IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

A Comparative Study on Various Techniques Related to Fingerprint Based Biometric Cryptosystems

Mutya Sirisha Adapa[1] and Venkateswararao Pallipamu[2]
Research Scholar, Department of Computer Science and Engineering[1]
Associate Professor, Department of Computer Science and Engineering[2]
Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh, India

Abstract: *In this digital era, data transmission through network is essential for everyone. Users are not confident that their data is secure when it is transferred through a network. So there is a need of protecting data transferring through network in a swollen manner. Cryptography is our conventional method for protecting information and communications using some keys. But keys can be stolen or forgotten. Due to these reasons biometrics are introduced for key generation. Keys generated using biometrics are specific to that person and are generated dynamically with their biometrics. By combining cryptography with biometrics, we can develop a secure system which can be used in different applications like law enforcement, border control, consumer biometrics, financial services and also to provide access for smart devices. In this comparative study of various attacks on Biometric Cryptosystems are discussed and related techniques used in Biometric Cryptosystems for key generation like Fuzzy Extractor and key binding techniques such as Fuzzy Vault, Fuzzy Commitment are discussed and their performance is analysed.*

Keywords: Cryptography, Biometrics, Fuzzy Extractor, Fuzzy Vault, Fuzzy Commitment.

I. INTRODUCTION

Biometrics is a scientific measure of an individual's physical as well as biological characteristics. These characteristics are used for authentication of a user or to identify a person to access smart devices and for better security. Conventional methods used for authentication such as PIN and passwords are nowadays replaced by Biometrics [1]. In conventional cryptographic methods, user authentication is performed by entering secret keys referred as passwords, where these keys are kept secret. But user faces problems in maintaining these keys as they can forget or keys can be stolen. Usage of biometrics came into existence as they are hard to forge. These biometrics are about 18 different models through which we can perform user authentication. Such models are Fingerprint, Face, Facial Thermos gram, Iris, Hand geometry, Hand Vine, Voice, Palm, Gait, Signature, Keystroke, DNA, Ear, Odour, Retina etc. When compared to the existing biometric traits fingerprint based biometric recognition systems are most flexible to use, adopt and most widely deployed model. In some biometrics like face, iris and voice, there will be periodic changes with respect to time. But in case of fingerprints there will be no change and are unique from person to person they are also easy to store, access, maintain and they retain forever. [3] As Humans have 10 fingerprints that is we can have choice of more than five times the amount of other biometrics, like iris or facial recognition. Even identical twins will have different fingerprints. Due to these benefits, more study is carried out on fingerprint identification and researchers focus on developing biometric authentication systems in place of traditional authentication systems. Biometric authentication systems are answering many questions that are raised in traditional authentication systems, such as password theft and forgetting of passwords. When fingerprints are used as a biometric trait then cryptographic key will be generated using the template stored in our database and this key cannot be revealed without a successful authentication of a biometric user. [4]

II. COMPARISON OF VARIOUS BIOMETRIC TRAITS

Biometrics are used in various applications for developing secure systems. Different characteristics of biometrics are being used depending upon the application and every biometric trait has its advantages and disadvantages. We cannot judge that a single biometric is sufficient for every application. Umutuldag and Sharath Pankanti [5][6] proposed some four properties to compare among different biometrics and three attributes of biometric systems to identify the suitable biometric trait for an application. Biometrics are used in various applications for developing secure systems. Different characteristics of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

biometrics are being used depending upon the application and every biometric trait has its advantages and disadvantages. We cannot judge that a single biometric is sufficient for every application. Umutuldag and Sharath Pankanti [5] [6] proposed some four properties to compare among different biometrics and three attributes of biometric systems to identify the suitable biometric trait for an application.

Table 1: Comparison of Various Biometric Traits with Different Properties of a Biometric System

Biometric	Absoluteness	Incomparable	Uniqueness	Immutable
Fingerprint	Me	Me	Hi	Hi
Face	Hi	Hi	Lo	Me
Iris	Hi	Me	Hi	Hi
Hand geometry	Me	Hi	Me	Me
Voice	Me	Me	Lo	Lo
Signature	Lo	Hi	Lo	Lo
Keystroke	Lo	Me	Lo	Lo
DNA	Hi	Lo	Hi	Hi
Ear	Me	Me	Me	Hi
Gait	Me	Hi	Lo	Lo
odour	Hi	Lo	Hi	Hi
Palm print	Me	Me	Hi	Hi
Retina	Hi	Lo	Hi	Me

Absoluteness: The quality of identifying and capturing without any restriction.
Uniqueness: Does all the people have this type of biometric trait.
Immutable: Unable to change or it is unchangeable over time.

Table 2: Comparison of various biometric traits with different attributes of a biometric system

Biometric	Performance	Suitability	Avoidance
Fingerprint	Hi	Me	Me
Face	Lo	Hi	Hi
Iris	Hi	Lo	Lo
Hand geometry	Me	Me	Me
Voice	Lo	Hi	Hi
Signature	Lo	Hi	Hi
Keystroke	Lo	Me	Me
DNA	Hi	Lo	Lo
Ear	Me	Hi	Me
Gait	Lo	Hi	Me
odour	Lo	Me	Lo
Palm print	Hi	Me	Me
Retina	Hi	Lo	Lo

Here performance refers to speed and accuracy of the system, suitability is the willingness of people to use the system and avoidance is the action of overcoming from a problem and Hi, Me and Lo refers to high, medium and low respectively. [5] [6]

2.1 Attacks on Biometric Authentication System

Nowadays biometrics are used to provide security to many applications, and they cannot be attacked. The attacker can get hold of the template stored in the database and launch various kinds of attacks to the biometric system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

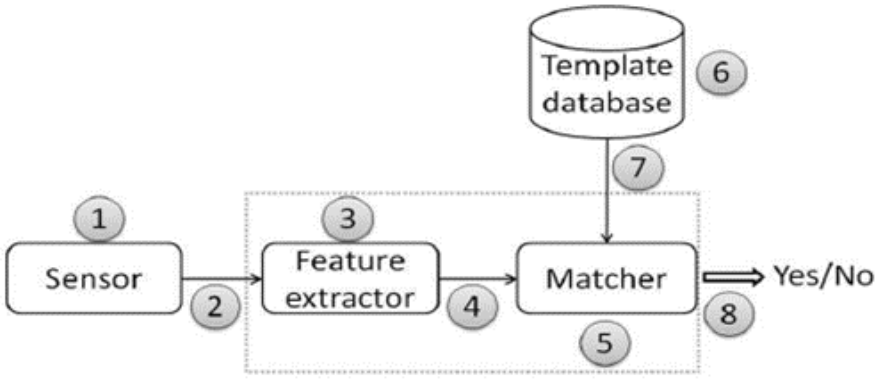

Figure 1: Points of attacks in generic Biometric System

In Fig 1, 8 possible attacks on a Biometric Authentication System are shown. 1 Attacks at the sensor are typically performed by a spoof biometric trait either by presenting fake biometric data or physically destroying the sensor device and making it out of service. 2. Intercepting a biometric sign and replay it into the system 3 & 5 there is a possibility of injecting Trojan Horse programs 4. Continuously injecting samples in order deny genuine users to access the system 6. Attacker can illegally obtain original biometric templates or they can modify 7. Altering the information to communication channel or even cut the communication channel and can make the system unavailable 8. Alter the transported matching information in order to allow an imposter access. [7] In addition, the extraction of characteristics in stored module and system database can be attacked either obtain the generated biometric template, modify it or introduce a new model preselected by the intruder. Other security vulnerabilities are linked to interfaces between modules, which could be intercepted to damage biometrics information transmitted through them. Finally, the comparator score and the final system decision can be changed at convenience of the attacker. [8]

Some of the possible attacks on biometrics are:

1. Spoofing: This attack occurs in input phase, by inputting a fake biometric data to sensor. Fooling the biometric device by inputting fake biometric as Spoofing.
2. Replay Attack: In this method attacker interrupts the biometric signal and replay it into the system. In some case a previously recorded image will be applied into the system instead of giving an original one.
3. Denial of Service Attack: Modifies the channel information in order to deny an authentic user to authenticate.
4. Hill-Climbing Attack: This method modifies the query image conveniently until it gets the desired corresponding score.
5. Trojan Horse Attacks: Injects Trojan horse programs either in feature extraction module or in matcher module. If the matcher is attacked by a Trojan horse, all given inputs will result in a high verification score.
6. Masquerade Attack: An artifact image is taken from the fingerprint template. So every time a person applies their fingerprint, the system will produce a match.
7. Tampering: An attacker will modify the model to obtain a high verification score during the match process. Thus, the system will be matched with all input data.
8. Substitution Attack: The attacker can change the user's model to match their own finger.
9. Overriding YES/NO response: System output is always a binary YES / NO (Match / No match) response.

III. Biometric Cryptosystems

Cryptography and biometrics are combined to obtain a secure sketch known as helper data. This helper data does not reveal any significant information about the biometric data. During authentication, using the query biometric features a cryptographic key is generated and the comparison is performed indirectly by checking the validity of the extracted key. If the genuine user's biometric data is not known, it must be computationally difficult to get the key from the helper data. However, if a query sufficiently close to the enrolled reference is presented, it must be easy to decode the helper data and recover the key. Typically, the intra-class variability is handled using error correction coding techniques.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

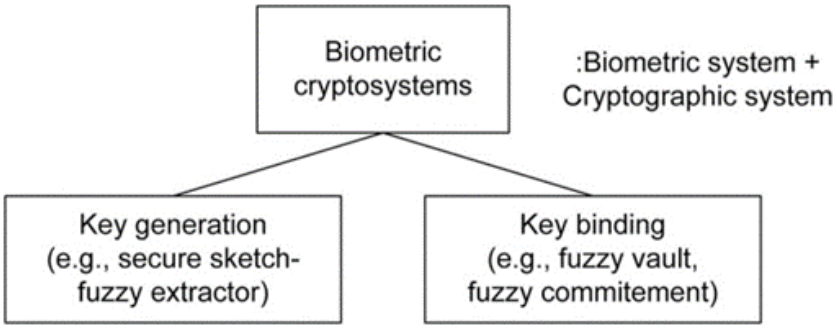

Figure 2: Categories of Biometric Cryptosystem

The Biometric cryptosystem approach is also divided into two categories: Key Generation and Key Binding. In the case of the Key Generation cryptosystems, the helper data is obtained from the biometric sample. In the key generation cryptosystems, the secret key will be generated by a special algorithm for given biometrically extracted points.[2]A successful implementation of this approach has been more difficult to achieve in practice. Secure sketch and fuzzy extractor concepts [8] are included in this category. In the key binding cryptosystems, the biometric data and the cryptographic keys are combined. Therefore, the key will not be generated unless the same person is involved in the system. Fuzzy vault and Fuzzy commitment are popular biometric key binding systems.

3.1 Key Generation Systems

A. Secure Sketch

Secure sketches are the key components in building fuzzy extractors. It is a one round information reconciliation protocol produces a string that does not decrease the entropy of v too much, and still allowing the recovery of v from a close v1. It allows to retrieve the actual value v from any neighbouring value v1. A random extractor is then executed on v to produce uniform bits but a computer extractor only helps if the minimum conditional entropy of v conditioned on the sketch is high enough. Most of the natural relaxation on minimum entropy requirement of the secure sketch is to require the entropy HILL. According to this definition, one could use a random extractor to obtain r from v, resulting in a pseudo-random key.[10]

B. Fuzzy Extractors

Fuzzy extractors develop trustworthy keys from noisy sources. It consists of two algorithms: Generate (used only once) and Reproduce (used successively). The Generate (Gen) algorithm accepts an input i and produces a key k and a public value p. The Reproduce (Rep) algorithm is able to reproduce r given p and some value i0 that is close to i (from Hamming distance). Significantly for security, knowledge of p should not reveal r that is, r should be uniformly distributed conditioned on p. This feature is needed because p is not secret.

Example: In a single-user location (where the user wants to reproduce the key k from a subsequent reading i0), it would be stored in the clear and in a key agreement application (where two parties have i and i0, respectively), the natural solution is to send p between the parties. More techniques are possible when interactive communication is permitted. Fuzzy extractors use ideas from information-reconciliation and privacy amplification and are defined as information-theoretic objects. Privacy extension is usually performed with a randomness extractor. Randomness extractors are well-understood. Polynomial-time reconstructions of randomness extractors can extract randomness from all distributions with min-entropy with the help a short uniform non secret seed. A single randomness extractor simultaneously works for all probability distributions with sufficient entropy. Furthermore, for randomness extractors, the parameter gap between negative results, nonconstructive positive results, and polynomial-time constructions is relatively small. Unfortunately, the state of fuzzy extractors is darker. There is no hard characterization of when key derivation is possible. Fuller, Reyzin, and Smith [11][12]present one possible notion called fuzzy min-entropy. They show a non-polynomial-time algorithm that derives a key from each distribution with fuzzy min-entropy. Wood age et al. [14] subsequently improved the parameters. As a negative result, Fuller, Ryzen, and Smith [10][11] and Fuller and Peng [13] show families of distributions where no fuzzy extractor can simultaneously work for the whole family, despite the fact that a fuzzy extractor exists for each element of the family. Thus, two main open areas of research for information theoretic fuzzy extractors are providing polynomial-time

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

constructions and providing constructions that simultaneously secure many distributions. A Fuzzy extractor can be formed from a secure sketch and a medium case random extractor. A medium case extractor is a generalization of a strong random extractor showed that all strong extractors are average-case extractors with a slight loss of parameters. [10]

3.2 Key Binding Systems

In a Key Binding cryptosystem, the helper data is obtained by binding the extracted biometric data with the key. This category includes the Fuzzy Vault [15] and Fuzzy Commitment [16] schemes.

A. Fuzzy Vault Scheme

There are several methods for protecting biometric templates in which Fuzzy Vault scheme is most popular, which is a key-binding biometric cryptosystems. In FV scheme an unordered set of points (set of biometric characteristics) is used to encrypt / decrypt a cryptographic key, thus obtaining an indecipherable safe. This scheme in addition to ensuring the key also guarantees the protection of the unordered set. The FV scheme works to secure a biometric vector, = $\{a1, a2, an\}$, a user-specific cryptographic key, of length M bits, is generated. Redundancy (which is generated by applying an error correcting code to) is added to, obtaining a coded key Kc of length N bits ($N>M$). Then Kc is used to represent the coefficients of a polynomial P of degree L ($L<n$). The A elements are projected into the polynomial P to obtain a set of real points $G = \{(ai, P(ai))\}$ $i = 1$ n. In order to hide the authentic stitches, glitter stitches which do not rest on P or do not cut the whole A, are added. Finally, a vault assembly is formed by the union of the assembly and the points of sequins. During authentication, a biometric request vector is presented to decode the safe and obtain. If the vector B substantially overlaps A, then B is able to identify many authentic points from the FV. On condition that the difference between the sets A and is small enough for the redundancy present in Kc to correct the points identified by mistake, the polynomial P will be successfully reconstructed and therefore the associated key is obtained. To successfully reconstruct the polynomial, at least $(L + 1)$ authentic points must be identified from the arch. The FV scheme has the advantage of offering high security [4]. More precisely, this property is determined by the number of glitter points included in the trunk, because by increasing the glitter points, the security of the system increases. Usually, the amount of glitter dots is an order of magnitude greater than the actual dots [17]. Another important advantage of this scheme is its ability to manage the intra-class variability of biometric data through error correction codes.

On the other hand, the FV scheme does not meet the revocability requirement. Since, from two different vaults of a same biometric trait, the genuine points can be easily identified (common points between the vaults) and then achieve decoded the vault. Hence, this scheme does not provide protection against cross-matching with different biometric databases. To solve this problem, in [18] the implementation of a hybrid approach is proposed, where first a salting scheme transforms the biometric feature vector and then the vault is constructed using the transformed vector. While the salting approach provides revocability, the FV scheme offers high security.[19]

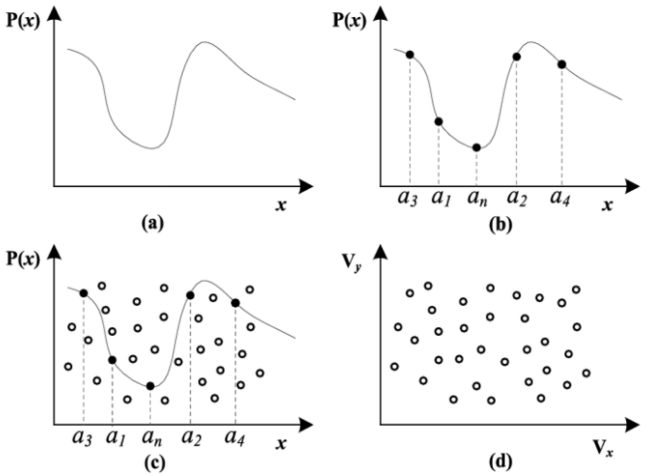

Fig. 3. Vault coding: (a) Construction of a polynomial using Kc as coefficients. (b) Polynomial projection for the A elements. (c) Randomly generation of chaff points. (d) Obtaining the final vault.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

B. Fuzzy Commitment Scheme

Fuzzy commitment scheme is biometric cryptosystem belongs to the key-binding approach in [18]. It combines the properties of Error Correcting Codes (ECC) and cryptography. Error Correcting Codes plays a vital role in the fuzzy commitment scheme. ECC used to check and correct the corrupted messages. In fuzzy commitment scheme, a biometric data is treated as a corrupted code word. This method consists of two phases Enrolment phase and Authentication phase During enrolment phase, user registration is done by accepting a biometric template BT, a key K(say as a code word) is chosen randomly. During enrolment phase Now the biometric template BT and key K are given as inputs for Helper Data Extraction module which computes the helper data HD of biometric template BT and key Resulting HD=F(BT,K). Now in the authentication phase a biometric query B and the helper data HD are taken as inputs for the Recover module to generate the key K'. If the difference between B and BT is smaller than the error correction capability of the ECC employed in this fuzzy commitment scheme, the Recover module can recover exactly the same key. The extracted key K ,is then checked with the enrolment key K to check the validity for match or no match of the biometric

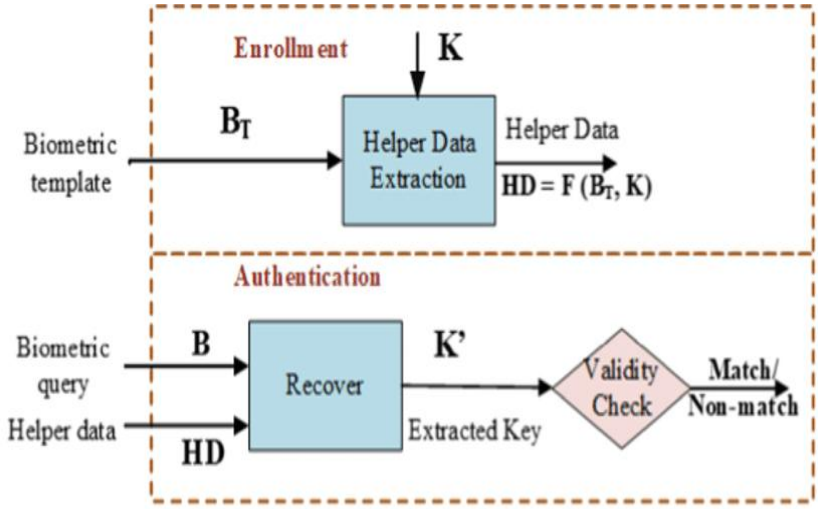

Figure 4: Fuzzy Commitment Scheme

A Biometric Cryptosystem can generate a key either by linking it with biometric characteristics, such as fuzzy commitment(FC) [16] and fuzzy vault (FV) [17,15], or generate the key directly from the biometric characteristics by the fuzzy extractor (FE) [9].

IV. Related Work on Biometric Cryptosystems

Teoh and Kim [20] have chosen the fuzzy engagement scheme for protecting fingerprint characteristics. As biometric characteristics can be converted into binary format, these characteristics are referred with a dynamic random quantization transformation. However, in most cases the minutiae of the fingerprints and the set extracted from the minutiae are a set of points and are not ordered. To safeguard these minutiae set of points, Uludag et al. [18] proposed a new method to protect critical data along with fingerprint using the novel fuzzy vault concept. They identified that, when a 128-bit AES keys are combined with fingerprint minutiae data a secure key is generated. But this approach suffers from high time complexity. Later, Nanda Kumar et al. [21] implemented a fully automatic and practical fuzzy vault system based on fingerprint minutiae for securing 128-bit AES encryption keys. In this method for image alignment helper data is used and achieved the highest genuine accept rate and a very low false accept rate. They also suggested that the performance of this fuzzy vault can be increased by using multiple biometric sources such as multiple fingers or multiple modalities (e.g., fingerprint, face and iris).Li and Wang[22] proposed an alignment-free fingerprint cryptosystem based on fuzzy vault using the local features which are not sensitive to transform. In this author considered two features like minutia descriptor and local structure. Which are merged with three different rules to encode and decode an alignment free fingerprint fuzzy vault. Fuzzy engagement and fuzzy vault schemes are key binding schemes whereas fuzzy extractors are key generation schemes and is introduced in [9][10].Artiest al. [23] proposed an authentication scheme, Fuzzy Extractor using fingerprint biometrics. They applied a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

construct called PinSketch which is used for digitally representing and quantizing the minutiae measurements. They have succeeded by achieving the authentication accuracy is within the acceptable range. Kai Xi et al. [24] proposed an alignment free fingerprint fuzzy extractor scheme. In this alignment process is eliminated using the minutia local structure features which are stable, discriminative, rotation and shift free. Here a new fuzzy extractor scheme based on nearly equivalent version of Dual Layer Structure Check is directly employed and a high verification accuracy is achieved when applied on database FVC2002.Later, many fuzzy extraction systems [25,26] have been proposed with improved performance. Liu and Zhao [27] proposed a method for securing fingerprint templates using l1 minimization which can generate a cipher text. Digital printing, matching is done in the encrypted domain, authentication is checked for accuracy among the model fingerprint and the request fingerprint. As the model is generated from the Minutia Cylinder-Code (MCC) [28] which is an appropriate and secure algorithm, and can achieve high security and recognition accuracy .Alam, B and Jin, Z.[29] proposed a voidable non-alignment pattern scheme to protect fingerprint minutiae. The proposed model scheme is the extended version of the polar grid-based 3-tuple quantization with a condensed feature length for a lower computational cost. To improve non-inevitability, a bit flipping strategy is proposed to inject noise into the proposed fingerprint model. Reza Mehmood and Arvind Selwal[30] presented a modified version of the fuzzy vault which increase the level of security of the model and the secret key. The polynomial whose coefficients represent the key is transformed using an integral operator for hiding the key where the key can no longer be derived if the polynomial is known to the attacker. The proposed fuzzy vault scheme also prevents the system from a stolen key reversal attack.

V. Performance Metrics of Biometric Cryptosystems

Even though biometric technology having its own benefits and is being used in many applications, this system is facing some challenges like insufficient accuracy under non-ideal conditions. As traditional password based authenticated systems check for 100% match where as in biometric cryptosystems 100% matching cannot be achieved. Here the accuracy is assessed using performance indicators for biometric cryptosystems like False Acceptance Rate(FAR) , False Rejection Rate(FRR) , Equal Error Rate(EER) and Genuine Acceptance Rate (GAR) .The accuracy of recognition usually depends on factors such as the quality of the input image and matching algorithms.[7][31]

False acceptance rate (FAR) is used to find the accuracy of a biometric system. Here the real users are identified and accepted whereas imposters are rejected. By this measure wrongly accepted impostors can be determined by the biometric system .[30]

False Acceptance Rate(FAR)is defined as the ratio between the total number of accepted imposter users and the total number of imposter users present.

Mathematically it is denoted as:

$$FAR = \frac{\text{Total number of accepted imposter users}}{\text{Total number of imposter users present}}$$

False Reject Rate (FRR) of a system is measured as the total number of genuine users that are falsely rejected by the biometric system.

Mathematically it is denoted as :

$$FRR = \frac{\text{Number of rejected genuine users}}{\text{Total number users}}$$

Genuine Acceptance Rate (GAR) is defined as the total number of genuine users accepted by the system [30] It is the total number of attempts in which a genuine user is properly accepted by the biometric system and categorized into a true class.

Mathematically it is denoted as:

$$GAR = (1 - FRR)$$

Equal Error Rate (EER): EER represents a point in the graph where False Acceptance Rate(FAR) becomes equal to False Rejection Rate(FRR). [31]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

Table 3: A Comparison of all the Techniques used in Biometric Cryptosystems are Tabulated

Year of Publication	Author	Technique	Best Performance	Databases
2005	Uludag, U.; Jain, A.K. [17]	Fuzzy vault with fingerprint minutiae data	FAR = 0	IBM-GTDB
2007	Arakala,A.; Jeffers,J.; Horadam K. [23]	Fuzzy Extractor	EER ≈ 10%	FVC2000
2007	Teoh and Kim [20]	Fuzzy commitment	FAR = 0, FRR = 0.9%	FVC2002 DB1
2007	Nandakumar etal.[21]	Fuzzy vault scheme	FAR= 0, FRR= 10%	FVC2002 DB2
2010	Li,P.;Yang,X.;Cao,K.;Tao,X.; Wang,R.;Tian,J [22]	Fuzzy vault scheme	FAR= 0.35, FRR = 17.5% FAR= 0, FRR = 10%	FVC2002 DB1, DB2
2011	Xi, K.; Hu, J.; Han, F. [24]	Dual Layer Structure Check (DLSC)	EER = 4.5%	FVC2002 DB2
2012	Yang etal. [26]	Fuzzy extractor	EER = 13%	FVC2002 DB2
2013	Karthi and Azhilarasan [25]	Feature Transformation Method	FAR=1% FRR = 1%	FVC2004
2013	Yang etal. [32]	A Minutiae basedFuzzy Vault scheme	FAR = 0.38%, FRR = 19% FAR = 2.25%, FRR = 8%	FVC2002DB1, DB2
2017	Liu and Zhao [27]	MCC matching scheme	FAR = 0, FRR = 8.6% FAR = 0, FRR = 34.4%	FVC2002 DB1, DB2 FVC2004 DB2
2018	Alam etal. [29]	Bit-toggling strategy	FAR = 0, FRR = 16% EER = 1%, EER = 2.07% EER = 6.11% EER =15.44% EER = 9.15% EER = 9.28%	FVC2002 DB1, DB2,DB3 FVC2004 DB1, DB2, DB3
2019	Raul Sanchez-Wendy, [8]	FV scheme using CRC FV scheme separating the error correcting and interpolation	FRR =21% FAR = 0%	100 users with 2 fingerprint images each.
2020	Mehmood and Selwal [30]	Fuzzy vault scheme	GAR= 92%,90%, 85%	FVC2002DB1,DB2,DB3,DB4

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

VI. CONCLUSION

Biometrics presents many advantages over password and token-based security. This survey study focussed on various issues related to biometric systems. The security and privacy concerns that biometric authentication raises are addressed. A comparison of all the techniques used in biometric crypto systems is done. Performances of different Techniques like Secure sketch, Fuzzy Commitment, Fuzzy Vault are tabulated and analysed as per their performance. In biometric cryptosystems performance metrics are False Acceptance Rate(FAR) , False Rejection Rate(FRR), Equal Error Rate(EER) and Genuine Acceptance Rate (GAR).It is observed that False Acceptance Rate(FAR) is almost zero in all the methods i.e. all techniques are succeeded in opposing the imposters, but False Rejection Rate(FRR) is varying means that for some extent genuine users are been rejected. The objective of this survey is fulfilled by analysing all the techniques used in biometric cryptosystems which are secure, user friendly and economic.

REFERENCES

[1]. Jain, A.K.; Flynn, P.; Ross, "A Handbook of Biometrics"; Springer: New York, NY, USA,2007.
[2]. Jisha Nair.B.J., Ranjith Kumari.S "A Review on Biometric Cryptosystems", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 6 Issue 1 September 2015, ISSN: 2278-621X
[3]. Ranjith JAYAPAL ,Pramod Govindan "Biometric Encryption System For Increased Security"- Electrical Engineering, University Of North Florida, Jacksonville, Florida, USA ,IEEE-2018
[4]. Targoviste, RomaniaI "Enhancing Security by Combining Biometrics And Cryptography"–International Conference 9th Edition Electronics, Computers And Artificial Intelligence 29 June - 01 July, 2017, EEE-2017
[5]. J. L.Wayman, "Fundamentals of biometric authentication technologies," Int. J. Image Graph., vol. 1, no. 1, pp. 93–113, 2001.
[6]. Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil k. Jain, "Biometric Cryptosystems: Issues and Challenges", proceedings of the IEEE, vol. 92, no. 6, June 2004
[7]. Wencheng Yang , Song Wang , Jiankun Hu , Guanglou Zheng and Craig Valli "Security and Accuracy of Fingerprint-Based Biometrics: A Review" published in Symmetry 2019
[8]. Hernandez, Gonzalo and Raul Sanchez, " Template protection approaches: Fuzzy Vault scheme" ,978-1-7281-1576-4/19©2019 European Union
[9]. Dodis, Y.; Reyzin, L.; Smith, "A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data" In Proceedings of the Advances in Cryptology Euro crypt 2004.
[10]. Benjamin Fuller ,Xianrui Meng, Leonid Reyzin, "Computational Fuzzy Extractors "June 23, 2020,at MIT Lincoln Laboratory and Boston University.
[11]. Benjamin Fuller, Leonid Reyzin, and Adam Smith." When are fuzzy extractors possible? In Advances in Cryptology "– ASIACRYPT, pages 277–306. Springer, 2016.
[12]. Benjamin Fuller, Leonid Reyzin, and Adam Smith. "When are fuzzy extractors possible?" IEEE Transactions on Information Theory, 2020.
[13]. Benjamin Fuller and Lowen Peng. "Continuous-source fuzzy extractors: Source uncertainty and insecurity", In 2019 IEEE International Symposium on Information Theory (ISIT), pages 2952–2956. IEEE, 2019
[14]. Joanne Woodage, Rahul Chatterjee, YevgeniyDodis, Ari Juels, and Thomas Ristenpart. "A new distribution-sensitive secure sketch and popularity-proportional hashing", In Advances in Cryptology–CRYPTO, pages 682–710. Springer, 2017.
[15]. Juels, A.; Sudan, M. "A fuzzy vault scheme" Des. Codes Cryptogr. 2006
[16]. Juels, A.; Wattenberg, M. "A fuzzy commitment scheme". In Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1999
[17]. Uludag, U.; Jain, A.K. "Fuzzy fingerprint vault" In Proceedings of the Workshop Proceedings—Biometrics: Challenges Arising from Theory to Practice, Cambridge, UK
[18]. Uludag, U.; Pankanti, S.; Jain, A.K " Fuzzy vault for fingerprints", In Proceedings of the 5th International Conference on Audio and Video based Biometric Person Authentication ,HiltonRye Town,NY, USA, 2005

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

[19]. Oyetola Oluwadamilola K., Osifeko Martins O." An Improved Authentication System Using Hybrid of Biometrics and Cryptography", 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)

[20]. Teoh,A.B.J.;Kim,J "Secure Biometric Template Protection Fuzzy Commitment scheme" IEICE Electron. Exp.2007.

[21]. Nandakumar, K.; Jain, A.K.; Pankanti, S. "Fingerprint-based fuzzy vault implementation and performance", IEEE Trans. Inf. Forensics Security. 2007

[22]. Li,P.;Yang,X.;Cao,K.;Tao,X.;Wang,R.;Tian,J." An alignment free fingerprint Cryptosystem based on fuzzy vault scheme" J. Netw. Comput. Appl. 2010

[23]. Arakala, A.; Jeffers, J.; Horadam, K." Fuzzy extractors for minutiae-based fingerprint authentication" In Proceedings of the 2007International Conference on Advances in Biometrics, Seoul, Korea

[24]. Xi, K.; Hu, J.; Han, F. "An alignment free fingerprint fuzzy extractor using near-equivalent Dual Layer Structure Check(NeDLSC)algorithm". In Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), Beijing, China.

[25]. Karthi, G.; Azhilarasan, M. "Hybrid multimodal template protection technique using fuzzy extractor and random projection". IJRCCT 2013.

[26]. Yang, W.; Hu, J.; Wang, S. A Delaunay "Triangle-Based Fuzzy Extractor for Fingerprint Authentication" In Proceedings of the 2012 IEEE 11thInternational Conference on Trust ,Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012.

[27]. Liu, E.; Zhao, Q. "Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with I1minimization". Neuro computing 2017.

[28]. Cappelli,R.;Ferrara,M.;Maltoni ,D. "Minuti a cylinder-code: A new presentation and matching technique for fingerprint recognition", IEEE Trans. Pattern Anal. Mach. Intell. 2010.

[29]. Alam, B.; Jin, Z.; Yap, W.-S.; Goi, B.-M. "An alignment-free cancellable fingerprint template for bio-cryptosystems", J. Network Computer, Appl. 2018.

[30]. Reza Mehmood and Arvind Selwal "Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics", The International Arab Journal of Information Technology, Vol. 17, No. 6, November 2020

[31]. Sheikh Imroza Manzoor, Arvind Selwal "Biometric Feature Template Security Schemes: An Overview" International Journal of Computer Sciences and Engineering, Vol-6, Special Issue-5, Jun 2018 E-ISSN: 2347-2693

[32]. Yang, W.; Hu, J.; Wang, S. A Delaunay "Triangle group based fuzzy vault with cancellability", In Proceedings of the 2013 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16–18 December 2013.