iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Recent Advancement in Biometric Fingerprint Template Security

Deepika Kansal[1], Akhilesh Verma[2]
[1]*M.tech, Computer Science and Engineering Ajay Kumar Garg Engineering College, Ghaziabad, India*
[2]*Asst. Professor, Department of Computer Science, and Engineering Ajay Kumar Garg Engineering College, Ghaziabad, India*

Abstract: ***One of the most important issues in a biometric system is the leakage of biometric template information. In this paper, we have discussed on biometric template security. Most of the template protection techniques fail to meet all the desired requirements of a biometric system like revocability, security, privacy, and accuracy, so protecting a fingerprint template is a big issue. In this paper, we begin by introducing about biometric after which we will describe attacks on a biometric system which targeting the biometric templates in a biometric system. Thereafter we will explore the existing biometric template protection scheme and techniques and include their strength and weaknesses. In the end, we will discuss the summary of this paper in the conclusion section.***

Keywords—Biometric, fingerprint, template, security, protection, techniques, approaches.

I. INTRODUCTION

Biometrics refers to the physiological or behavioral characteristics of an individual. In biometrics many physical and behavioral characteristics such as the face, iris, fingerprints, hand geometry, palm print, gait, voice and keystrokes dynamics. In a traditional authentication system, passwords and access PINs are easily forgotten, stolen and easily guessed so in comparison to traditional system biometric systems are reliable, popular, and efficient and provide a more secure identification and authentication. A biometric recognition has two operations namely, the enrollment stage and the recognition stage. In the enrollment stage, the biometric system acquires the biometric trait of a person and extracts some feature set from it and stores the extracted feature set into a database as a template. In the recognition stage, the system again acquires the biometric trait of a person also extract feature set and compare this feature set against the templates to determine an identity of a person or verifying it [2] [3]. Biometric security is to provide a high-security level for verification and identification so the popularity of a biometric system is increasing and the template protection becomes more important. Most biometric systems use a centralized database to store the extracted biometric template. In the biometric system some template protection approaches can be classified into two classes called (1) transformation approach and (2) biometric cryptosystems. Transformation approaches use a user-specific password to transform the biometric features. There are a number of transformation based schemes have been proposed called, an optimal transformation that preserves the matching accuracy at the same time and it is non-invertible. Biometric cryptosystems associate a key which is external to a user to obtain the helper data. The helper data never reveal any information about the template [5]. A biometric system has some components which are classified into 5 categories called: Sensor, Feature extractor, the Template database, Matcher module and a Decision module [3].

II. BIOMETRIC SYSTEMS ATTACKS & THREATS

A. Biometric System Threats and Attacks

To understand some attacks which are targeted at biometric systems, we familiarizing ourselves with various biometric system attacks identified in existing literature. Figure 1. shows a graphical representation of these attacks into the biometric system. These biometric attacks are categorized as follows:

B. Attack on the Scanner

This attack also is known as “Type 1 attack”, in this recognition scanner can physically destroy by the attacker and cause a denial of service. A fake biometric fingerprint trait can also create by the attacker such as an artificial finger to bypass fingerprint recognition systems, or inject a fingerprint image between the sensing element and the rest of the scanner module to bypass fingerprint recognition systems.

C. Attack on the channel between the scanner and the feature extractor

This is the "Type 2 attack" and also called the "Replay attack". When a biometric trait acquires by the fingerprint scanner module into a biometric system then, the scanner module sends the biometric trait to the feature extractor module for the processing. On that point, the hacker can appropriate the fingerprint and replace with the individual.

D. Attack on the feature extractor module

This is the "Type 3 attack". In this attack, the feature extractor module replaces by the attacker in a Trojan horse like a worm or virus. In this attack, Trojan horse could be used for gathering (harvesting) user's fingerprints extracted features and send this for the attacker.

E. Attack on the channel between the feature extractor and matcher

This is called the "Type 4 attack". There is the difference in this attack is that the attacker appropriates the communication channel between feature extractor and matcher to steal feature values of an admissible user and replay it to matcher at an end time.

F. Attack on the matcher

This attack is known as "Type 5 attack". In this attack Trojan horse replaces with a matcher by the attacker. Commands can send from the attacker to the Trojan horse to produce scores of high matching and send a "Yes" to bypass the biometric authentication mechanism to an application.

G. Attack on the system database

This attack is called as "Type 6 attack". In this attack, the attacker compromises the security of database where all the fingerprint templates are stored. Database compromising can be done by initiative openness in the database software or burst an account on the database. In any way, new fingerprint templates can add by the attacker also can modify existing templates or delete the templates.

H. Attack on the channel between the system database and matcher

This attack is known as "Type 7 attack". In this attack, the attacker appropriates the communication channel between database and matcher to steal and replay data each of two or adjust the data. At this point, this attack is known as"Type 7 attack".

I. Attack on the channel between the matcher and the application

This attack is known as "Type 8 attack". In this attack, the attacker appropriates the communication channel between the matcher and the application to recount already acquiesce data or adjust the data.

III. BIOMETRIC FINGERPRINT TEMPLATE SECURITY

In this classification, we analyze the susceptibility arrange by the biometric template attacks. After that, we criticized the type 6 attack which is the attack on biometric templates in the database.

A. Biometric Template Compulsions

After study attacks on biometrics systems, we needed to understand what the sensitivities biometric templates were disclosed to due to these attacks. We confirmed that attacks on biometric templates can lead to the following compulsions;

1) Biometric keys easily being guessed and the biometric template can be easily replaced by an unauthorized person.
2) The biometric template is not secure, templates of fingerprints can be extracted easily by using special reactant while voice and face templates can be taped or captured and caught.
3) Biometric template extracted from rough images are personally stored in a database so, rough images can be easily recaptured by using some restrict facility.
4) Cross-matching can be conducted by colluding and sharing among various applications [15].

There are the 2 main failure modes of a biometric template can be divided into 2 classes called: [1] intrinsic failure [2] failure due to an adversary attack. Intrinsic failures occur due to inherent limitations in the sensing, feature extraction, or matching technologies. In adversary attacks, a resourceful hacker attempts to circumvent the biometric system for personal gains.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

B. Biometric Template Attack in the Database

We realized from the study of biometric system threats and attacks that "Type 6 attack" is where the attacker attacks on the biometric template in the database. As seen in this type of attack, the programmer can add new templates, modify actual templates or rub templates.

One of the most harmful attacks on a biometric template system happens when it is across the biometric templates. We saw that how attacks on the templates can lead to heavy compulsions where a template can be recovered by an attacker's templates to acquire illegal admittance to a

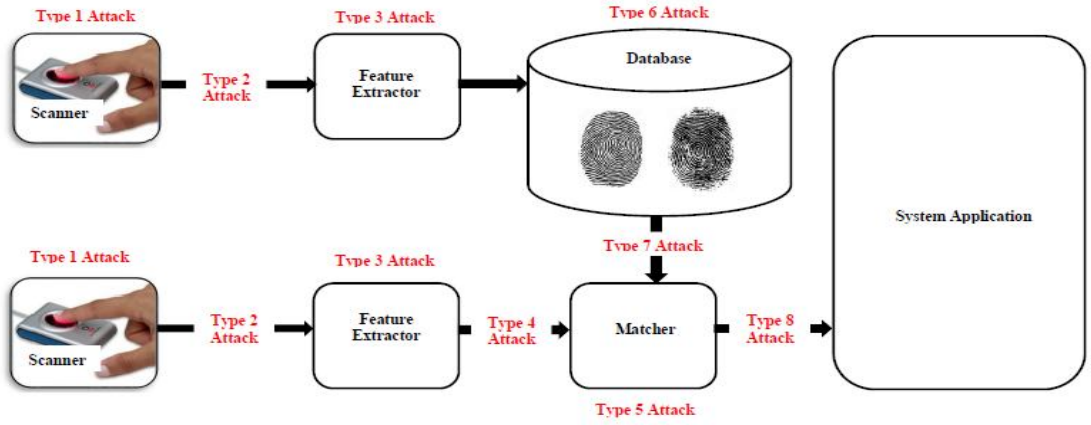


Fig.1 Graphical Representation of possible Biometric System Attacks

system. We more alert against biometric templates being saved in plaintext style and contend that blockhead proof techniques are necessary for securing memory of biometric templates to safe zone both safety of the biometric system and that of the users [3].

Attacks on the template can lead to the following three vulnerabilities. (i) A template can be replaced by an fraud template to gain unauthorized access. (ii) A physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait). (iii) To gain unauthorized access, the stolen template can be replayed to the matcher. The most straightforward way to secure the biometric system, including the template, is to put all the system modules and the interfaces between them on a smart card (or more generally a secure processor). In such systems, known as match-on-card or system-on-card technology, sensor, a feature extractor, matcher, and template reside on the card. The advantage of this technology is that the biometric information never leaves the card. However, system-on-card solutions are not appropriate for most large-scale applications; they are expensive and users must carry the card with them all the time.

Having already known the types of biometric system thrust that exist and seeing that most of the major thrust is addressed at biometric templates, we go ahead survey the biometric template protection techniques used to protected biometric systems across these attacks.

IV. BIOMETRIC TEMPLATE PROTECTION TECHNIQUES

Biometric Template Protection patterns are classified into Feature Transformation and Biometric Encryption. Jain et al in (Jain, Nandakumar, & Nagar, 2008) classified the various biometric template protection techniques as (i) Feature Transformation and (ii) Biometric Encryption. This has been the groundwork on which biometric template approaches have been restricted. We examine and review the actual biometric template approaches in article established on these categories. Fig 2 below shows a visual image of biometric template protection techniques which we have discussed in this chunk.

A. Feature Transformation

In this further approach, a transformation function (F) is applied to the biometric template (T) while the database stores only the transformed template (F(T; K)). Usually, the parameters of the transformation function derive from a random key (K) or the

password. Another way to classify these schemes is by categorizing them in invertible and non-invertible transforms. In the case of invertible transforms, an adversary has access to the key and to the transformed template, this way being able to recover the original biometric template (or a close approximation of it), having in mind that security of the invertible scheme is based on the secrecy of the key or password. Yet, the non-invertible transformation schemes are more effective, considering that they apply a one-way function on the template, making so more difficult computationally to invert a transformed template, although the key may be known [1] [8].

B. Cancellable Biometrics

In order to prevent the theft of biometric templates, it is aspired to modify them over revocable (unstable) and non-invertible transformations to produce Cancelable biometric templates. Cancellable biometrics is truly defined for biometric template protection. The schemes modify according to the distinct biometric procedure but we calmly focus on minutia adapted fingerprint templates. A common method for minutia protection is by mapping two or more minutia to the pattern function. Therefore, it is tough to arbitrate the original location to which a minutia be part of.

In repeated distortion of biometric signals or features on the noninvertible transforms, cancelable biometrics involves. This approach reduces the compromise of the stored templates using the substitution of a transformed version of an image instead of the original. It is very useful when a person is contributed to various applications. These kinds of approaches are used for the authentication and identification purposes [7]. Cancelable biometrics refers to an intentional and systematically repeatable transformation of biometric data for the purpose of protecting sensitive user-specific features. The principal objectives of cancellable biometrics templates are Diversity, Cancelability, Reusability, Non-invariability, and Performance. Cancelable biometrics provides a perfect secrecy [4] [10].

C. Bio-hashing

Bio Hashing methods are basically an extension of random projection. In BioHashing wavelet transform called a feature extraction method is first used in the input biometric data to extract the biometric feature. Using a user-specific tokenized random number (TRN), n orthogonal pseudo-random vectors, are generated. The dot product of the feature vector and all the random vectors is then calculated [2]. Finally, a binary discretization is applied to compute the n-bit BioHash template.

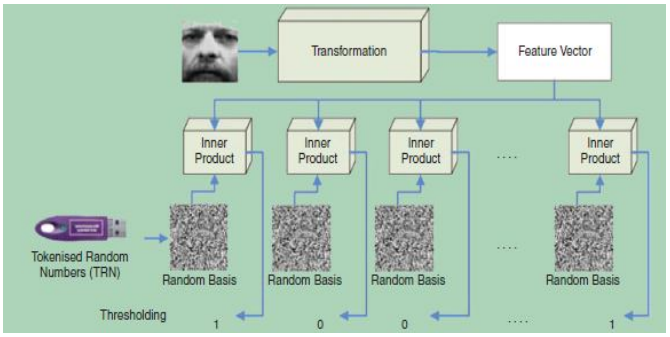


Fig.2 An overview of BioHashing

In contrast to Cancellable biometrics, the key or password used in bio-hashing increases the entropy of biometric template which further deters adversary attacks. Direct mixing of a pseudo-random number (which is kept secret) and biometric data is used to compute a binarized key of 80-bits key with a 0.93% false rejection rate of the system. The major drawback of bio-hashing is its reduced performance when a legitimate token is retrieved and presented by an adversary purporting to be a legitimate user.

D. Biometric Cryptosystems

Biometric cryptosystems protect a cryptographic key using the biometric or we can also say that, generate a cryptographic key from the biometric by using some secure sketch techniques or fuzzy vault. In traditional system identity authentication is based on simple passwords which have always been easy to break so to overcome these drawbacks, cryptographic secret keys and passwords have been proposed. Biometric cryptosystems subdivided into Key Generation and Key Binding [4][11].

1) Key Generation: While exploring biometric cryptosystem we discovered from the literature that in Key Generation a biometric key is derived directly from the biometric data. In the key generation scheme, helper data are derived only from the biometric template. From a given biometric sample and the helper data, the keys are directly generated. This technique also applied to face biometrics called "BioHashing". However, to generate biometric hashes secret user-specific tokens have to be presented at authentication, basically, the BioHashing approach operates as the key-binding scheme. BioHashing can be seen as an instance of "Biometric Salting" [4].

2) Secure Sketches and Fuzzy Extractors: A significant which is allowed for correcting of error codes in biometric data and generating linear encryption keys for use in encryption and decryption in the biometric cryptosystems, Dodis et al's scheme of using secure sketches and fuzzy extractors. In their later published research work they alleged that they were formally defining secure and efficient techniques for;

3) *Fuzzy Extractor:* To apply cryptographic techniques for biometric template security, fuzzy extractors convert biometric data into strings. They are used to encrypt and authenticate user's records, with biometric inputs as a key. Historically, the first biometric system of this kind was first designed by Jules and Wattenberg and was called 'Fuzzy commitment', where the cryptographic key is committed using biometric data. "Fuzzy", in that context, implies that the value close to the original one can extract the committed value [20]. Later, Jules and Sudan came up with Fuzzy vault schemes which are order invariant for the fuzzy commitment scheme but uses a Reed–Solomon code. The codeword is evaluated by polynomial and the secret message is inserted as the coefficients of the polynomial. A set of features of the biometric data, the polynomial is evaluated for different values [21]. So Fuzzy commitment and Fuzzy Vault were per-cursor to Fuzzy extractors. The fuzzy extractor is a biometric tool to authenticate a user using its own biometric template as a key. Fuzzy extractor reliably extracts the randomness R from its input. Fuzzy extraction is error tolerant in the sense that R will be never change. R can be used in a cryptographic application as a key.

4) *Secure Sketch:* Secure sketches produced the public information about its input w that did not reveal w and allowed the exact recovery of w and given another value that is very close to w. This was an advantage to reproduce error-prone biometric inputs that made it possible for it to be reliably used.

E. Fuzzy Commitment

Fuzzy Commitment is originally designed to protect a cryptographic key and it is later being perceived as a technique for biometric template protection. Fuzzy commitment is meant to accept input in a binary string. It has been pointed out that fuzzy commitment is information theoretical secure only if the bits extracted from biometric features are uniformly and independently distributed. To secure biometric traits represented in binary vector, fuzzy commitment is used [6]. A fuzzy Commitment scheme is a smart biometric cryptosystem framework which can deal with hamming errors happening between different biometric samples. A fuzzy commitment scheme is a biometric- key binding scheme, to modify biometric intra-user variations, which relies on error correction code (ECC) completely. In the fuzzy commitment, the larger key size or higher security always trade with poor key release success rate due to the security-performance tradeoff [10]. So it is highly susceptible to a number of security and privacy attacks.

The main difference between fuzzy vault and fuzzy commitment is that biometric traits in fuzzy vault are represented in the form of point set which is secured by hiding them with chaff points while the biometric traits secured by fuzzy commitment are represented in the form of binary vectors which are divided into a number of segments and each segment is separately secured.

One limitation of a fuzzy commitment scheme designed using typical algebraic codes is that these codes do not meet the Hamming bound. These codes may produce a decoding failure when one attempts to use a non-matching descriptor to release the key.

F. Advantages of Biometric Keys

Some of the advantages of using biometric keys as compared to traditional biometric passwords are as follows;

traditional biometric system, passwords can be easily forgotten and misplaced while biometric keys cannot be misplaced or forgotten.

Biometric keys are difficult to copy and distribute them while traditional passwords can be easily copied and distribute also.

Biometric keys are not easy to guess, unlike passwords.

G. Other Biometric Template Protection Schemes

Some other biometric template protection schemes are as follows:

1) *Watermarking:* Use biometric fingerprint templates as a message is the main aim of watermarking scheme. Watermarking is used for the copyright protection in order to enable biometric recognition after the extraction of the watermark. A watermarking technique is used for fingerprint images using the Discrete Wavelet Transform Singular Value Decomposition (DWT-SVD). Generate a combined minutiae template containing minutiae features of each of the two Fingerprints captured in enrolment phase and stored in a database. For matching the two query fingerprints against the enrolled template, a two-stage fingerprint matching process is proposed in the authentication process. Reconstruct a fingerprint look like an image from combined minutiae template. Watermark Embedding Technique or the algorithm should be imperceptible i.e. embedding watermark should not affect the quality of original image. MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio) is calculated between the original image and the corresponding watermarked image to calculate the superiority of a watermark embedded images. The watermark should be robustly embedded into an image which remains in fact after any type of image processing. The added watermark images information should not be removed beyond reliable detection i.e. watermarking technique should be as secure as possible. It should consume less time for watermarking [10].

Bhatnagar and Raman 2009 performed work; "A new robust reference watermarking scheme based on DWT-SVD" This paper represent the novel semi-blind watermarking technique based on SVD (singular value decomposition) and DWT (discrete wavelet transform) for validity and security. They used a gray level emblem picture as watermark instead of arbitrarily generated Gaussian noise kind watermark.

Ramakrishnan 2011 performed work; represent the projected of watermark embedding technique using a mixed image which satisfies together imperceptibility and toughness necessities. They used SVD of vertical and diagonal details of Wavelet Transformation to insert watermark image.

Rajani and Ramashri 2013 performed work; represent to develop a mixture of SVD (Singular Value Decomposition) and DCT (Discrete Cosine Transform) frequency by hybrid watermarking algorithm domains and Canny Edge detector. A Non-blind watermarking technique is the projected technique. By means of Singular Value Decomposition (SVD), the toughness of the technique can be improved. By incorporating edge detector imperceptibility of the watermark image can be improved.

H. Rivest, Shamir and Adleman (RSA) Technique

RSA (Ron Rivest, Adi Shamir, and Len Adleman) is one of the most popular algorithms used in asymmetric key cryptography.RSA is a widely used Public-Key cryptographic algorithm. According to this, the Public key is known to everyone whereas the Private-key is known only to the user who originally owns the data. RSA involves the three steps are called: Key generation, Encryption, and Decryption. RSA involves a public key and a private key. The public key is used for encrypting messages and can be known to everyone. Messages encrypted with the public key can only be decrypted by using the private key.

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. Along with an auxiliary value, as their public key a user of RSA creates and then publishes the product of two large prime numbers [18]. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

I. Elliptic Crypto Curve (ECC) Technique

Elliptic curves provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real-time performance is a critical factor. So we use ECC for key generation. The use of ECC is very inviting for various reasons. The first and probably most important reason is that comparison to any other public-key cryptography, ECC offers better security with a shorter key length

J. RSA and ECC Algorithms Comparison

When ECC is compared with RSA, the key size is too smaller than RSA. It provides relatively small block size, high speed, and high security. For example, the level of security achieved with ECC using a 160-bit key is equivalent to conventional public key cryptography (e.g. RSA) using a 1024-bit key. There is huge importance of shorter key lengths especially in applications having limited memory resources because shorter key length requires fewer memories for key storage purpose. Elliptic curve cryptosystems also require less hardware resources than conventional public-key cryptography. Now at the security level, ECC is more secure than

RSA. RSA can be cracked successfully, uses 512 bits and for ECC the number of bits is 97, respectively [19]. It has been analyzed that the computation power required for cracking ECC is approximately twice the power required for cracking RSA.

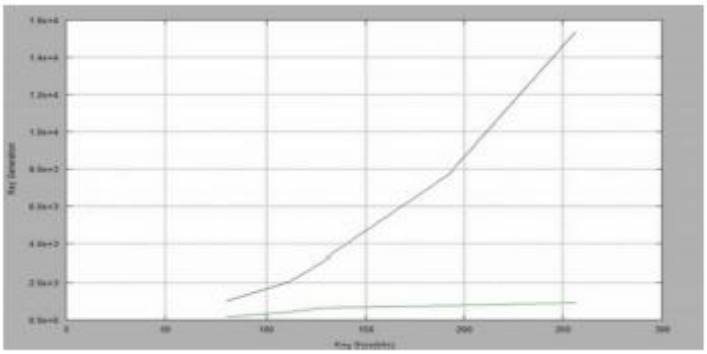


Fig.3 Key size comparison of ECC and RSA

H. Features of an ideal biometric template protection scheme

We found out there are four features should consist when a biometric template protection algorithm is designed:

1) *Diversity:* The secure biometric template must not allow cross-matching across databases, thus ensuring their user's privacy.
2) *Revocability:* It should be straightforward to revoke a compromised biometric template or the ability of the algorithm to cancel the compromised template and generate the new one from the same biometric trait. Revocability property ensures that cross-matching across biometric databases is not possible, thereby preserving the user's privacy.
3) *Security:* Extract the original template from the protected template must be computationally difficult to achieve. This ensures the secrecy of the user's biometric template. This property discourages adversaries from recreating original biometric traits and using them as a physical spoof of stolen templates.
4) *Performance:* The biometric template protection scheme should not reduce the matching speeds of templates and the recognition performance i.e. the FAR and FRR rates need to be acceptable.

V. CONCLUSION

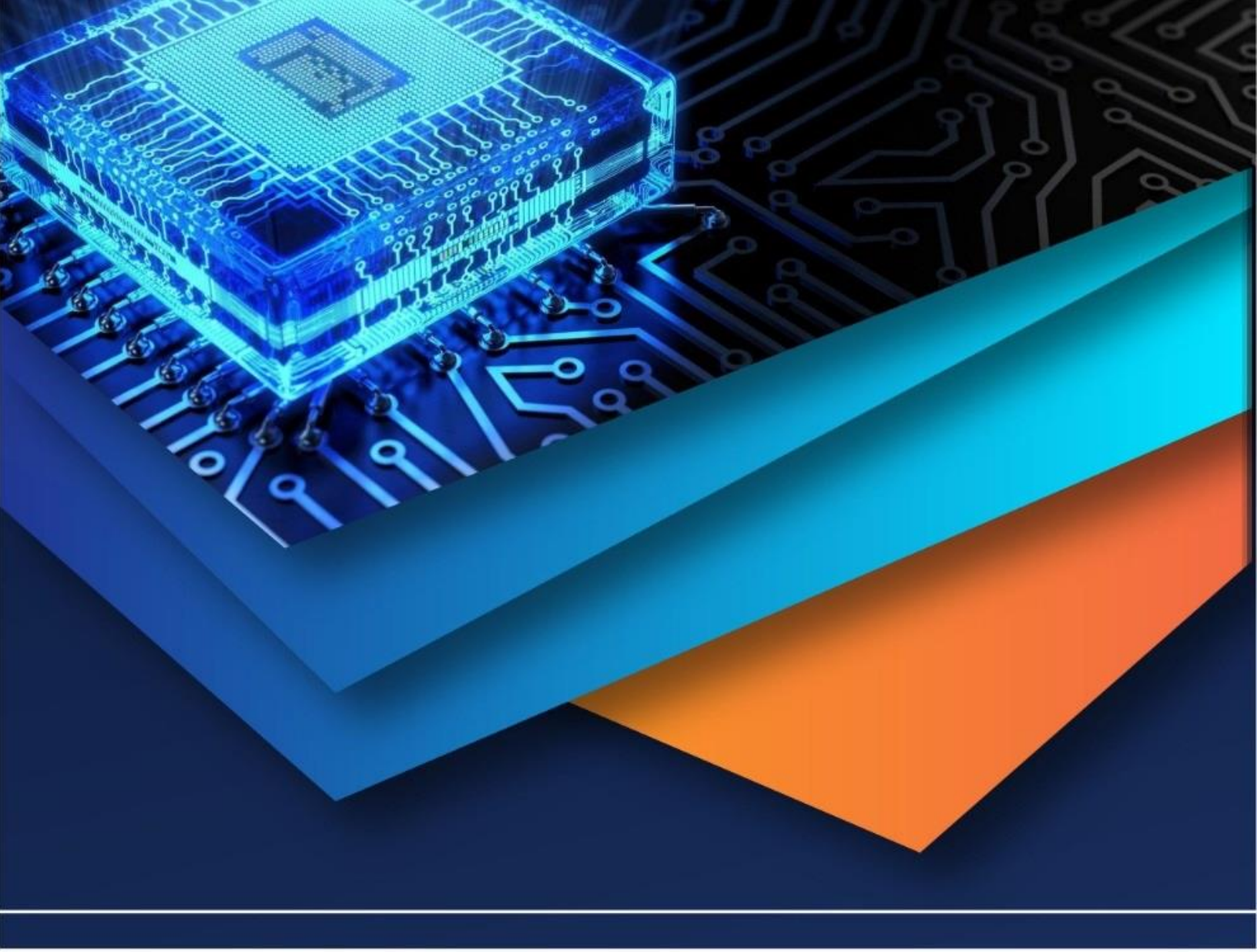
Among the various susceptibilities of a biometric system, leakage of biometric template information is a major security and privacy concern due to the strong linkage between a user's template and his identity and the irrevocable nature of biometric templates. In this paper, we discussed biometric systems processed to describe biometric attacks and threats noted in existing literature. We establish out from existing literature that most of the biometric attacks target biometric templates. We then determined susceptibilities that biometric templates are exposed to as a result of these attacks and explore the 'Type 6' attack on biometric templates. Some various biometric template techniques which generally fall under feature transformation and cryptosystems were explored to identify their strengths and weaknesses. a result of these attacks and finally shows what researchers have been working on to stop these biometric template attacks. It was noted that in all aspects of an ideal biometric template protection scheme, there was no particular biometric template protection technique that proved satisfactory and for that reason, there was still need for more research work to be done to set up secure, reliable, efficient and foolproof biometric template protection techniques. A two-step encryption and decryption approach will propose for future work for securing biometric fingerprint templates stored in a database.

REFERENCES

[1] Mihailescu, Marius Iulian; New enrollment scheme for biometric template using hash chaos-based cryptography Procedia Engineering, 69, 1459-1468, 2014 Elsevier

[2] Patel, Vishal M; Ratha, Nalini K; Chellappa, Rama; Cancelable biometrics: A review IEEE Signal Processing Magazine, 32, 5, 54-65, 2015 IEEE

[3] Mwema, Joseph; Kimwele, Michael; Kimani, Stephen; A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates International Journal of Computer Trends and Technology 20, 1, 18-Dec 2015
[4] Supriya, VG; Manjunatha, SR; Chaos-based cancellable biometric template protection scheme-a proposal International Journal of Engineering Science Invention, 3, 11, 2319-6726, 2014
[5] Nagar, Abhishek; Nandakumar, Karthik; Jain, Anil K; A hybrid biometric cryptosystem for securing fingerprint minutiae templates Pattern Recognition Letters, 31, 8, 733-741, 2010 Elsevier
[6] Li, Peng; Yang, Xin; Qiao, Hua; Cao, Kai; Liu, Eryun; Tian, Jie; An effective biometric cryptosystem combining fingerprints with error correction codes Expert Systems with Applications, 39, 7, 6562-6574, 2012 Elsevier
[7] Kanagalakshmi, K; Chandra, E; A Novel Technique for Cancelable and Irrevocable Biometric Template Generation for Fingerprints Global Journal of Computer Science and Technology, 2013
[8] Jain, Anil K; Nandakumar, Karthik; Nagar, Abhishek; Fingerprint template protection: From theory to practice Security and privacy in biometrics 187-214, 2013, Springer London
[9] Hartloff, Jesse; Bileschi, Maxwell; Tulyakov, Sergey; Dobler, Jimmy; Rudra, Atri; Govindaraju, Venu; Security analysis for fingerprint fuzzy vaults Biometric and Surveillance Technology for Human and Activity Identification X 8712 871204 2013 International Society for Optics and Photonics
[10] Jin, Zhe; Teoh, Andrew Beng Jin; Goi, Bok-Min; Tay, Yong-Haur; Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation Pattern Recognition, 56, 50-62, 2016 Pergamon
[11] Murillo-Escobar, MA; Cruz-HernÃ¡ndez, CÃ©sar; Abundiz-PÃ©rez, F; LÃ³pez-GutiÃ©rrez, RM; A robust embedded biometric authentication system based on fingerprint and chaotic encryption Expert Systems with Applications 42, 21, 8198-8211, 2015 Pergamon
[12] Nasiri, Ali Akbar; Fathy, Mahmood; Alignment-Free Fingerprint Cryptosystem Based On Multiple Fuzzy Vault and Minutia Local Structures 5th SASTech, Mashhad, Iran 2011
[13] Jain, Anil K; Nandakumar, Karthik; Ross, Arun; 50 years of biometric research: Accomplishments, challenges, and opportunities Pattern Recognition Letters, 79, 80-105, 2016 Elsevier
[14] Supriya, VG; Manjunatha, SR; Chaos-based cancellable biometric template protection scheme-a proposal International Journal of Engineering Science Invention, 3, 11, 2319-6726, 2014
[15] Li, Cai; Hu, Jiankun; Attacks via record multiplicity on cancelable biometrics templates Concurrency and Computation: Practice and Experience 26, 8, 1593-1605, 2014 Wiley Online Library
[16] Chandra, Sayani; Paul, Sayan; Saha, Bidyutmala; Mitra, Sourish; Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network IOSR Journal of Computer Engineering (IOSR-JCE) 12, 1, 16-22, 2013
[17] Kumar, Sunil; Garg, Aditi; A Fingerprint Template Protection using Watermarking International Journal of Computer Applications, 149, 8, 2016 Foundation of Computer Science
[18] Sridevi, Mrs. R; Biometric cryptosystem for VOIP security using RSA key generation 2014 Citeseer
[19] Lal, Avanindra Kumar; Dutta, Sandip; ECC based biometric encryption for network security Journal of Computing, 3, 6, 2011
[20] Dodis, Yevgeniy; Ostrovsky, Rafail; Reyzin, Leonid; Smith, Adam; Fuzzy extractors: How to generate strong keys from biometrics and other noisy data SIAM journal on computing, 38, 1, 97-139, 2008 SIAM
[21] Juels, Ari; M. Sudan A fuzzy vault scheme Proceedings of the 2002 IEEE International Symposium on Information Theory, 408, 2002
[22] Jain, Anil K; Nandakumar, Karthik; Nagar, Abhishek; Fingerprint template protection: From theory to practice Security and privacy in biometrics 187-214, 2013 Springer



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY