Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

Fingerprint Protection Techniques in A Biometric Recognition System

Manish Kumar
THDC Institute of Hydro. Eng. & Tech.
Tehri, India

***Abstract*- Biometric recognition system is a way of built the identity of individual on his/her behavioral traits like finger print, face, palm print, iris, retina. Biometric system provides the e-Authentication mechanism that electronically verifies the identity of individual. Biometric system gives guarantee that the biometric identity of individual which is unique. The objective of this paper is to study biometric security system and then consider the various technique of secure to biometric template in a biometric system database. There are various types of security attack which may encounter the biometric database and compromise the biometric security in biometric system. We are going to study the various types of biometric protection technique and their strength and weakness. Security is important issue in biometric template database because if compare the password or PIN or tokens, the biometric fingerprint cannot be produce same biometric traits of individual again. We are presenting an analysis of different biometric template protection technique with their advantage and drawback.**

Index Term- Feature transform technique, Salting, noninvertible function, Biometric Cryptosystem, key binding technique, key generation technique

I. INTRODUCTION

Biometric recognition system is widely integrating information system and provides e-Authentication mechanism that guarantees that the biometric trait of individual is unique. Unlike passwords and access PINs which are easily forgotten, stolen and easily guessed at in traditional authentication systems, biometrics are reliable, secure, efficient and a quick means of validating users if proper procedures and measures of using them are put into consideration [1]. Biometric system may be vulnerable to adversarial attack which is encounter by the opponent. Current authentication systems based on physiological and behavioral characteristics of person known is biometrics, such as fingerprints, inherently provides solutions to many of these problems and may replace the authentication component of the traditional [2]. We are analyzing existing biometric template protection techniques. In this paper we summarize the various aspects of template protection approaches that is to be proposed in the literature. A reliable identity management system is urgently needed in order to combat the epidemic growth in identity theft and to meet the increased security requirements in a variety of applications ranging from international border cross in to security information in databases [3]. The identities like password, PIN or ID cards are not reliable identity because these identities may be misplaced or stolen by someone. Biometric recognition system establishes the identity of an individual using his / her behavioral traits. The use of biometric traits for security and secure applications including personal identification, access control, forensics applications, e-commerce, e-government and e-health is receiving an increasing attention [4].

II. BIOMETRIC PROTECTION TECHNIQUE

There are different types of vulnerabilities in a biometric recognition system by the leakage of biometric template which leads to break the security system. A widespread approach to biometric authentication is to confine the biometric templates of all users during the enrollment phase and to store [5]. There are various available template protection techniques but these techniques somehow failing to fulfill property of an ideal biometric template protection scheme. There are two challenges in biometric recognition system: first is we have to need to select suitable representation where we can capture most of discriminatory feature that can be secured using available template protection technique and second challenge is we need to register biometric fingerprint during enrollment and matching without using any information could be reveal. A biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process [6]. The purpose of template protection of prevent these types of attack. An ideal biometric template protection scheme should follow these properties:

a) Diversity: In this property the secure biometric template should not match across databases so

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

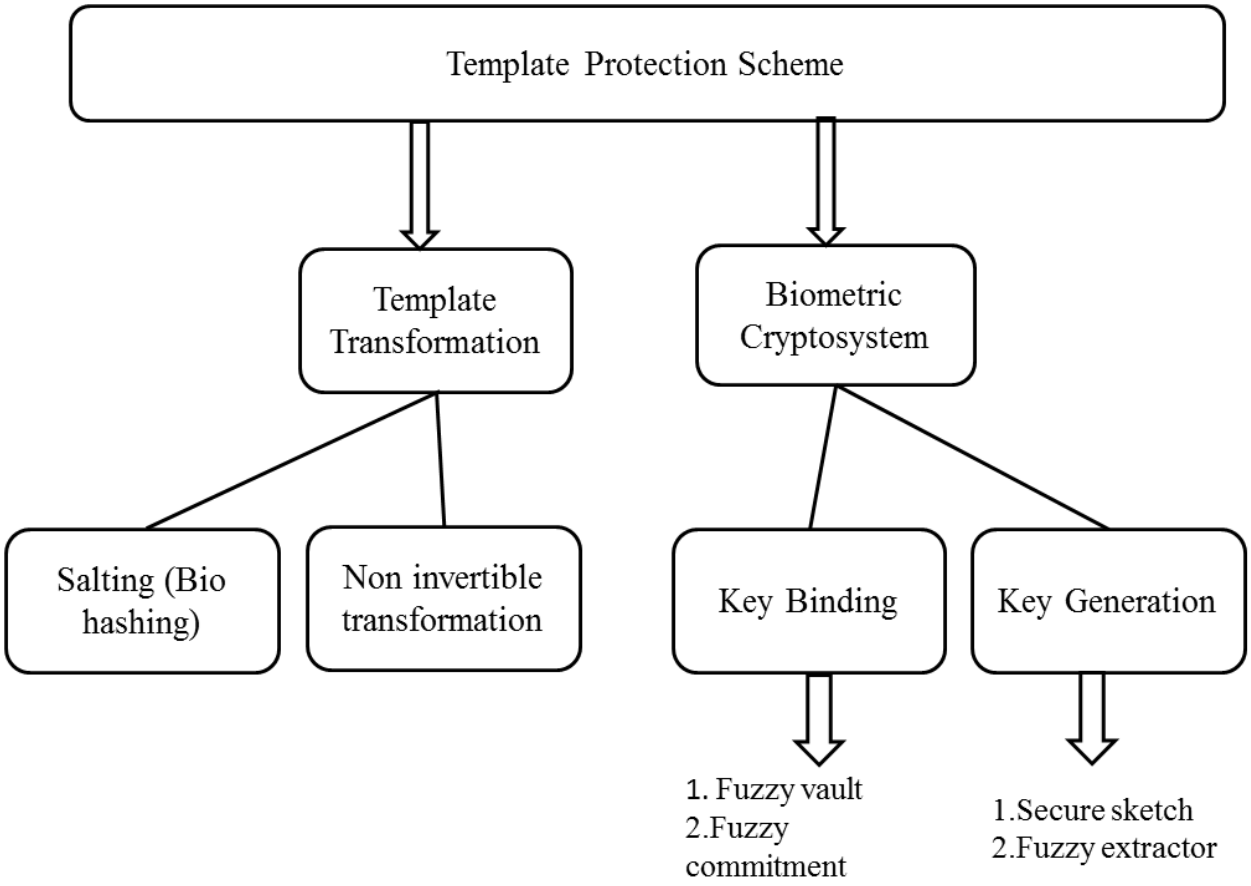

Figure 1: Biometric protection scheme

that the privacy of biometric template will be secure.

b) Revocability: In this property to revoke a compromised biometric template and reissue a new biometric template should by the same biometric data.

c) Security: The security of the biometric system should computationally hard to encrypt the original biometric template from the secure biometric template.

d) Performance: performance of biometric template protection technic should not abase the recognition performance of the biometric system.

In the literature survey template protection technique can be categorized into two categories: Feature transformation technique and biometric cryptosystem. (see Figure 1).

1. Feature Transformation Technique

In feature transform approach we use a transformation function which is applied on the biometric template and then this transformed template will be stored in the database. The parameter of feature transformation should be a random key or password. On the other side at the time of query the same transformation function is applied and it should be match against the transformed template. Feature transform schemes can be categorized in to two more technique is salting and noninvertible transforms. In feature transform technique we apply the transform function (F) with finger print (T) at the time of enrollment. Then the biometric template will be stored in the database

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

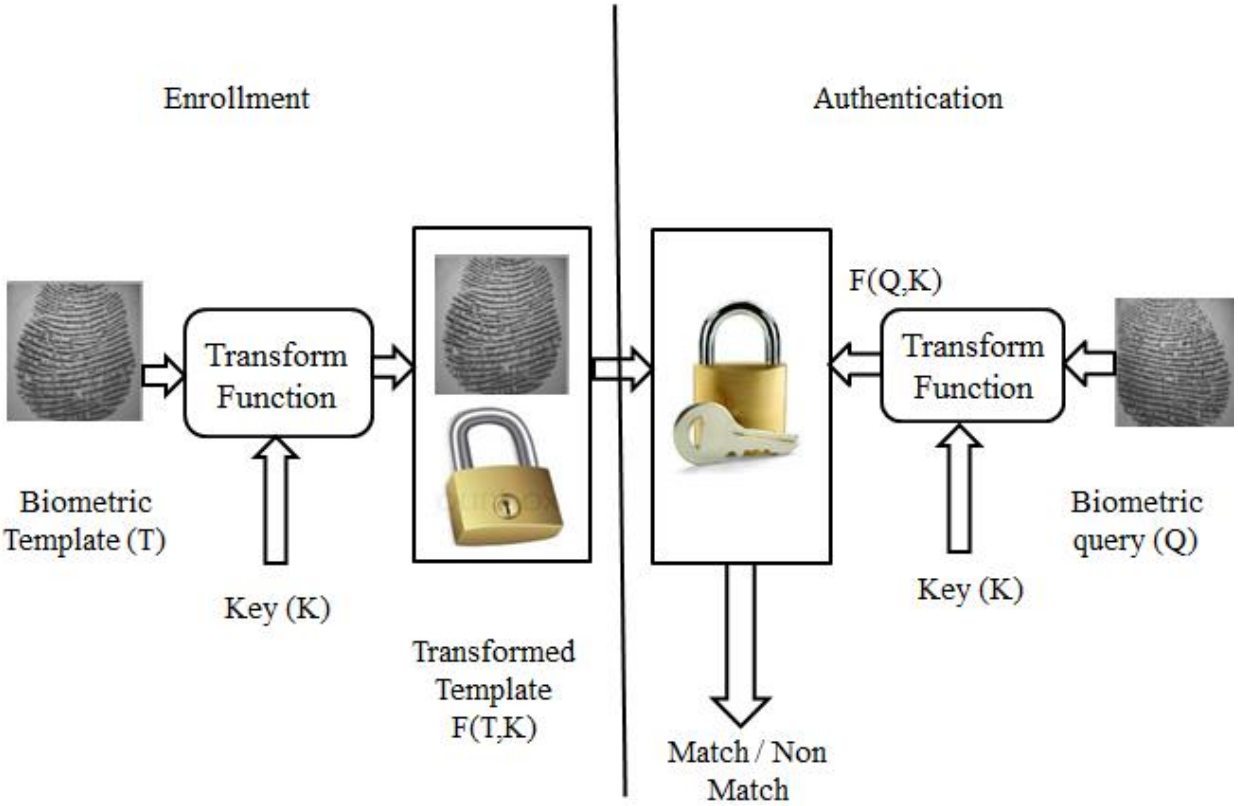

Figure 2: Enrollment and Authentication using transform function

combine form of transform function and Biometric Template, F:(T,K). at the time of authentication we apply the same transform function with the biometric query (Q). If the transformed query F:(Q,K) will be will be apply to the transformed template F:(T,K) for direct matching. Transform function use the user specific key and then modify the template. Template transformation technique can be further divide into two more category first is salting and second is non-invertible function.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

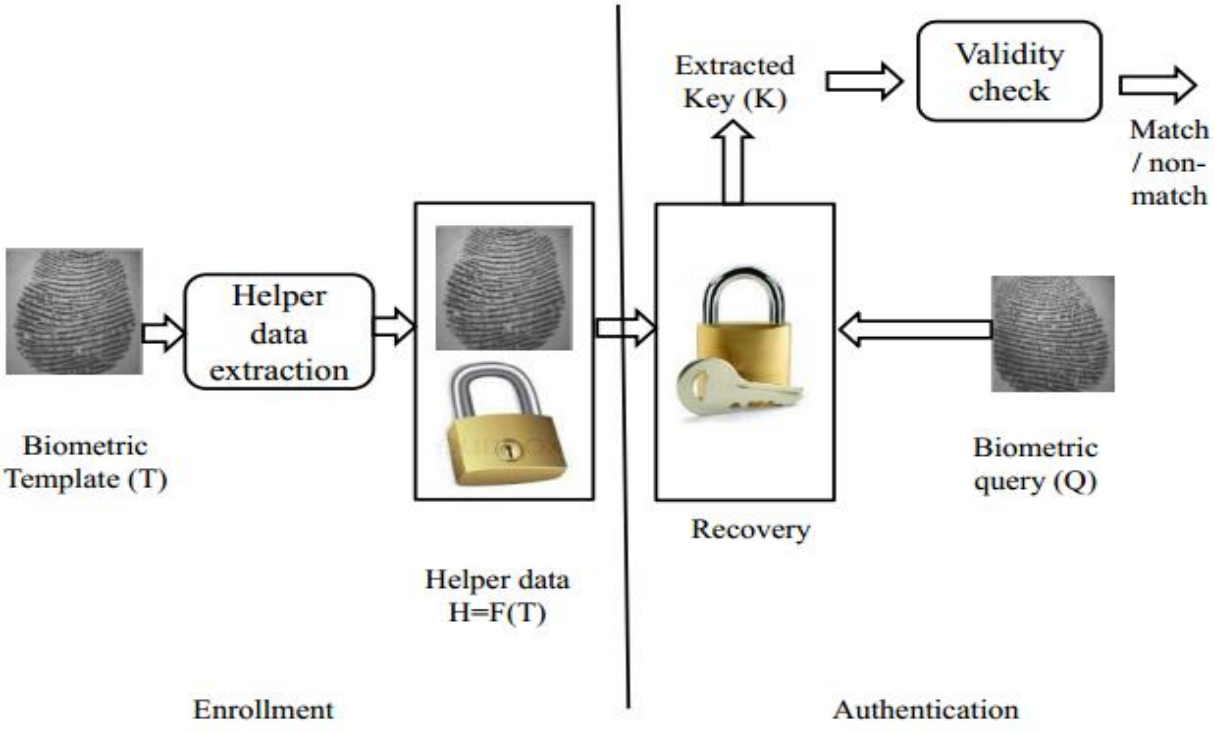

Figure 3: Biometric cryptosystem using the helper data

2. *Biometric Cryptosystem*

Helper data does not reveal any important information about the original biometric template. In authentication we extract the cryptographic key from the query features for matching. In biometric cryptosystem the error correction code is used for verify the validity of extracted key.(see Figure 3.) sketch is the combine form of the biometric template and error correcting code word. In this technique the error correcting code word is defined by a key itself. Biometric cryptosystem is useful for using the sketch so that we can secure the key and also secure the biometric template. Biometric cryptosystem can be further categorize into two more technique first is key binding cryptosystem and key generating cryptosystem.

III. RELATED WORK

Teoh at al, [7] described an approach for salting thais is Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. In this technique the author introduced the biometric-hash framework using biometric vectors and token which derived random sequences. Author analyze the different biometric hashing framework using random multispace quantization (RMQ) operation. Author find the discriminative feature analyze by the Fisher Discrimination Analysis (FDA) [8] and project the obtained vectors on a randomly selected set of orthogonal directions. Random projection is used by the salting mechanism. After obtained the feature vector random projection is binarized. Security is concerned by the user specific random projection matrix, if third party access the projection matrix they can access some information Biometric cryptosystem is the method for secure the biometric key from biometric feature or generate a because some information may be lost during the binarization[9].

Andrew B. J. Teoh[10] et al. define the biometric hash framework where the biometric data is derived from a secret password or physical token, the technique is called random multispace quantization process. The Random Multispace Q uantization is completed in three steps: first is feature extraction transformed the biometric data using the Fisher Discrimination Analysis. The biometric feature further mapped onto a random subspaces in the form of vector. Each vector is quantized into a binary outcome. The idea is that single random subspace is extended into a multi space in the form of Random Mix vector. Multi Space Quantization uses the secret password or serial number as the cryptographic key. In this method biometric hash framework describes the integration of biometric and secret password is used. The attacker is difficult to capture the biometric data because quantization output is independent in terms of input and quantization output are maximum unpredictable.

Ratha et al. [11] define Cancelable Templates for fingerprints, in this technique one –way transformation is used for securing the biometric data, instead of storing the original biometric authentication. There are three transformation functions are used. The work of transformation function is transform the minutiae so that we get transformed minutiae. The first transformation function is Cartesian transformation. In Cartesian transformation the fingerprint minutiae is move to fit into a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

rectangular grid, where each cell of rectangular grid take a new position. The second transformation technique is polar transformation, in polar transformation the fingerprint minutiae is move to fit into rectangular grid and rectangular grid in the form of shell and shell is divided into sectors. Size of sectors may be different. The third transformation function is functional transformation, in functional transformation translate the biometric minutiae uses the 2 D Gaussians and electric potential field for transformation.

Abhishek Nagar et al.[12] proposed a method to measure of non-invertibility which is called Coverage-Effort (CE) curve. This method measures the number of attempt that is used by attacker for recover the original biometric data. The computation of CE curve by the three steps: first is pre-image computation which compute the pre-images of each transformed minutiae. Second step is Minutiae Likelihood Computation whish estimate the relative probability of each minutiae and third step is Non-invertibility measure computation which sort the pre-images according to their likelihoods and compute the converage.

Chulhan Lee et al.[13] proposed a new method for cancelable fingerprint template which need not alignment. Alignment free cancelable fingerprint templates generated by some steps: preprocessing, minutiae extraction, calculation of invariant value, changing function, minutiae movement and generation of a cancelable template, matching transformed templates.

Bian Yang et al. [14] proposed a minutiae based template protection algorithm which is suitable for fingerprint minutiae templates called key controlled non-invertible transformation. In this technique uses linear and non-linear geometrical transformations which map original minutiae based template to a protected coordinate based template. the technique prevent coordinate and more suitable than fuzzy vault and enhance the security against template linking, inversion, correlation and conjugation.

CONCLUSION

Biometric authentication is more important and more secure authentication now a days. In this paper we have presented a research focus on biometric security using Template transformation technique and Biometric Cryptosystem against various security attacks. Salting (Biohashing) and non invertible transformation technique cover under template transform and key binding and key generation cover under the Biometric Cryptosystem. Some method have discussed in literature which protect the biometric templates. The more focus on non invertible transformation technique that is one way function means it is easy to compute but hard to invert. The best way is to securing template from unauthorized party is non invertible transform technique because if an attacker gain access to the key and transformed template, they can not recover the original biometric template.

REFERENCES

[1] Joseph Mwema, Michael Kimwele, Stephen Kimain, “A Simple Review of Biometric Template Protection Preventing Adversary Attacks on Biometric Fingerprint Templates”, International Journal of Computer Trends and Technology (IJCTT), Volume 1- Feb 2015, pp 12-18, ISSN : 2231-2803.

[2] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, 2004, “Biometric cryptosystems: Issues and challenges”, In Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92: pp.948–960.

[3] Anil K. Jain, Karthik Nanda kumar and Abhishek Nagar: “Biometric Template Security” EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008.

[4] Vincenzo Piuri, Fabio Scotti, “Biometric privacy : Technologies and applicatons”, 2011, Proceedings of the International Conference on Optical Communication Systems (OPTICS), pp 7-7, 2011.

[5] N. Radha, S. Karthikeyan,“A study on Biometric Template Security” ICTACT Journal on Soft Computing, July 2010, Issue-01, pp 37-41.

[6] Anit K. Jain, Arun Ross, Umut Uludag, “Biometric Template Security : Challenges and Solutions”, Biometric template security: challenges and solutions” in Proceedings of the European Signal Processing Conference (EUSIPCO’ 05), Antalya ,Turkey, September 2005.

[7] Andrew B. J. Teoh, Alwyn Goh, David C. L. Ngo, ”Random Multispace Quantization as an Analytic Mechnism for BioHashin of Biometric and Random Identy Inputs”, IEEE Transactions on Pattern Analysis and Machine INtellignence, vol. 28, no. 12, ppp1892-1901, 2006.

[8] Chong Siew Chin, Andrew Teoh Beng Jin, David Ngo Chek Ling, “High Security Iris verification system based on random secret integration”, Computer Vision and Image Understanding, vol. 102, no. 2, pp. 169-177, 2006.

[9] Tee Connie, Andrew Teoh, Mechael Goh, David Ngo, “PalmHashing : a novel approach for cancelable biometrics”, Information Processing Letters, vol. 93, no.1, pp. 1-5, 2005.

[10] Andrew B. J. Teoh, Alwy Goh and David D. L. Ngo, “Multispace Quantization as an Analytic Mechanism for Biohashing of Biometric and Random identity inputs”, IEEE transaction on pattern analysis and machine intelligence, VOL.28, NO. 12, DECEMBER 2006.

[11] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, Ruud M. Bolle, “Generating Cancelable Fingerprint Templates”, IEEE Transaction on Pattern analysis and Machine Intelligence, VOL. 29, NO. 4, APRIL 2007.

[12] Abhishek Nagar, Anil K. Jain, “On the security of non-invertible fingerprint template transforms”, First Inernational workshop on Information Forensics and Security, dec, 2009, ISSN: 2157-4766.

[13] Chulhan Lee, Jeng- Yoon Choi, Kar-Ann Toh, Sangyoun Lee, “Alignment-Free Cancelable Fingerprint Templates based on Local Minutiae Information”, IEEE Transaction on Systems, MAN AND CYBERNETICS- Part B: CYBERNETICS, VOL. 37, NO. 4, AUGUST 2007.

[14] Bian Yang, Christoph Busch, Patrick Bours, Davrondzhon Gafurov,”Non-invertible Geometrical Transformation for Fingerprint Minutiae Template Protection, Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN), may, 2009, ISBN: 978-1-61284-168-7.