A Study on Biometric Template Protection Techniques

Poongodi.P[1], Betty.P[2]

1- PG Scholar, Department of CSE, Kumaraguru College of Technology
2-Assistant Professor, Department of CSE, Kumaraguru College of Technology
Coimbatore, Tamil Nadu

***Abstract*— Biometrics is a technique that is used to identify a person using quantifiable biological or behavioral characteristics. It is used to identify individuals in a group that are under surveillance based on stored templates in the database.To prevent fradulent acts like faking ID badge or licences and to ensure Security and privacy Biometric is used.Though Biometric process has several advantages it is vulnérable to attacks which compromise the Security objectives of the system.The different modules of biometric system are affected by various attacks of which securing the biometric template became a serious issue. In biometric systems the template and the database are critical parts. Biometric template is usually attacked by the attackers. Item is vulnerable to attacks which cause lack of security.Biometric Security must ensure Confidentiality, integrity, availability. Different types of template protection schemes like Biometric cryptosystem, Watermarking technique, Intelligent approach are available. Biometric cryptosystem securely bind a digital key to biometric or generate a key from the biometric resulting in biometric template protection. Watermarking approach is the process of embedding one pattern into another pattern. Intelligent based approach is simple and efficient. This approach is capable of autonomous action whenever the things go wrong in the system. A detailed survey on these template protection schemes and their advantages and disadvantages was discussed.**

***Keywords*— Biometric template-Security-Multiagent system-Database audit.**

I. INTRODUCTION

The demand for authenticating a person is growing, due to the prospering of electronic commerce and fear of terrorism. Traditional ways of personal identification like ID cards and passwords are no longer sufficient. People now turn their attention to biometrics. Biometrics is physiological or behavioural characteristics unique to individuals. This includeFingerprint,handgeometry,handwriting,iris,retinal,vein, voice.As biometrics use just parts of human body, they are practically impossible to get lost and the efforts of thinking of untraceable password can be avoided. Additionally, in most of the cases, authentication using biometrics is more convenient and faster than using ID cards and passwords.

Security is a quality of being secure or free from danger or protection against adversaries-from those who would do harm intentionally. Confidentiality, integrity, availability are the main properties of Biometric security. A successful organization should have following layers of security in place to protect its operations

Physical security: It involves protection of physical items, objects, or areas from unauthorized access and misuse.
Personal security: It involves protection of the individual or group of individuals who are authorized to access the organizations and its operations. The risk of staff or contractors exploiting their legitimate access to secured information for unauthorized purpose is controlled.
Operational security: It involves protection of the details of a particular operation or series of activities.
Communication security: It involves protection of communication media, technology and content from adversaries.
Network Security: It involves protection of networking components, communication, contents etc.
Information Security: It involves protection of information assets.

II. REVIEW OF BIOMETRIC TEMPLATE PROTECTION TECHNIQUES

A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample. Templates play a vital role in biometric authentication process. Initially biometric trait like fingerprint, iris is captured by the sensor, salient features are extracted using some feature transformation technique and get converted into digital form. This digital information is stored in the database which is known as Biometric template. Later the template is used during authentication purpose.
Attacks on Biometric template are the following

a) Template can be replaced by an imposter's template to gain unauthorized access

b) Physical spoof can be created from template to gain unauthorized access to the system.

c) The stolen template can be replayed to matcher to gain unauthorized access.

An ideal template protection scheme should possess the following properties:
Diversity: The secure template [1] must not allow across matching across the databases, thereby ensuring users privacy.
Revocability: It should be straightforward to revoke compromised template and reissue a new one based on the same biometric data.
Security: It must be computationally hard to obtain original biometric template from secure template.

Performance: The biometric system should not degrade the recognition performance of the biometric system.
Different types of template protection techniques are shown in Fig 1.

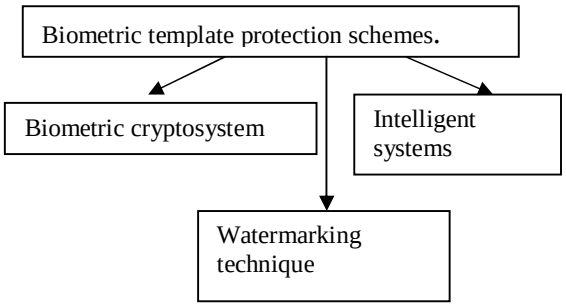


Fig 1.Different Template Protection Techniques

A. Biometric cryptosystem

In [2] Biometric cryptosystem approach some public information about the biometric template is stored. Because of this, this approach is known as helper data based method. Helper data does not reveal any significant information about the original biometric template. It is further classified into 2 types Key binding and Key generating approach. If the key is obtained by binding a key independent of the biometric features with the biometric template is known as Key binding approach. If the helper data is derived from the template and the key is directly generated from the helper data and query biometric features is Key generation biometric cryptosystem.

1). Advantages of Biometric cryptosystem

1.Tolerant to intra-user variation.
2.In cryptographic application direct key generation is very useful.

2). Disadvantages of Biometric cryptosystem

1. Generation of key with high stability and entropy is difficult.
2. Diversity and revocability is not ensured.
3. Careful attention is needed while designing helper data as it is based on specific biometric features.

B. Watermarking approach

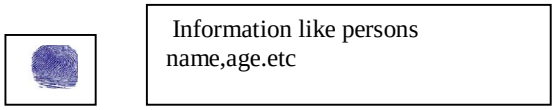
By using watermarking approach [4] security of Biometric template is ensured. The template can be damaged or forged by the attacker. Process of embedding one pattern i.e. one biometric trait into another pattern is known as Watermarking approach. Only if the attacker knows the watermark information he can forge or replace the biometric template. Parity checker method is used in watermarking approach. Fig 2. explains working of Watermarking approach.

1). Advantages of watermarking approach

1. Hard to forge the stored biometric template.
2. Provides high security to biometric template.

2). Disadvantages of watermarking approach

1. Time complexity in inserting watermark features.



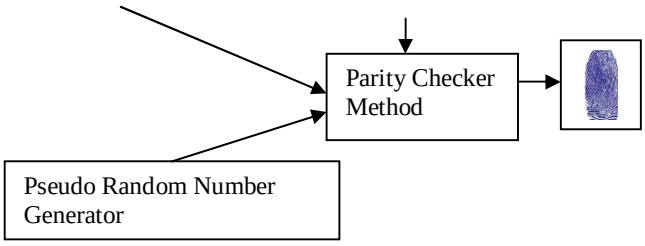


Fig 2. Watermarking approach

C. Intelligent Approach

An Intelligent agent is a computer system situated in some environment, and that is capable of independent action in this environment in order to meet its design objectives. Agent properties are 1.Autonomy 2.Socialability, 3.Proactivity, 4.Reactivity, 5.Adaptability, 6.Intelligence, 7.Reasoning, 8.Ability to plan, 9.Learning and adaptation. There are different types of agents 1.Simple reflex agents acts on the basis of the current perception. It does not consider percept history i.e. it does not act on past history. It is based on the condition-action rule: if condition then action. 2. Model based reflex agent, can handle a partially observable environment. It [3] maintains an internal model. The precepts history are stored inside the internal model by using this model agent reflects some unobserved aspects of the current state, 3.Goal based agent is based on the capabilities of the model-based agents, by using "goal" information. Goal information describes situations that are desirable. From this goal information, the agent chooses the situation that can be reached definitely. Searching and planning are the subfields of artificial intelligence devoted to find action sequences that achieve the agent's goals, 4.Utility based agent has to model and keep track of its environment, tasks involved in utility based agent are perception, representation, reasoning, and learning, 5.Multi agent system is a computerized system consists of multiple interacting intelligent agent within an environment. The problems that cannot be solved by a single agent are solved by multi agent system. Cooperation between multiple agents helps to solve the complex problems that cannot be solved by individual agent in a group. Cooperation, Coordination and Negotiation are the main properties of multiagent system.

Intelligent agent [4] plays a vital role in providing security to Biometric template. Knowledge of a human expert is encoded as a set of rules. These rules are used by the agent to analyse the security related events taking place in the system. Set of facts are collected that describe a certain situation in the audit records. These facts are compared with predefined rules. If the rules i.e. if the conditions match a notification are given to the system administrator. As a result user is terminated from the current activity. If the activity is normal then normal operation is carried out.

III. Comparative Study of Different Template Protection Approach

TABLE I
COMPARISION OF DIFFERENT TEMPLATE PROTECTION SCHEMES

Approaches	Methods	Advantages	Disadvantages
Biometric cryptosystem	Key binding, Key generating, Fuzzy commitment, Fuzzy vault methods used	1.Tolerant to intrauser variation. 2.Useful in cryptographic application	1.Generation of key with high stability and entropy is difficult. 2.Diversity and revocability is not ensured.
Watermarking approach	Invisible Watermarking, Parity checker method is used	1.Ensures high security to the Biometric template	1.Time complexity in inserting watermark pattern
Intelligent approach	Rule based method, Expert system based method	1.Robust 2.Capable of Autonomous action.	1.Requries more expert knowledge in defining the rules

Table 1 explains the methods of different template protection schemes, its advantages and disadvantages.

IV. Conclusion

Based on the study of various Biometric template protection techniques intelligent approach is robust when compared to other two techniques. In Biometric cryptosystem diversity and revocability is not ensured. Although watermarking approach is robust it is time consuming while inserting watermark image. In Intelligent approach, it is capable of autonomous action if anything went wrong in security related events in the system. Incident response is there while using intelligent approach. It also requires expert Knowledge while defining the rules.

References

[1] Anil K.Jain, Karthick Nandakumar and Abhisek nagar“BiometricTemplateSecurity",Journal on Advances in Signal processing, special issue on biometrics, January 2008.

[2] Andrew B.J.Teoh,Yip Wai Kuan,Sangyoun Lee,”CancellableBiometricsand Annotations on Biohash”,Pattern Recognition 41,2008.

[3] Maithili Arjunwadkar,R.V.Kulkarni,”The rule based intrusion detection and prevention model for Biometric system", Journal of Emerging Trends in computing and Information Science 2010.

[4] Shweta Malhotra,Dr.Chander Kant,"A Novel Approach for securing Biometric Template",Internal Journal of Advanced Research in Computer Science and Software Engineering May 2013.

[5] Maithili Arjunwadkar,R.V.Kulkarni,”Intelligent Intrusion Detection Tool For Biometric Template storage", Journal of Artificial Intelligence2012.