Endowing Double Layered Protection for Fingerprint Biometric Security System

Sasi Rekha Sankara, Booma Sankari

SRM University, Kattankulathur, Tamil Nadu, India, 603 203
rekhas_2006@yahoo.co.in

Abstract

Security plays a vital role from foyer to finale of essentials. According to research, Biometric is the pinnacle of high level of security, even though, recently Pilfering is strangely increasing in case of all biometric authentications, hence security of the biometric data is very essential for the real world applications. Fingerprint Biometric identification is very popular among the various biometric techniques and also where major pilfering was happening.

In this paper, we propose a more secure biometric fingerprint authentication, which addresses the concerns of user's privacy, security, and authentication. A small area sensor is used as an external device for laptop and desktop for fingerprint authentication. Fingerprint matching can be used as an additional to the password as a security measure in many secure sectors like online banking, online shopping or even replace online digital signatures. In this authentication system, we use the user's id and password as the initial level of security. The client and server do not exchange the user's extracted feature, i.e., finger print directly. Instead, a third party Enrollment Server is used to authenticate and encrypt the extracted fingerprint using an asymmetric encryption. The Enrolment server even sets the threshold value and sends the data to the actual server providing more security. This biometric authentication is designed to provide high security over public networks and trustworthy identity verification system through which the level of pilfering can be greatly reduced.

Keywords— Biometrics, Security, Fingerprint, Authentication, Encryption;

I. Introduction

Biometric is popular high security discipline used nowadays to access, measure and analyse biological data statistically to provide user authentication. Accessing of secured data or physical entry to restricted locations by unauthorised personals can be controlled and prevented. At the moment lot of company use simple biometrics identification to recognize employees, restrict the outsider's entry to high security labs and research fraternity. Regular scanning can be avoided by storing biometric data using digital encryption, smart cards and use it in applications like National ID card, building entry, computer access, security identification for bank safes, office-home security systems, internet banking and also at retail transaction at point of sales terminal. Biometric systems can be customized according to applications need but the basic requirements are Interface like scanner to capture biometric image from human input. Image processing needs to be performed using Digital Signal Processing. The result and access control information needs output interface. These three are essential requirements other than this it also needs other factors like power management, memory and finally a software that integrates all the mechanism.

Cryptography, on the other hand, "concerns itself with the projection of trust: with taking trust from where it exists to where it is needed". The problem of combining cryptography with biometric data is the noise, results are only fairly accurate not exact. The other predicament is that many users don't prefer to store data in a central database. Even though we say that biometric is unique to an individual but the data is not a secret as it can be captured by intruders using hidden cameras for face and iris or finger print from everywhere. It's hasty to rely only on biometrics as it is used in global scale at present.

II. Related Work

There is also some theoretical work on key extraction from noisy data. The fuzzy extractor is a recently proposed primitive to extract strong keys from noisy data such as biometrics. In this proposal, Dodis, Reyzin and Smith apply an error-correction code to the input, followed by a hash function and prove that the information leakage from the input data into the output of the hash function is negligible. This sort of approach can be useful if the noisy data can be kept secret. However, biometric applications lie between the extremes of secret data and fully public data. People leave behind fingerprints, and their irises can be photographed in a hidden; a biometric sample stolen in this way will reveal most of its entropy to the attacker. A related issue is issuing multiple keys for different applications. The fuzzy extractor scheme was modified by Boyen [22], in that a fixed permutation is applied to the iris-code bits before hashing. The compromise of one key derived from an individual's biometric does not compromise any other key derived from the same biometric using a different permutation. But this revised design still assumes that biometric data remain secret, and it fails completely whenever the original biometric is stolen. The third theory paper is by Juels and Wattenberg. Their fuzzy commitment scheme starts out with a random key, adds redundancy and XOR's this with the biometric code. So the key is completely independent of the biometric data. Our scheme is somewhat similar to theirs but with a number of important differences. First, we have developed a concrete coding scheme that works well with real biometric data. None of the papers so far, whether practical or theoretical, have solved this critical engineering problem. Second, we add an auxiliary secret – a password and an interaction with a token such as a tamper-resistant smartcard. We designed our scheme to give the best security available given the limitations of these authentication factors such as biometrics that might be compromised, passwords that might be guessed and tokens that might be reverse-engineered. This paper discusses privacy- enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) – while engaging a broad audience to consider the merits of the BE approach to verifying identity, protecting privacy, and ensuring security; The central message is that BE technologies can help to overcome the prevailing "zero-sum" mentality by adding privacy to identification and information systems resulting in a "positive-sum," win/win scenario for all stakeholders involved.

.

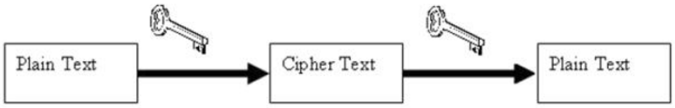
III. BIOMETRICS SYSTEM

"Biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and or behavioral characteristic possessed by that person" [2]. Signal processing, Data Transmission, Data Storage, Collection and decision system are the five subsystems in generic biometric. The proper enrolment increases the performance of the bio-crypt system. The performance falls due to poor system, low Enrollement quality, environmental factors and accidental events. The system fallback is high and security is compromised due to poor quality biometric data.

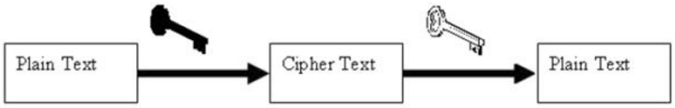
IV. CRYPTOGRAPHY

Hiding of information is known by a technique called as Cryptography. "Cryptography is exclusively to encryption, the process of converting ordinary information (plain text) into unintelligible data (ciphertext)" [8]. Decryption is a reverse process of converting the cipher text to plain text. Ciphering consists of a pair of algorithms which execute this encryption and the decryption process. There are two instances which control the cipher operation which are key and algorithm. The key acts a secret parameter known only to the sender and receiver of messages basically the communicants without which it's easy to break the message code.

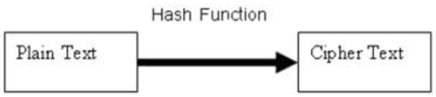
There are popular applications which use cryptography as security feature like E-commerce, ATM systems and password systems. It is used for authentication of data to protect it from alternation and theft. There are three types of cryptographic schemes used like "Secret Key (or symmetric) cryptography, Public-Key (or asymmetric) cryptography and Hash Functions", these are shown in Figure (1-3). In a public key encryption system two key are used while a single secrete key is used in symmetric encryption system. Whereas Hash function calculates a fixed length value from the plain text which is hard to recover. Each of these methods uses certain methods for optimization like integrity check used in Hash Function for plain text. In case of encrypted messages secret key a session key is generated based on encrypted message. Non-Repudiation is used in asymmetric scheme.



a) Secret Key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.



b) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

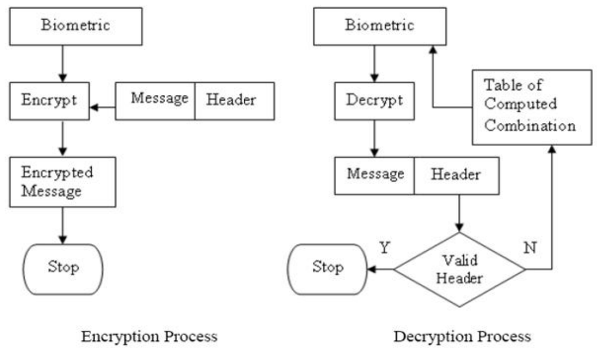


c) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

V. MERGING OF TWO TECHNOLOGIES BIOMETRICS AND CRYPTOGRAPHY

The two most popular technologies which complement each other in field of security is Biometrics and Cryptography. The trust is a key factor in providing assurance that the identified person is the correct individual. Whereas cryptography in protuberance by " taking trust from where it exists to where it is needed". Both key and document constitute to the secrecy of biometric feature using a key deploying various methods. These are the factors that needs to be looked into problems faced by using of Cryptography in Fingerprint Based Biometrics in designing a secure system

- System performance scales down highly because of poor quality image
- Inconsistency and instability is high as the same fingerprint image cannot be reproduced from the same user.
- Various security problems arise due to insecure storage media and key management



Fig

VI. FINGERPRINT IMAGE ANALYSIS

Though a large number of biometric features are used for identification, fingerprint is the oldest and commonly used. The main advantage of fingerprint biometric when compared to others is that it's cheaper, easy acquisition and operation simplicity. The simplicity has brought fourth broad collection of sensors in commercial market. These sensors can easily scan the fingerprint, also work on image processing by accepting a valid image and rejecting a fake one. The fingerprint needs to be classified as it acts crucial aspect in any fingerprint application because the quality of captured image and validity relies on the performance. A fingerprint is a collection of associated curves in which the dark and bright curves known as ridges and valleys. Valley and ridge patterns are main texture in the local structure of a fingerprint with minutiae points constituting to the details. The global structure puts a smooth flow to the overall patterns. The analysis of ridges to valley is done to check the image validity; image quality is checked using global and local structure. The Region of Interest (ROI) of fingerprint is detected from which useless and ineffective furrows and ridges of image are discarded as it contains only background information.

A. Analysis of Fingerprint Pattern Using Local Information

The fingerprint components derived from regions that are spatially restricted which are used for local representations of the fingerprint image. The fingerprints baseline local information is from salient features of the ridges, pores of ridges, finger ridges. The "minutiae of ridges" acts as a minute detail which is a widely used local feature. Finger pattern brings out minutiae a point that occurs at ridge ending or ridge bifurcation or local discontinuities. The minutiae types that have been identified sum up to 150 in no. Finger print system uses two types of minutiae which are ridge bifurcation and ridge ending. The fingerprint is converted into a compact and valid representation when it's localized. The validity judgment of fingerprint image is dependent on the following factors: ridge, image contrast, valley clarities, graphical representation of fingerprint elements and noise infection play a vital part in valid judgment of the fingerprint image. The pixel value represents the grey value maps and the light intensity which is derived from local fingerprint information. Local information is used to infer pixel representation in enhanced form, calculation of threshold, using enhancement percentage for performing validity check and grey level for segmentation. Factors like smudginess, goodness and dryness are determined by the local analysis of the whole fingerprint. The wetness is identified from factor like domination of black pixel, dryness of finger by comparing the average ridge thickness larger than value of one valley. Statistical value play a vital role in identifying the damages in a fingerprint image by calculation Standard Deviation and Mean Value from a fingerprint local block division. A small deviation of valley and ridge is valid in a fingerprint.

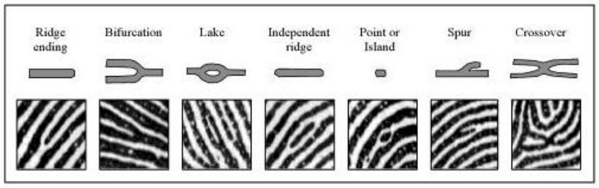


Fig : Minutiae of Ridges

B. Global Analysis

Finger's attributes is globally represented by a examining single entity which represents the entire finger. The valleys and ridge patterns in a human finger has a global structure. The information that is derived from a finger print has a lot of key facts. The foremost resultant information received from the patterns valleys and ridges of a human finger image is overall flow. Traditionally minute points are used which provides un-prejudiced information when compared to the current technique of global representation. The fingerprint classification is contributed by features singularities and global ridge structure available in global finger print structure. These two techniques are very advantageous to the alignment of images of finger print which are poor or incomplete. The finger print images are analyzed for localized texture pattern using global structure, while the invalid fingerprint images are detected by analyzing the ridge to valley structure. The distinctiveness that is available in these images is continuity and uniformity. These two characteristics ensure that a whole image is used. Though a lot of structuring features are used amongst that the most frequently used are:

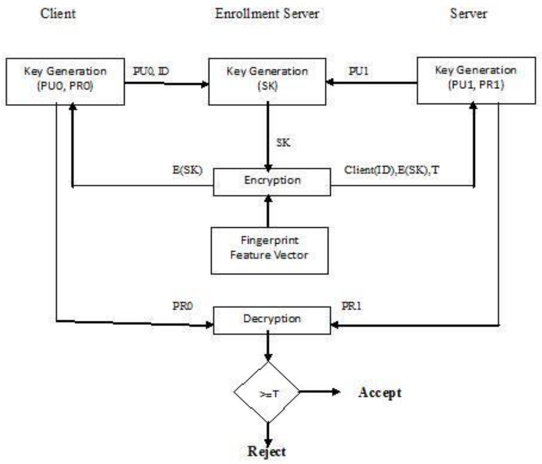
Fig

- Singular points – The core and the depth are most popularly used orientation field. The higher most of the innermost curving ridge and the meeting point where the three ridges meet. These two characteristics are widely used for classification and registration of finger print.
- Ridge orientation map – Its representation of the ridge valley structure. The special operations like filtering, image enhancement, classification and minutia feature verification.
- Frequency Map of Ridge – The ridge distance value perpendicular to the local ridge orientation is used to calculate the reciprocal. This value of the fingerprint image is expansively used for contextual filtering.

VII. CRYPTO KEY GENERATION

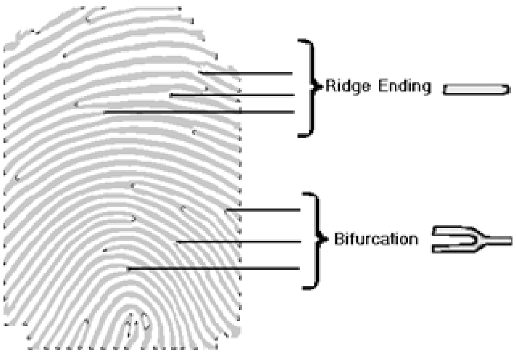
The minutiae from the acquirement stage are taken as inputs for the key generation stage where some mathematical operations are performed. These mathematical operations generate vectors from the set of minutiae points and these vectors can be considered as a 109 key in simple way. A reconstruction of minutiae points will be used to make these points more secure to generate a combined encapsulated cryptographic key based on reforming graph and adjacency matrix of extracted minutiae data.

Block diagram of server & client



VIII. AUTHENTICATION

1. In this algorithm the client who wants to log into the system has to cross the basic security barrier of giving his username which is used to verify the identity of the client to the server. The authenticated client is asked for the scanning the fingerprint, from which the feature vector is calculated. The client encrypts the extarcted image using its own private key PR0, [Epro(Xi)]. The client is requested to give its password which is encrypted using the secrete key (SK) along with the encrypted fingerprint image [Esk(Pwd,Epro(Xi))]. The client id is also sent along with this data to the server [CID+Esk(Pwd,Epro(Xi))] → S. The server decrypts the packet using the appropriate keys sets and retrieve the values. The server compares the received image with the existing sets and compares the threshold value. If the image is up to threshold value its accepted else its rejected.



1) Algorithm

2. The client computes Feature Vector from the extracted Finger Print Test Data.
3. The Finger Print Feature is encrypted using the Client’s private key [Epro(Xi)]
4. The encrypted feature vector together with the client password is encrypted using the Secrete Key [Esk(Pwd,Epro(Xi))]
5. The encrypted packet is sent with the client id to the Server. [CID+Esk(Pwd,Epro(Xi))]
6. The Server decrypts the packet and checks with client Biometric Sample using threshold value
7. If Xi>=T
8. Return Accepted to the client
9. Else
10. Return Rejected to client
11. endif

IX. ENROLLMENT

The Enrollment of the client, giving multiple samples to the Enrollment Server (ES), for example in a banking system the client may go to the bank security enrollment officer and give their finger biometric samples. The client is asked to come in person to check the personnel identity and assure the system that the first time samples are extorted from the authentic account holder. The Enrollment Server calculates the threshold value based on the procured sample set. To employ double level security both Symmetric and Asymmetric Encryption methods are employed. The ES generates a Secrete Key (SK) using a prime random number generator which will be applied by both Client and Server. At the same time the Enrollment Server notifies both client and server to generate the asymmetric key pair using RSA. The both Client and Server generate a Public and Private Key pair using RSA (PU_0, PR_0) and (PU_1, PR_1). The server sends the Public Key PU_1 to the Enrollment Server. The next step is that client sends its identity (CID) and its public key PU_0 to the Enrollment Server which will be sent to the server. The Secret key is sent client in an encrypted format using the clients public key PU_0 $[E_{PU0}(SK) \rightarrow C]$ by the Enrolment Server. The Enrollment Server sends the Secrete Key, Client ID (CID), Public Key PU_0 and threshold value T $[E_{PU1}(SK,CID, PU_{0,} T) \rightarrow S]$ to the server. The Client and Server decrypt Secrete Key using their private keys. Finally the Enrollment Server notifies both Client and Server about success of enrollment procedure.

2) Algorithm

1. Enrollment Server (ES) collects multiple samples from client biometric,
2. ES sets the Threshold Value based on samples
3. ES generates the Secrete Key (SK) for client and server.
4. Client generates a Public and Private Key pair using RSA (PU_0, PR_0)
5. Server generates a Public and Private Key pair using RSA (PU_1, PR_1)
6. Server send its Public Key’s to ES
7. Client sends its identity and public key to the Enrollment Server
8. The ES sends the encrypted Secrete Key (SK) to client using PU_0 $[E_{PU0}(SK) \rightarrow C]$
9. The ES sends to the Server, the encrypted value of SK along with Client ID (CID), Public Key PU_0 and threshold value T $[E_{PU1}(SK,CID, PU_{0,} T) \rightarrow S]$
10. Both Client and Server decrypt SK using their private keys
11. The client and Server is then notified about success by the ES.

RESULTS

Factors	Finger without cryptography	Finger without cryptography
Equal Error Rate	2-3.3%	<1.5%
Failure to Enroll	3%	2.2%
Nominal False Accept Rate	2%	<1.3%
Nominal False Reject Rate	0.1%	<1%
Liveness Aware	No	Yes

Conclusion:

To conclude in the above work we are trying to remove the falsification as well as to give more security to e-users by merging two popular technologies of biometrics and cryptography. We affirm the security difference when comparing to the existing fingerprint systems used for authentication. Our main future work is to enhance the security and reduce the timing using a different encryption methodology.

REFERENCES

[1] Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (March 2007) at www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

[2] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm" in *Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition ,and applications* Innsbruck, Austria ACTA Press, 2006, pp. 95-98 .

[3] M. S. Altarawneh, W.L.Woo, and S. S. Dlay, "BIOMETRICS AND FUTURE SECURITY," in *Proceedings of MU International Conference on Security, Democracy and Human Rights*, Mutah, Jordan,

10-12 July 2006.

[4] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, “Handbook of Fingerprint Recognition”.

[5] M. Christodorescu. Private Use of Untrusted Web Servers via Opportunistic Encryption. In Web 2.0 Security and Privacy, 2008.