Robust Security Model for Biometric Template Protection using Chaos Phenomenon

Prof. Maithili Arjunwadkar
Assistant Professor
Modern College Of Engineering, Pune
Maharashtra , India

Prof. Dr. R. V. Kulkarni
Professor & Director
SIBER,
Kolhapur , Maharashtra , India

ABSTRACT
Modern biometric technologies claim to provide alternative solution to traditional authentication processes. Even though there are various advantages of biometric process, it is vulnerable to attacks which can decline it's security. Different schemes are proposed to protect from different attacks. This paper presents biometric process, attacks on biometric process, study of different protection techniques used to protect against different attacks. The authors have designed protection model of bio-hashing technique using Session key. This key is generated using Chaos phenomenon.

General Terms

Biometric template Protection Approach

Keywords
Security, biometric process, biometric template protection schemes, chaos phenomenon

1. INTRODUCTION
Modern biometric technologies like biometric based authentication system that uses physiological (e.g. thumb print, retina scan, iris) or behavioral (e.g voice, keystroke, touch) claim to provide an alternative for traditional authentication systems that are based on password (token-based) and key (knowledge based). Biometric process or biometric encryption process is divided into two processes namely enrollment & authentication process. During the enrollment process, the user's physiological & behavioral characteristics are captured by the sensor. The different feature extractor or key binding algorithms are used to create biometric template. The template is stored during enrollment process to be compared in the future to the one produced during an authenticate process. The stored template & the one produced during authentication process is compared by matching algorithm that produces matching result (response Yes/NO). The match response is then sent to the application, on which a decision algorithm is implemented for granting or denying access to the user.

2. LITERATURE REVIEW
Even though there are various advantages of biometric process, it is vulnerable to attacks, which can decline it's security. Ratha et al [3] analyzed these attacks and grouped them into eight classes. Dimitriadis [4] also suggests different attacks on biometric process. This paper considers only template database attacks which involve the attack on template database (e.g. adding new template, modifying an existing template, removing template etc.) The biometric template is stored in smart card, central repository and sensing device. The imposter can insert a fake template or templates in the system where biometric templates are stored centrally to gain unauthorized access and lawful user faces Denial of service. To avoid this smart cards are preferred. In that case, the template is stored in write once and erased or destroyed if altered technique. When this scenario is not an option, strong security controls or protection schemes must protect the template. [2]
To protect the database from imposter, different schemes are used.
The template protection schemes proposed in the literature can be broadly classified into two categories

- Feature transformation approach
- Biometric cryptosystem.

In the feature transform approach, a transformation function (F) is applied to the biometric template (T) and only the transformed template (F(T;K)) is stored in the database. The parameters of the transformation function are typically derived from a random key (K) or password. The feature transform schemes can be further categorized as invertible and non-invertible transforms. In invertible transforms, an adversary gains access to the key and the transformed template, it can recover the original biometric template (or a close approximation of it). Hence, the security of the invertible scheme is based on the secrecy of the key or password. On the other hand, non-invertible transformation schemes typically apply a one-way function on the template and it is computationally hard to invert a transformed template even if the key is known. Biometric cryptosystems were originally developed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features, so known as helper data-based methods. Biometric cryptosystems can be further classified as key binding and key generation systems depending on how the helper data is obtained. When the helper data is obtained by binding a key (that is independent of the biometric features) with the biometric template, we refer to it as a key-binding biometric cryptosystem. Note that given only the helper data, it is computationally hard to recover either the key or the original template. Matching in a key binding system involves recovery of the key from the helper data using the query biometric features. If 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 leads to a key generation biometric cryptosystem. Some template protection techniques make use of more than one basic approach. [5]

Bio-hashing or salting is one of the invertible transformation biometric protection scheme approach, in which user specific key or password is used for transformation. In this approach key needs to store securely or password needs to be remembered by the user and present during authentication. [6]

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect biometric template. If a cancelable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancelable biometrics is non- invertible approach. [7] Even if the transformation function is known & the resulting transformed biometric data are known, the original (undistorted) biometrics cannot be recovered. Steganography and Watermarking techniques are considered. Steganography is the science of hiding information. Steganography based techniques can be suitable for transferring critical biometric information from template storage to the matcher. A Watermarking technique can be used for protecting database as well as transferring on channel. Watermarking is technique in which one pattern is embedded or inserted into another pattern for example finger print data can be embedded with face data. Another technique which is used to prevent channel attack is challenge-response system. One approach is the image based Challenge-response method where the challenge is presented to the sensor and the response string computed depends on the challenge string and the content of the input image acquired [3].To make these approaches and techniques robust, intelligent models can be used like Chaos phenomenon.

3. MODEL DEVELOPED FOR BIOMETRIC PROCESS.

- **Chaos Phenomenon**

Chaos variables are usually generated by the well-known logistic map. The logistic map is a one-dimensional quadratic map defined by:

Xn+1= μ Xn(1-Xn)

Where 0<=X(n)<=1 'μ' is a control parameter. For μ=3.99 or μ=4, generates chaotic evolutions. Chaotic system is deterministic and sensitive to the initial values. According to this feature, it has complex active action, which can be used to protect data content. For example, the random sequence produced by chaotic phenomenon can be used to encrypt data in secret communication. This property makes the initial value suitable for the key that controls the data encryption or decryption. The one-way property makes neural network a suitable choice for hash function also [1, 8].

The model described in fig. 1 stores the encrypted Biometric Template using Session Key. This approach is nothing but bio-hashing or salting approach using key. A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications session.

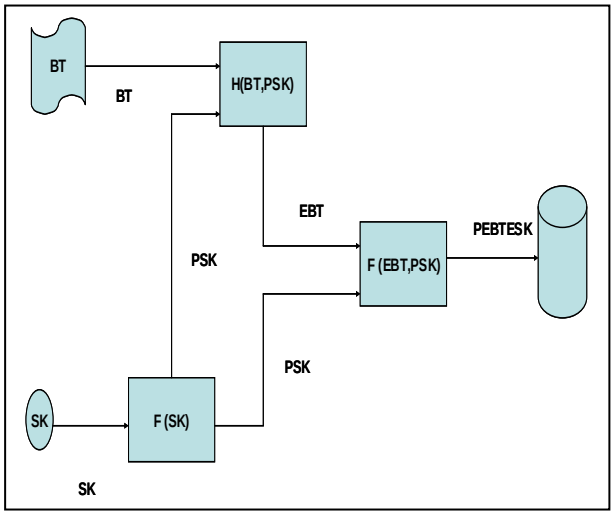

FIGURE 1: Salting technique Enrollment phase

BT: Biometric Template generated from Biometric process or Biometric Encryption Process

SK: Session key can be created using chaotic phenomenon As a result no chance of value of session key getting duplicated. The FIGURE 2 shows 100 session keys generated by chaotic phenomenon which are not repeated

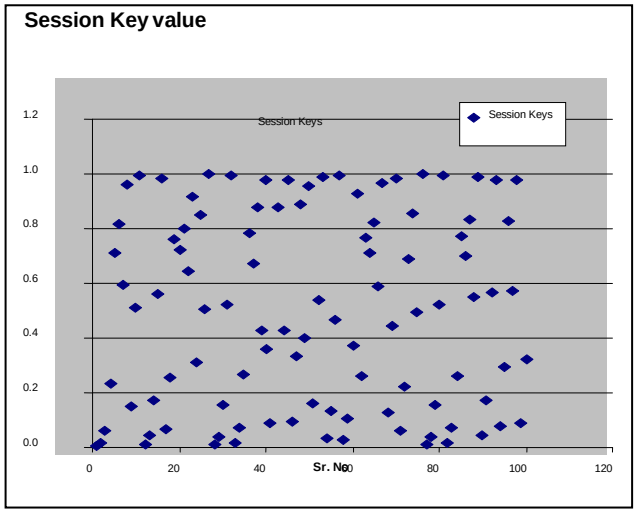

FIGURE 2: session keys

Graph shows no repetition of session keys when μ =3.99. This can make guessing of session key very difficult when it is generated by chaotic phenomenon.

PSK: Permuted session Key. To generate this expanded permuted transformation of SK ,F(SK) function is used.

EBT: Encrypted Biometric template. To generate this encrypted template hash function H(BT,PSK) is used. The neural networks have also a one-way property. For example, if a neuron has multi-inputs and single-output, then it is easy to obtain the output from the inputs but difficult to recover the inputs from the

output. These properties make them suitable for hash function design.[8]

Hash function H(BT,PSK) uses simple X-OR function & both F(SK),F(EBT, PSK) functions uses permutations of bits of SK, EBT and ESK respectively

PEBTPSK: Permuted encrypted BT and permuted SK To generate this final concatenated Biometric template F(EBT,PSK) is used.

Same Session Key & functions are used for decryption of encrypted biometric template.

4. FUTURE RESEARCH

In this paper the authors studied different invertible and non-invertible biometric template protection schemes and different techniques like steganography, watermarking, challenge-response techniques to protect biometric templates. They designed bio-hashing model using session key which is created using Chaos Phenomenon. Intelligent models like ANN, expert system, fuzzy logic models can be used for enhance those approaches or techniques. In future the research will expand the other different methods using these models for approaches and techniques. And design an expert system with rules for selecting specific approach and technique to avoid attacks on biometric system using these intelligent models.

5. CONCLUSION

In spite of the various advantages of biometric process, it is vulnerable to attacks which can reduce their security. Intruder can attack on biometric template database Different protection approaches are proposed to protect biometric template. The protection schemes like bio-hashing using session key which is generated by chaotic phenomenon is designed. The session key generated using this approach, makes this model robust to avoid risk of guessing of session key.

6. REFERENCES

[1] Neural Network Learning based chaos by Truong Quang Dang Khoa & Masahiro Nakagava in International Journal of computer & system Science & engineering 1:2 2007

[2] International Journal of computer & system Science & engineering 1:2 2007

[3] Intelligent system for information security Management: architecture & design issues by Marina Hentea in Informing science & information technology vol. 4 2007.

[4] Ratha, N.K., J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3

[5] Biometric risk and controls by Christos K. Dimitriadis in Information Systems control Journal Vol 4 2004

[6] Uludag U, Jain AK (2004) Attacks on Biometric Systems: A Case Study in Fingerprints. In Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI 5306:622{633

[7] Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric Cryptosystems: Issues and Challenges. Proc. IEEE, 92:948{960

[8] Security of Biometric Authentication System By Parvathi Ambalakat Biometric 21st Computer Science Seminar One way hash functions based on neural network Shiguo Lian,Jinsheng sun, Zhiquan Wang

[9] Risk and Controls By Christos K. Dimitriadis, www.isaca.org

[10] Artificial neural network notes.