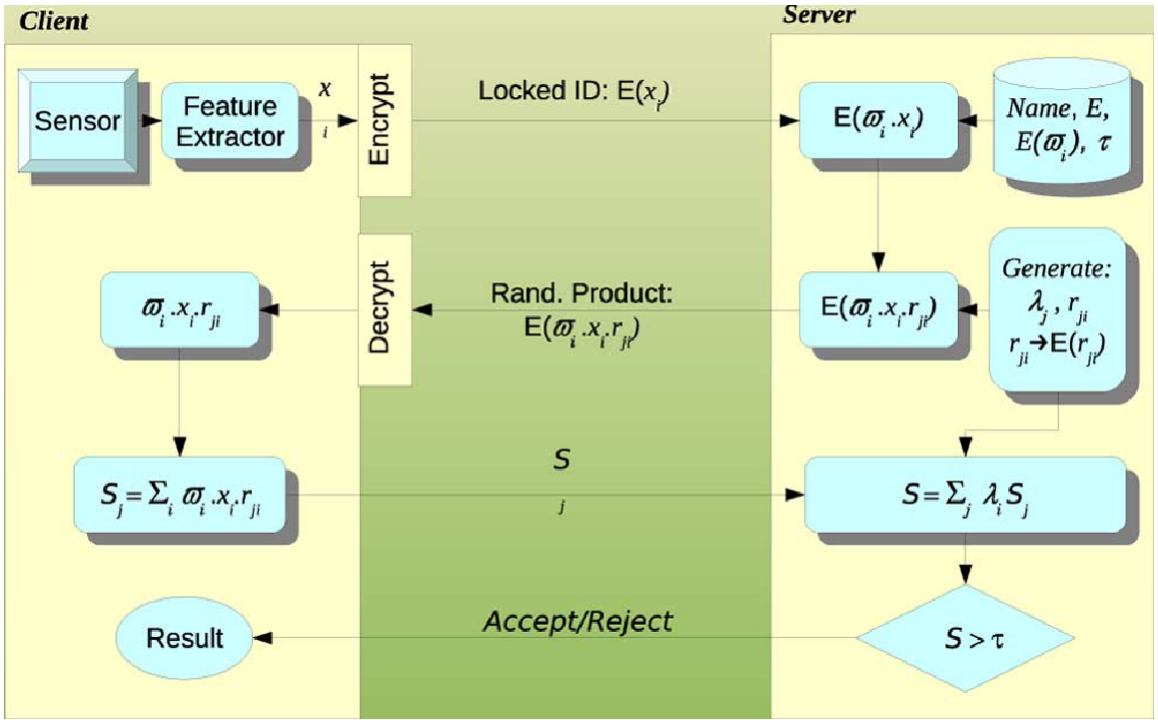
2. Biometric verification:

In this process biometric data that is finger print data compare with whole database data using the skeleton matching technique .in this matching depend on the each pixel of image.

3. Result forwarding:

Result forwarding is process output result passed to client side

Process Architecture Diagram:



REFERENCE:

Maria De Marsico, Michele Nappi, Daniel Riccio and Genoveffa Tortora, "NABS: Novel Approches for Biometric Systems", **IEEE TRANSCATIONS ON SYSTEMS, MAN AND CYBERNETICS, VOL.41. NO.4, JULY 2011.**