IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. IV (Sep. – Oct. 2015), PP 129-132
www.iosrjournals.org

Securing Biomtric Template Over Non-Secure Channel using Cryptography and Helping Data

Manmohan Lakhera
Assistant Professor, Computer Science Omkarananda Institute of Management & Technology Rishikesh, India
Dr MMS Rauthan
Dean, Department of Computer Science, HNB Garhwal University, Srinagar Garhwal, India

Abstract: *the security of biometric template is a very important aspect in the biometric system. Biometric template are the very important parts of biometric systems and attacker mostly attack on template over non-secure channel so securing them is a very crucial. In this research paper our focuses on securing biometric template in non-secure channel. We develop an algorithm for securing fingerprint template and fetching partial information of IRIS as a helping data. AES is used as a cryptographic algorithm.*
Keywords-component: *Encryption, Public Key, Private Key, Verification, Password*

I. Introduction

The main concern of how to secure stored biometric data is the vital design challenge that is addressed by this paper. Main vision of this paper is to secure stored biometric data with help of password. It focuses on secrecy of passwords in the case where password stored in personal computer's database in normal text format is compromised that's why passwords are not stored in normal text format, and only the hash code of password is stored. The hash is effectively impossible to invert. During verification a user enter password, which insert at the time of enrollment. Permission is only granted when the hash value of the new inserted password have matches the hash value of the stored password which had entered at the time of enrollment. The secrecy of password never compromised even if attacker studies about the stored hash value because of the non-invertible features of hash value. Basically biometric system divides into different modules. The sensor module obtained an individual's row biometric data in the different form like audio, video, image. Required Biometric data is extracted by extraction module. During user enrollment the extracted biometric data, label with the user's individuality, is stored in the database and is known as a biometric template. At the time of user verification the corresponding module compares the set biometric data extracted during verification with the stored biometric data and produces match result. Produces result is verified by the decision module this match either verified individual identity or rejects the verification request. Thus, the biometric system behaves like a pattern recognition system which contains two different classes genuine and fake. These classes identified that user is original user or fake user. If fake then corresponding class reject the request and if genuine then corresponding accept the request and provide access to the required system or database.

II. Related work

The biometric data attack is categorized in various categories which contain different type of threat these are as follows this point of attack is known as "Attack on the feature extractor module". In this attack, the attacker can replace the feature extractor module with a Trojan horse [1].

Biometrics cannot be revoked: A biometric feature is permanently associated with an individual, and a compromised biometric sample wills compromise all applications that use that biometric. Such compromise may prevent a user from re-enrolling [2]. Note, however, that this concern implies that biometrics is secret, contradicting the previous consideration.

Biometrics are not secret: Technology is readily available to image faces, fingerprints, irises and make recordings of voice or signature- without Subject consent or knowledge [3][4]. From this perspective, biometrics is not secret.

As per Ross et al. [5] have demonstrated a technique to reconstruct fingerprint images from a minutiae description, without using match score values. First, the orientation map and the class are inferred based on analysis of local minutiae triplets and a nearest neighbor classifier, trained with feature exemplars. Then, Gabor-like filters were used to reconstruct fingerprints using the orientation information. Correct classification of finger print class was obtained in 82% of cases, and regenerated images resembled the overall structure of the original, although the images were visually clearly synthetic and had gaps in regions which lacked minutiae. Another valuable contribution of this work is calculation of the probability density fields of minutiae; such information could be used to attack fingerprint based biometric encryption schemes

Hill [7] if some data of biometric (minutia) are available, then there is some possibility to effectively build artificial biometrics that pass verification. Schneier [7] briefly summarized that if the biometric data of an individual is theft, it means the identity of an individual is theft. This means that once the biometric feature is compromised, user lost their identity, so the security of biometric data is more important. Biometrics contains sensitive personal information this is another type threat. [8][9][10] Shown that fingerprints hold some genetic information. Ratha et al. [11]find out the different type of attack that can be produce against a biometric system (i) the artificial finger used at the sensor using false biometric attribute, (ii) the biometric data resubmitted which is modified by attacker (iii) Biometric feature extractor may be swapped by a Trojan horse program that produces prearranged biometric attribute sets, (iv) real biometric set of attribute may be replaced with fake set of biometric attribute, (v) Trojan horse program replace the matcher which create a problem at the verification time so the security required for biometric security, (vi) the biometric data stored in the database may be modified or removed, or new biometric data may be inserted in the database, (vii) the final result output by the biometric system may be dominated and (viii) the data may be modified in the network at time when various Communication channel communicate with biometric system. An artificial biometric (such as an artificial finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of attack. The biometric data detectors do not take the real values obtained from the sensor but instead it is forced to generate the value which is given by the attacker. The biometric attribute extracted using the data obtained from the sensor is replaced with a fake biometric attribute set. The matcher component could be attacked to produce high or low matching scores, regardless of the input biometric set. The channel between the database and matcher could be negotiated to alter transferred biometric data. One of the attacks is to change the final matcher result itself. All of these attacks have the risk to reduce the integrity of a Biometric system [12]. Sun et al. [13] projected a template called KMT, or Key-Mixed Template. The basic idea behind the projected template is to use the template in combination with a secret key to create a new Biometric template. Template and secret key is combined at the use end and verified at the server side with database. By having a separate secret key per verification system, having a template compromised does not necessarily mean the attacker can gain access to all systems that use that biometric template. This new template can help to prevent backend attacks, snooping, and tamper attacks without a performance hit. Andrew B. J. Teoh et al. [14] was proposed the concept of cancelable biometrics to express biometric templates that can be cancelled and restored with the addition of another independent authentication factor. A kind of cancelable biometrics that merges a set of user-specific random vectors with biometric features is known as BioHash. The quantized random projection collection on basis of the Johnson-Linden strauss Lemma was employed to accomplish the mathematical foundation of BioHash. Depending upon this model, they have explained the characteristics of BioHash in pattern recognition in addition to security viewpoints and provided some methods to resolve the stolen-token problem. [15]The two major requirement of biometric template protection is cryptosystem and cancelable biometrics which is also known as helper database and feature transformation respectively

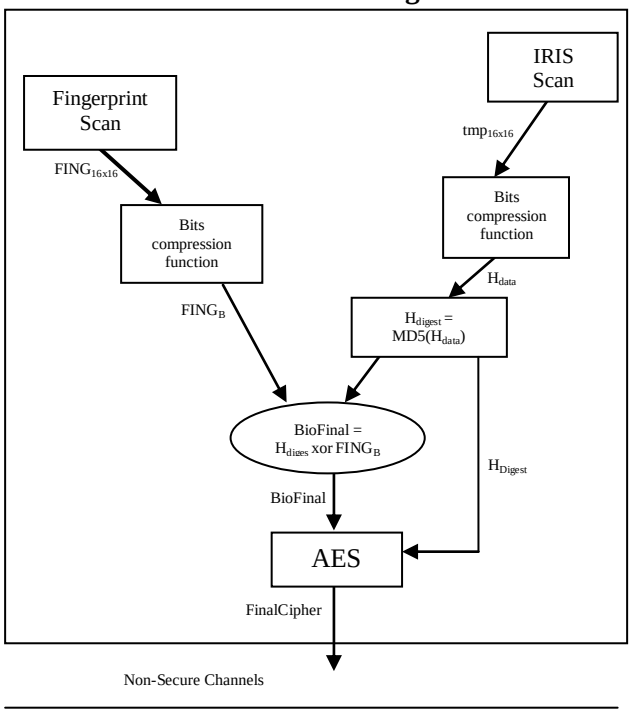
Incapable of being reversed: It may be impossible to reconconstruct the secure biometric template from stored referenced biometric data (feature).While normal biometric template can be easily generated.

Observability: multiple versions of protected biometric secure template not allow reconstructing while normal Templates can be regenerated by same biometric data.

III. Notations

In this research paper $FING_{16X16}$, tmp_{16X16} are the 16X16 bit array used for storing the captured fingerprint and Iris data bits. $FING_B$ and H_{data} are 8X16 bit array where selected data of $FING_{16X16}$ and tmp_{16X16} is stored. H_{digest} is a variable where hash result of H_{data}(IRIS) stored. BioFinal is a variable where XOR result of H_{data} and $FING_B$ stored; CipherFinal is variable which contain the final cipher text of proposed method.

IV. Block Diagram



V. Equations

$$FING_{16X16} = Caputred(Fingerprint)$$
$$tmp_{16X16} = Caputred(IRIS)$$
$$FING_B = Selected(FING_{16X16})$$
$$H_{data} = Selected(tmp_{16X16})$$
$$H_{digest} = MD5(H_{data})$$
$$BioFinal = FING_B \text{ xor } H_{data}$$
$$CipherFinal = AES(BioFnal, Key(H_{digest}))$$

$Selected(FING_{16X16})$
Begin:
FOR I=0 to 16
FOR J=0 to 16
IF J mod 2= 1 then
$FING_B = FING_{16X16}[i][j]$
End:

$Selected(tmp_{16X16})$
Begin:
FOR I=0 to 16
FOR J=0 to 16
IF J mod 2= 0 then
$H_{data} = tmp_{16X16}[i][j]$
End:

I. ALGORITHM FOLLOW BY SECURIING BIOMETRIC DATA IN INSECURE CHANNEL

Step1: Captured fingerprint image from biometric device
Step2: Choose selected 128 bit data from inserted fingerprint and store the selected data into $FING_B$
Step3: Captured helping data IRIS from biometric device.
Step4: Compress the inserted IRIS data into 128 bit and stores it into H_{data}
Step5: helping data (H_{data}) converted into the 128 bit digest data H_{digest}

Step6: Xored the fingerprint data $FING_B$ and hash value of helping data H_{digest}. the xored result store into BioFinals.
Step7: In AES algorithm BioFinal is used as a plaintext and H_{digest} as an encryption key.
Step8: Final Cipher text CipherFinal send by non-secure channel.
Step9: H_{digest} send via RSA to the destination.

VI. Conclusion

We have discussed how to biometric data send in no-secure channel. We have specifically highlighted techniques that can secure biometric feature from attacker or unauthorized person. We discuss the importance of Public Key Cryptography and AES to enhance the confidentiality of biometric data. Security for Biometric data in non-secure channel may be used to protect the communicated biometric data when the user send the biometric data via non secure channel. Also, this technique provides security at the time when user claim for their biometric data for verification process. The verification process is also undergoing via security process.

References

[1] Ao Shan, Ren Weiyin, Tang Shoulian "Analysis and Reflection on the Security of Biometrics System" 2008 IEEE..
[2] Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40:614{634
[3] Schneier B (1999) the Uses and Abuses of Biometrics. Communications of the ACM 42:136, 1999.
[4] Inter National Committee for Information Technology Standards (INCITS) (2006) Study Report on Biometrics in E-Authentication, Technical Report IN-CITS M1/06-0693
[5] Ross A, Shah J, Jain AK (2005) Towards Reconstructing Fingerprints from Minutiae Points. In Conf. SPIE Biometric Technology for Human Identification II, 5779:6880
[6] Hill, Chris J, "Risk of Masquerade Arising from the Storage of Biometrics"Australian National University: s.l.Bachelor of science thesis, Dept. of CS, Nov 2002.
[7] Schneier.,"Bruce., Inside risks: The uses and abuses of biometrics," Communications of the ACM, Vol 42 ed, ACM New York, NY, USA, August 1999
[8] Babler, "W.J, Embryologic development of epidermal ridges and their configuration,"Birth Defects Original Article Series, Vol. 27(2). ed., New York, 1991.
[9] Mulvhill, J.J, "The genesis of dermatoglyphics," Published by Elsevier Inc, 4 ed, October 1969.
[10] Penrose, L.S. "Dermatoglyphictopology," Nature,Vols. 205:545–546 ed, s.l, 06 February 1965.
[11] N. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength,"Proc. Audio and Video-based Biometric Person Authentication(AVBPA), pp. 223–228 ed, June 2001
[12] U.Uludag, A.K.Jain, "Hiding biometric data," IEEE Transactions On Pattern Analysis And Machine Intelligence,11 ed., Michigan State Univ., USA, Nov.2003
[13] S. Sun, C Lu, and P. Chang, "Biometric Template Protection: A KeyMixed Template Approach," Digest of Technical Papers. International Conference, Las Vegas, NV: Consumer Electronics, 2007. ICCE 2007, 10-14 Jan. 2007
[14] Teoh AB, Yuang CT, "Cancellable Biometrics Realization with Multispace Random Projections",IEEE Trans Syst, pp:1096-106, ed, 2007.
[15] Christian Rathgeb and Andreas Uhl, "A survey on Biometric Cryptosystems and Cancelable Biometrics," EURASIP Journal on Information Security, Austria, 2011