Survey of Threats to the Biometric Authentication Systems and Solutions

Sarika Khandelwal
Research Scholor,Mewar University,Chitorgarh. (INDIA)

P.C.Gupta
Kota University,Kota(INDIA)

Khushboo Mantri
M.tech.student, Arya College of engineering ,Jaipur(INDIA)

ABSTRACT
Biometric authentication is an exciting field in the system security domain. The challenges associated with this domain need to be addressed in detail since the security of the biometric template is itself a big challenge. Biometric template once lost or copied cannot be changed like simple password. This paper summarizes and discusses major challenges; Categorization of the attacks and their known remedies has also been highlighted. This work is an attempt to establish a thought in front of research community that the methods proposed recently do not sufficiently encompasses the concrete security procedures to make the biometric template safe.

Keywords
Template security, Biometric, Fuzzy vault, Biometric cryptography, attacks on biometrics.

1. INTRODUCTION
To achieve greater level of security to any identification system or verification system it is always required to be supported with concept of passwords for identification. The major problem with password based verification system is that, passwords or PINS can be stolen or lost[1].The suggested and preferred way for individual identity verification which seems to be robust and always available is use of biometric traits such as fingerprint, iris, palm print etc. Any biometric trait which is unique to an individual can be used for individual identification. The major advantage in using biometric trait for identification is that there would never be a problem of forgetting the passwords and it cannot be stolen. Since the biometric templates are stored in the database, security of biometric template is major area of concern. Biometric template stolen once simply means that an individual's identity is stolen, as you cannot change this identity like passwords. As biometric cannot be changed like passwords hence particular biometric trait will become useless if it has been compromised. This paper is an attempt to list out various attacks on biometric template as well as methods that has been proposed till now for biometric template security.

The major categories of securing biometric template includes: Transformation and biometric cryptosystem. In transformation, biometric template is transferred into some other form and stored in that form. Whereas in biometric cryptosystems, concept of key attached to biometric data with cryptographic algorithm is implemented.

There are three different approaches that can be used to secure biometric templates using biometric cryptosystems. They are biometric cryptography, biometric fuzzy vault and biometric certification system.

2. BIOMETRIC CRYPTOSYSTEM
Instead of storing a biometric trait or password as it is enrolled, it is preferred to encrypt a biometric and/or password first and then it is stored to achieve better security of biometric template. Encrypting a biometric template is known as biometric cryptography. It is a method to use cryptography with biometric trait to protect a key. Since long keys are difficult to remember, it is required to be stored somewhere which is big challenge for security of the key. Biometrics can be used in cryptographic key management in 3 different modes: Key binding mode, Key release mode, key generation mode [2].

Key binding mode uses key as well as biometric template to bind them together as a single template. Here neither the key nor the biometric template is stored separately. If an intruder gets the template, then also it is difficult to get the key and even if he gets both the template as well as key he/she cannot create a template since algorithm to bind those is not known. This seems to give better security to the template as well as key since an intruder must have knowledge of key, biometric template as well as the algorithm used to bind them. The only limitation of this system is intra-class variation in biometric data. For example, over a period of time biometric trait may change due to noise, skin condition etc.Key binding mode of biometric cryptosystem is shown in fig.1.

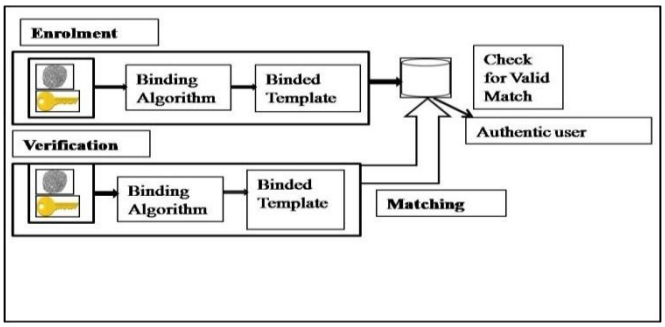

Fig.1: Key binding mode of biometric cryptosystem

As shown in fig.2, key release mode is used to provide the stored key to the genuine user depending on the match of biometric trait that is stored in the database at the time of enrolment. Here biometric as well as key is stored in the database separately. Once the biometric match is found, key is release to the user assuming genuine user. Even though key is secured with the help of biometric trait, biometric template itself is required to be secured in this system because if some imposter gets access to the templates, he/she can breach the system.

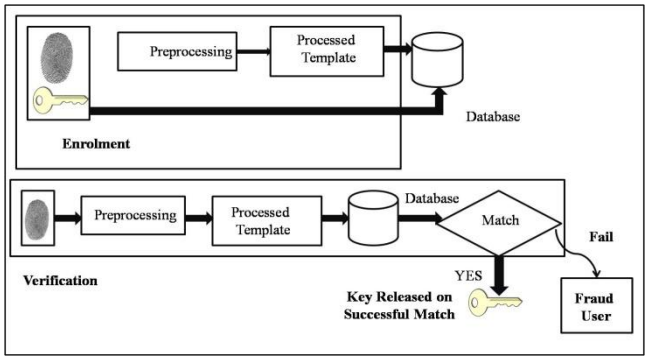

Fig.2: Key release mode of biometric cryptosystem.

Key generation mode is used to generate the key by presenting the biometric trait to the system. At the time of enrolment, Feature extraction of biometric is done and a unique key is generated from those features. This key is not stored in the database. As cryptographic key is required to be unique,the major problem with this system is that, different alignment and orientation of same biometric will produce different keys. This will degrade the performance of the system. The higher level of security in this approach can be achieved by sending the key to an authenticated mobile number or mail ID for which also constraint can be given related to expiry of this key within a specific time which will further reduce chances for an intruder to get into the system. This approach seems to be far securing than presenting the key directly to the user after verification of biometric trait.Key generation mode of biometric cryptosystem is illustrated in fig.3.

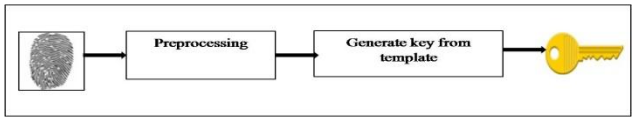

Fig.3: Key generation mode of biometric cryptosystem

To enhance the security of all the above said approaches, it is suggested to combine two or three biometric to form single multi-biometric template. Now this multi-biometric template can be used in key generation, key binding as well as key release mode.

There is need to design a biometric cryptosystem in key generation/key binding mode which provides more security to the template as well as key, which is cost effective, which can provide better storage requirement, and should able to handle intra-class variations ion biometric data..

3. TEMPLATE SECURITY APPROACHES

Different strategies that are available to secure biometric template are generally based on cryptographic key binding/key generation mode. It includes transformations like salting or bio-hashing, cryptographic framework like Fuzzy vault, fuzzy commitment, secure sketches, fuzzy extractor etc.

3.1 Transformation:

To secure a template it can be transformed into another form using either invertible or non-invertible transformations. Some of such transformations are salting or bio-hashing.

Salting: It is a template protection scheme in which template is converted or transformed into a different form using user specific key [3].The basic advantage of using salting for protecting biometric template is its low false acceptance rate. If a biometric template is compromised, a different template of same biometric can be generated using different key. As the transformation is invertible, if any intruder gets an access to the transformed template and the key, he/she can get the biometric template, which seems to be getting the identity of an individual which is a major drawback of salting.

The random multi-space quantization technique proposed by Teoh et al. [4] is good example of salting. Salting can be done by extracting most distinguishing features of a biometric template say minutia of a fingerprint and then obtained vectors can be projected in randomly selected orthogonal direction. This random projection vectors serves the basis of salting [5].Intra-user variations are handled by binary conversion of feature vector obtained after random projection.

Another more robust approach to secure a template is to use a transform which is non-invertible. In noninvertible transform, the template is transformed into some other form using a key. But it is practically hard to invert an original template from the transformed template even if we have key. Ratha et al [6] have proposed a method for noninvertible transformation of fingerprints. He has proposed three non invertible transformations. Three functions that were used are Polar, Cartesian and Functional to convert the template into noninvertible form.

3.2 Fuzzy vault:

Fuzzy vault is biometric construct used to bind key as well as template together in a single framework. The ability of fuzzy vault to handle intra-class variations in biometric data makes it more popular to use.

In order to secure a template using fuzzy vault, a polynomial is evaluated using secret key and some identifying points say minutia points in fingerprint templates are added to it to form a fuzzy vault. Some chaff points are also added to enhance the security. The more the chaff points, better is the security of template. The security of fuzzy vault is based on infeasibility of polynomial reconstruction problem[7].V.Evelyn Brindha[8] has proposed a robust fuzzy vault scheme in which fingerprints and palm prints are combined together to enhance the security of the template. In his work, Fingerprint template is preprocessed first by removing false minutia points, also the palm prints are preprocessed. Both the processed templates are combined together to encode a fuzzy vault. Combination of two modalities enhances the security of the vault. Some results using fuzzy fingerprint vault have been reported [9-15].However, the major problems with all these approaches are that these do not consider all possible issues of fingerprint alignment, verification accuracy etc.Some of the difficulty and importance of alignment problem related to rotation in fuzzy fingerprint vault is explained by P. Zhang[16]. Chung and Moon [11-13] proposed the approach to solve the auto-alignment problem in the fuzzy fingerprint vault using the idea of the geometric hashing [17].

Yang and Verbauwhede [18] has used the concept of automatic alignment of two fingerprints of fuzzy vault using the idea of reference minutia. The reference minutia was generated with the distance and orientation of two nearest neighbor minutia. But the impractical assumption that two reference minutia can be accurately extracted from both the enrolled and input fingerprint lead their result to FRR of 17% and FAR of 0%.

Jin Zhe[19] has proposed protected template scheme which is alignment free. The new minutia representation technique

known as minutiae vicinity decomposition is used where each minutia is decomposed into four minutiae triplets. From these triplets a geometric feature is extracted to construct a fingerprint template. The given algorithm consists of following stages. (a) Minutia Vicinity Formulation (b) Minutia Vicinity Decomposition (c) Invariant Features Extraction (d) Protected Template Formulation (e) Template Matching. The experimental results show that it is computationally hard to retrieve minutia information even when both protected template and random matrix are known. Besides that, the scheme is free from alignment and light in complexity.

Another problem that is reported in literature with fuzzy vault is that, Fuzzy vault is susceptible to correlation attack. That is two fuzzy vault created using same fingerprints can be correlated to reveal fingerprint minutiae hidden in the vault.

Sungju Lee[20] has proposed a fuzzy vault in which correlation attack is avoided using an approach to insert chaffs in a structured way such that distinguishing the fingerprint minutiae and the chaff points obtained from two applications is computationally hard. Instead of randomly inserting the chaff points, it is inserted structurally for which direction information of minutiae was used. The result shows that the designed fuzzy vault is resistant to correlation attack by a factor of about 153.

3.3 Mixing Features of two Fingerprints to secure a template:

Instead of storing a single fingerprint, two fingerprint features are mixed together and are stored as a single template. Arun Ross[21] has proposed a method to secure a fingerprint by storing it as a mix feature of two fingerprints. The advantages this method is that as a template is mixture of two fingerprints, it looks like a fingerprint only and hence any algorithm which can be applied on single fingerprint can be used to process this template also. Another advantage of mixing fingerprint is that the identity of original fingerprint cannot be easily deduced from mixed fingerprint. As the identity cannot be deduced from the mixed fingerprint, this method seems to be more secure to protect a fingerprint identity. The approach used in mixing the fingerprint features are shown in fig.4. The experimental results have proved that the new fused fingerprint can be used for identification. For mixing the features of two fingerprints, a single fingerprint is decomposed into spiral components and continuous components to get four components' of two fingerprints, these are combined to get two mixed templates that is spiral component of one fingerprint is mixed with continuous component of other fingerprint.

3.4 Fuzzy extractors and secure sketches:

Fuzzy extractor extracts uniform string R from its input template in a noise tolerant way that is even if the input template is not same as enrolled one but is close to enrolled template to a accepted level, it produces the same uniform string R. Fuzzy extractor is a combination of secure sketch and fuzzy randomness extractor.[24].

Secure Sketches: Secure (or fuzzy) sketches, introduced by (Dodis et al.,2004), correct errors in noisy secrets by releasing a helper string S. That is it generate some public information related to the input which itself is not capable for recovering the template.

Given this public information and a random input which is close to the enrolled input will reproduce the original template. The randomness extractor is used to map the non-uniform input into uniformly distributed string. When a query template is required to be matched to the input, fuzzy extractor uses the sketch of the input which is public along with the query template to generate the input exactly. Fuzzy extractor is designed in such a way that if the query input is within the threshold distance of the enrolled one then the reconstruction will be successful.

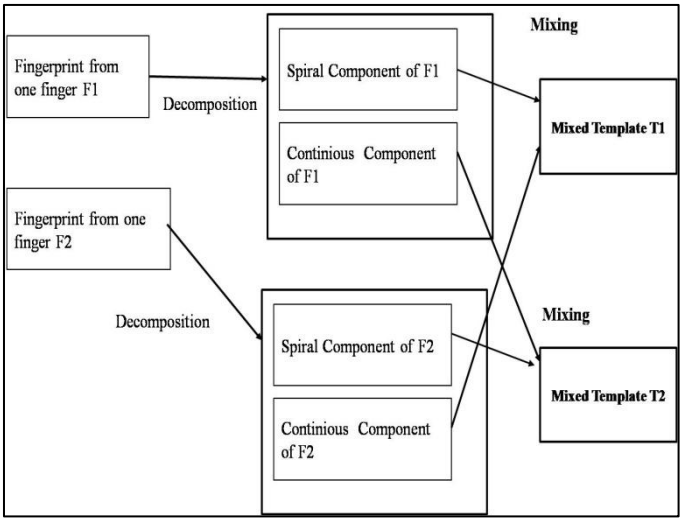

Fig4. Mixing two fingerprint features to protect a template [21].

4. ATTACKS ON BIOMETRIC SYSTEM:

Biometric system can be attacked by an intruder with different types of attacks on the system. Biometric system can be attacked at various level as shown in fig.5 There are 8 different points at which biometric system can be attacked as shown in fig.5. The 9thpoint of attack on biometric system is also found in some of the latest studies.

Type 1 attack includes presenting the fake fingerprint to the sensor that mimics like an authorized user. Example includes presenting gelatin fingerprint to the sensor. This attack seems to be most successful since it does not require anything else other than a fake fingerprint. This attack does not require knowledge of a matching algorithm nor access to template database. Putte and Keuning [25] tested several fingerprint sensors to check if they accept fake fingerprint. The authors has created fake fingerprint with cooperation of the real owner as well as without cooperation of the owner. Matsumoto et al. [26] attacked 11 different fingerprint verification systems with artificially created gummy (gelatin) fingers.

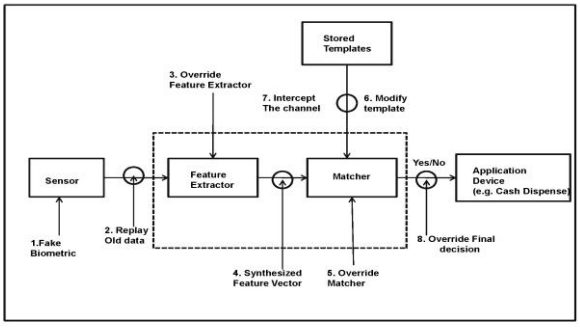

Fig.5.Attack points on biometric system. (Adapted from [23])

To overcome such fake biometric attacks, Derakhshani et al. [27] proposed two software-based methods for fingerprint liveness detection. They used a commercially available capacitive sensor and the sole input to the livens detection module is a 5-second video of the fingerprints. In their static method, the periodicity of sweat pores along the ridges is used for livens detection. In the dynamic method, sweat diffusion pattern over time along the ridges is measured. Live fingers, fingers from cadavers, and dummy fingers made up of play dough are used in the experiments. A back propagation neural network (BPNN) based classifier is used to distinguish live fingers from cadaver/dummy fingers. The static method leads to an EER of nearly 10%; the dynamic method leads to an EER in the range of 11-39%, where a false accept event is a cadaver/dummy finger being classified as live, and a false reject event is a live finger being classified as a cadaver/dummy.

Type 2 attack is to attack the channel between sensor and feature extractor module. But this attack is not possible where sensor and feature extractor modules are embedded in the same machine. This can be done by replay attack i.e. the biometric that is submitted to the sensor can be replayed by bypassing the sensor.

Type 3 attack is to attack the feature extractor module. This can be done by overriding the feature extractor module and forcing it to generate the features values that an unauthorized user wants.

Type 4 attack is on the channel between the feature extractor and the matcher. Features extracted by the extractor can be replaced by a different feature set. This type of attack is difficult because the feature extractor and matcher are not separate. This attack is possible only if the matcher is remote and the features extracted have to be sent to the matcher for matching purpose.

Type 5 attack is on the matching module and to force it to produce high or low matching score irrespective of the input.

Type 6 is attack on the stored database template i.e. to modify one or more template stored in the database. This could result in fraudulent authorization of an individual or a denial of service.

Type 7 attack is on the channel between database and matcher. Example includes Sniffing traffic to steal templates, injecting template to falsely authenticate a malicious user.

Type 8 attack is to override the decision made by the decision module as per the requirement of the hacker.

A new attack reported in literature is type 9 attack which is similar to type 4 attack but it has potentially long lasting effects. This attack could permanently add malicious template into the database.

Other attacks on biometric identification or verification include FAR attack, cross matching attack etc.

a) FAR attack: FAR (False acceptance rate) is when the system accepts the user assuming it is genuine even though it is not. FAR of 0.01% means that out of 104 samples of a biometric any one may have same features as that of enrolled biometric. FAR attacks can be made if one is having access to huge biometric database.

This type of attack cannot be prevented by template protection schemes discussed above.

b) Cross matching attack: It is also known as linkage attack. If different applications are using same biometric for identification, similar identities of same person may be stored in different databases. Different application may be correlated exploiting the identity. In order to prevent this attack, Template protection scheme can be used. In template protection scheme, different pseudo identities are generated from same template. These pseudo identities are independent and random and hence linkage can be avoided.

c) Hill climbing attack: Hill climbing attack is possible only if biometric system releases the information about partial match. It is an optimization method to improve searching efficiency. In this type of attack, based on the matching score, the similarity between the target image and modified image can be iterated. Hill climbing attack is impossible in helper data template protection since comparator uses the exact match of the stored secret hash and the live calculated one. However, in the biometric encryption method, the biometric samples are randomized by multiplying a random pattern and the original biometric information is still hidden in the randomized image. A quantized hill climbing can be used to attack it as shown in [22]. In biometric encryption, no similarity score is directly available, however, a value, which is comparable with quantized scores, can be obtained with the help of a linkage table. In each of the iterations modifications are not applied globally, but locally, so that the changes can cause sufficient improvements of the (quantized) similarity score. In [22], an example of a quantized hill climbing is given for facial images. A small facial gallery is collected and Eigen faces of the images are calculated. An initial image is chosen and divided into 4 quadrants. Noise is added on a quadrant; meanwhile, the opposite quadrant is varied slightly in the Eigen face space, so that similarity score creases at least by one quantized level. The experimental results show that a match able similarity to the target image can be obtained for a randomly selected initial image. In cancelable biometrics, the comparison is also based on similarity. Theoretically, a hill climbing attack should be possible. However, its feasibility might be influenced by the non-invertible function used.

5. CONCLUSION AND DISCUSSION:

To identify an individual uniquely, biometric template matching is still best method. But to make biometric template a robust method to identify an individual security issues discussed in this paper needs to be addresses. Since the biometric are limited for an individual, it is required to be protected to be stolen or misused. This paper has discussed various methods of protecting a biometric template to make it more secure. This paper has also given the different possible attacks that can be prevented to make a biometric identity system more secure and safe. This paper has tried to figure out major challenges existing in the field of biometric security.

6. ACKNOWLEDGMENTS

I thank to the management of Geetanjali Institute of Technical studies, Udaipur to make all the resources available to me to conduct this survey. I thank all those persons involved directly or indirectly to make this work available for publication.

7. REFERENCES

[1] K. Mitnick, W. Simon, and S. Wozniak, The Art of Deception: Controlling the Human Element of Security. Wiley, 2002.

[2] KarthikNandakumar,Anil K. Jain, Sharath Pankanti,"Fingerprint-based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics And Security, December 2007

[3] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar," Review Article Biometric Template Security", EURASIP Journal on Advances in Signal Processing

Volume 2008, Article ID 579416, 17 pages doi:10.1155/2008/579416.

[4] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 1892–1901, 2006.

[5] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfacesversusfisherfaces: recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and MachineIntelligence, vol. 9, no. 7, pp. 711–720, 1997.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle,"Generating Cancelable Fingerprint Templates," IEEE Transactionson Pattern Analysis and Machine Intelligence, vol. 29,no. 4, pp. 561–572, April 2007.

[7] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Proceedings of IEEE International Symposium on Information Theory, vol. 6, no. 3, pp. 408,2002.

[8] V. Evelyn Brindha "Biometric Template Security using Fuzzy Vault" 2011 IEEE 15th International Symposium on Consumer Electronics

[9] T. Clancy, et al., "Secure Smartcard-based Fingerprint Authentication," in Proc. of ACM SIGMM Multim., Biom. Met.& App., pp. 45-52, 2003. Article (CrossRef Link)

[10] U. Uludag, et al., "Fuzzy Vault for Fingerprints," in Proc. of Audio- and Video-based Biometric Person Authentication, pp. 310-319, 2005. Article (CrossRef Link)

[11] K. Nandakumar, et al., "Fingerprint-based Fuzzy Vault: Implementation and Performance," IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744-757, 2007. Article (CrossRef Link)

[12] S. Yang and I. Verbauwhede, "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," in Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 5, pp. 609-612, 2005. Article (CrossRef Link)

[13] Y. Chung, et al., "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," LNCS 3822, pp. 358-369, 2005. Article (CrossRef Link)

[14] D. Moon, et al., "Fingerprint Template Protection Using Fuzzy Vault," LNCS 4707, pp.1141-1151, 2007. Article (CrossRef Link)

[15] D. Moon, et al., "Configurable Fuzzy Fingerprint Vault for Match-on-Card System," IEICE Electron Express, vol. 6, no. 14, pp. 993-999, 2009. Article (CrossRef Link)

[16] P. Zhang, J. Hu, C. Li, M. Bennamound, and V. Bhagavatulae, "A Pitfall in Fingerprint Bio-Cryptographic Key Generation," Computers and Security, Elsevier, 2011. Article (CrossRef Link)

[17] H. Wolfson and I. Rigoutsos, "Geometric Hashing: an Overview," IEEE Computational Science and Engineering, vol. 4, pp. 10-21, Oct.-Dec. 1997.

[18] S. Yang and I. Verbauwhede, "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," in Proc. of IEEE International Conference on

[19] Jin Zhe "Fingerprint Template Protection with Minutia Vicinity Decomposition" 978-1-4577-1359-0/11/$26.00 ©2011 IEEE

[20] Sungju Lee, "A Practical Implementation of Fuzzy Fingerprint Vault" KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 5, NO. 10, October 2011 pg. 1783-1798.

[21] Arun Ross and Asem Othman ,"MIXING FINGERPRINTS FOR TEMPLATE SECURITY AND PRIVACY" 19thEuropian Signal processing conference(EUSPICO-2011),Barcelona,spain,August-29-sept 2-2011 ISSN 2076-1465

[22] Adler, A.: Reconstruction of source images from quantized biometric match scoredata. In: Biometrics Conference, Washington, DC (September 2004)

[23] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

[24] S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 760–769, 2007.

[25] T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App., pp. 289-303, 2000.

[26] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems", Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275-289, 2002.

[27] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use Acoustics, Speech, and Signal Processing, Vol. 5, pp. 609-612, 2005. Article (CrossRef Link)