International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 14 No. 4 Feb. 2016, pp. 997-1004
© 2016 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

Cryptographic schemes for minutiae template protection

***Ramón Santana Fernández*[1], *Vivian Estrada Senti*[2], *and Yanio Hernandez Heredia*[2]**

[1]Biometric research, University of Informatics Science, Havana, Cuba

[2]University of Informatics Science, Havana, Cuba

[2]Software development, University of Informatics Science, Havana, Cuba

ABSTRACT: The recent implementation of biometrics solutions for user authentication in public networks has caused great concern about the safety and privacy of biometric data. Different vulnerabilities detected on automated fingerprint identification systems could reveal minutiae data if they are stored in plain text. In order to solve these security issues, several fingerprint minutiae template protection schemas have been proposed, among which there are the fuzzy vault, biohasing and cancellable or non-invertible fingerprint templates. To carry out an efficient biometric data protection process, the schema must meet three basic requirements: cryptographic security, revocability and performance; however, most of the schemas described to date fail in this task. A fingerprint minutiae template protection scheme must capture as much identifying information of the fingerprint as possible and solve the problem of template alignment before the comparison process is performed in the protected domain. A study on the cryptographic scheme of fingerprint minutiae template protection models and alignment methods was conducted in this work. Emphasis was placed on the cryptographic bases of minutiae template protection scheme and existing algorithms for aligning protected templates, highlighting the weaknesses of each one. As a result, the knowledge necessary to design an alignment-free minutiae template protection model was obtained.

KEYWORDS: Fuzzy vault, Fuzzy commitment, cancellable templates, fingerprint template protection.

1 INTRODUCTION

The use of passwords or smart cards as identification tokens provide high levels of security for people identification; however, this kind of identifiers can be lost, stolen or forgotten; compromising the integrity and privacy of the protected resources. Biometrics, by other hand, have been applied as an identifier in personal identification for decades with great achievement in governmental and criminal systems, with high levels of acceptance and accuracy in private networks and controlled environments. Nowadays the range of application of biometrics has been expanded to daily tasks in networks with less security than private networks. The personal identification in ATMs, access controls, in personal car configuration or bank transactions are some examples. The main aim is to increase the security level in the identification process and fight against identity fraud. Using biometrics traits, like fingerprints or face, as personal identifier decreases the possibilities of stealing, misplacing or forgetting the identifier, but preserving the privacy, security and integrity of the biometric data transmitted across public networks has become a challenge. The main concern about biometric security is the identifiers' property of irrevocability. Different from passwords or identification cards, biometric identifiers are invariant through a person's natural life, and cannot be changed.

Biometrics is described in Dahiya & Kant (2012) as the measurement of biological data, used for person authentication through physical traits, like fingerprint, and behavioral traits, like signatures. From the user's perspective (Jain, Nandakimar, & Nagar, 2012) a biometric system must accomplish two fundamental characteristics: only legitimate users must have access to the logical or physical resources protected by the biometric system and the personal biometric data stored must be used to restrict and control the access to the protected resources. In different analyses conducted by Jain, Nandakumar, & Nagar, (2008) and Prasad (2013), eight vulnerabilities have been detected in a generic biometric system architecture through which several kinds of attacks can be performed to obtain the biometric information and data belonging to a person. In (Jain, Nandakumar, & Nagar, Biometric Template Security, 2008) it describes different attacks and its main purposes to compromise the biometric data used in the authentication process into the biometric system when the data is in plain text. Privacy attack, subversive attack, contamination or cover attack, hill climbing attack, synthetic biometric submission and masquerade attack are some examples of it focused on retrieving biometric data. The primary target of this attacks are: the feature extractor, template matching, the biometric database and the communication channels between them as shown in Figure 1.

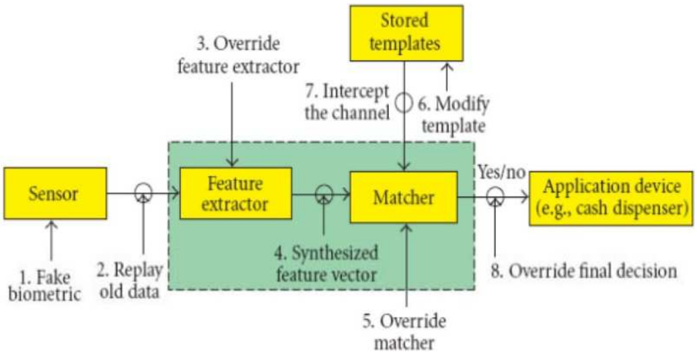


Fig. 1. Vulnerabilities on general biometric identification system architecture

The partially or fully leak of information from the fingerprint minutiae template allows the fingerprint image reconstruction process proposed by Cappelli, Lumini, Maio, & Maltoni (2007), the insertion of the minutiae template between the extractor and matcher or the substitution of the original template in the channel between the matcher and the biometric data base. By this way the biometric system security may be compromised and the protected resources could be obtained by the attacker. Another consequence is the denial of service to a genuine and authorized person, the owner of the biometric trait can be tracked on each biometric database in which the same biometric trait is used for authentication proposes. The most important problem generated from the biometric template theft is the loss of this biometric trait and the security and privacy of the protected resources for his entire life.

Several solutions to decrease the minutiae template leak of information in a biometric system have been proposed. The application of traditional cryptography to the fingerprint template protection process is one of them (Jain, Nandakimar, & Nagar, 2012). However, factors like non-lineal distortion caused by the elastic property of the skin, the fingerprint sample rotation and translation, among others, make harder the minutiae matching in the protected domain using this method at a significant level. The main reason resides in the fact that the mathematical functions used in this process are highly sensible to small data changes and a little variation on the input data may cause great variations on the output data. The biometric data have a variability degree when the sample is taken, that is the reason why the minutiae template matching in the protected domain has a very poor performance. To execute this process with better results, a decryption process is mandatory. Hardware malfunction, the access to the shared memory by a Trojan horse or other malicious piece of software represents a risk because the biometric data is in plain text (Jain, Nandakumar, & Nagar, 2008). Other solutions have been analyzed and as result some minutiae template protection scheme have been proposed. The most frequently cited and with better results are the fuzzy vault (Juels & Sudan, 2002), non-invertible template transformation (Ratha, Chikkerur, Connell, & Bolle, 2007), biohashing (Belguechi, Rosenberger, & Ait, 2010) and fuzzy commitment (Juels & Wattenberg, 1999; Juels & Wattenberg, 2013). These models are the cryptographic bases of the hybrid models of template protection scheme, proposed to eliminate or deal with problems like minutiae alignment or allow the revocability property. These schemes propose a way to transform the original minutiae template into protected minutiae templates from the original feature or from a derivation of the original feature. The main advantage of this schemes are that they allow the matching process in the protected domain with better results than traditional cryptography.

This paper analyzes the minutiae template protection schemas described above and it is organized as follows: related works are referenced in Section 2 as Background, the cryptographic schemes for minutiae template protection are described in Section 3 and Conclusions and future work are presented in section 4.

2 BACKGROUND

The first minutiae fingerprint template protection schemes described in the consulted bibliography are fuzzy commitment scheme (Juels & Wattenberg, 1999), fuzzy vault scheme (Juels & Sudan, A Fuzzy Vault Scheme, 2002), the cancellable templates or non-invertible template scheme (Ratha, Connell, & Bolle, 2001) and biohashing scheme (Beng Jin, Chek Ling, & Goh, 2004). Several approaches have been proposed to address different issues and for different applications but the principles of each scheme are the same. Jain, Nandakimar & Nagar (2012) analyze the state of the art of biometric template protection and their main characteristics. To address the alignment issue due to fingerprint rotation and translation, some approaches have been proposed, such as those by Zhe & Teoh Beng Jin (2011); Belguechi, Rosenberger, & Ait (2010); Ahmad (2013); and Li, Yang, Tian, Shi, & Li (2008), but the problem remains. The main objective, when a fingerprint template protection scheme is proposed, is to obtain as much information as possible from the biometric template to resolve translation, rotation and non-lineal distortion.

2.1 MAIN FINGERPRINT MINUTIAE TEMPLATE PROTECTION CHARACTERISTICS

Minutiae template protections have been classified by some authors (Jain, Nandakimar, & Nagar, 2012; Sharma & Kumar, 2014) in biometric cryptosystems and template transformations:

1. Biometric cryptosystems: a secure sketch, derived from the original biometric information, is generated and stored instead of the original template. The secure sketch, also named helper data, must be as close as the real data to, in presence of the individual feature, obtain the template but in its absence, the sketch must be computationally hard enough to prevent retrieving the original features.
2. Non-invertible transformations: the transformation of the biometric template with a function, using a specific key. There are three kinds of transformations: polar, Cartesian and functional.

Other authors (Poongodi & Betty, 2014) have recently classified minutiae template protection into biometric cryptosystem, intelligent system and watermarking technique:

1. Biometric cryptosystems: as in Jain, Nandakimar, & Nagar (2012), the biometric cryptosystems use a secure sketch derived from the original data and some public information is stored as helper data. The helper data cannot reveal any important information about the fingerprint data. This class can be subdivided into two types, key binding and key generation. In key binding, a key independent of the biometric feature is bound to the biometric template. In key generation, the key is generated from the helper data and queries the biometric feature.
2. Watermarking technique: this uses a watermarking technique, like those proposed by Malhotra & Kant (2013) to ensure biometric security. These advantages are:
    a. The stored biometric template is hard to forge.
    b. It provides high security to the biometric template.
3. Intelligent system: it is described as a computer system in some environments capable of independent actions to meet some objectives. This class has 9 properties and there are different types of agents.

As result of the analyses of both classifications, it is considered that the watermarking technique is an approach to protect information and is not considered as a class, while the intelligent system is considered a practical issue, not a theoretical approach, which groups various ways to perform template protection. To formulate an efficient biometric template protection scheme, three fundamental principles must be taken into account as proposed by Jain, Nandakimar, & Nagar (2012):

1. Cryptographic security: if an attacker obtains a protected biometric template, it must be computationally hard to retrieve the original data.
2. Revocability: it must be possible to obtain several protected templates from the same original biometric data. In case an attacker obtains two or more protected biometric templates, the original biometric data should remain cryptographically secured.
3. Performance: biometric performance should not be affected, measured in terms of FAR/FRR.

Considering the fact that a biometric authentication system must respond in the shortest time possible, the computational cost and response time must be considered as part of performance requirement of a biometric template protection scheme. Another important question to consider is on what feature the protection is carried out. As a conclusion from the analysis of this requirement, the development of a fingerprint minutiae template protection scheme is quite a challenge and can be done starting with three different kinds of features:

1. From the original biometric feature set.
2. From an intermediate set of feature derived from the original feature set.
3. From a fixed length feature set derived from the original or intermediate feature set.

The proposed scheme using the original feature (Juels & Sudan, 2002; Beng Jin, Chek Ling, & Goh, 2004) do not take into account the alignment process and must be done separately. The proposed scheme using an intermediate set of feature (Zhe & Teoh Beng Jin, 2011) are invariant to rotation and translation, and the critical process is the selection of the identificative feature from the minutiae information. The fixed length is commonly used in other biometric traits, like iris, but it can be used in the biohashing scheme as explained by Belguechi, Rosenberger, & Ait (2010).

2.2 Fingerprint template alignment

In order to enhance the fingerprint template matching process on the protected domain and due to translation, rotation, non-lineal distortion and overlapping properties of the fingerprint a pre -alignment process is required as explained by Zhang, Feng, & He)2014). These variations are known as intra-class variations and are the main consequence of the decreasing performance in the matching stage. To perform the minutiae alignment, some techniques have been proposed (Boonchaiseree & Areekul, 2009; Jeffers & Arakala, 2007; Jeffers & Arakala, 2006; Zhang, Feng, & He, 2014; Maltoni, Maio, Jain, & Prabhakar, 2009), among those are:

1. Most representative minutiae or focal point.
2. Singularities detection.
3. Topological structure alignment.
4. Iterative Closest Point.

However, it is considered an unsolved issue yet (Sonar & Dahad, 2014). The impact of this process in a biometric system can be negative because a miss selection and evaluation on the most representative minutiae or focal point may lead to poor performance. The iterative closest point is an iterative algorithm and depend on the directional field among other and the singularities core and delta in a fingerprint image are not always present. The minutiae structure formation using Voronoi neighborhoods, minutiae triplets, five neighborhoods analyzed by Jeffers & Arakala (2006) is one of the most suitable for this problem. From these minutiae structures, a rotation and translation invariant set of features can be extracted (Zhe & Teoh Beng Jin, 2011) to perform the encryption.

3 Cryptographic Minutiae Template Protection Schemes

The main goal of the biometric template protection process is to avoid minutiae template information leak and for this reason several methods have been proposed, among which there are fuzzy vault, non-invertible template transformations or cancelable templates and biohashing scheme.

3.1 Fuzzy vault

It is a cryptographic construction based on the fuzzy commitment proposed by Juels & Wattenberg (1999); Juels & Wattenberg (2013) designed to encrypt a disordered set of features. The fuzzy vault was proposed by Juels and Sudan in 2002 and it is designed as an error -tolerant encryption form. The security safety of this method is based on the computationally hardness to resolve the polynomial reconstruction problem (Clancy, Kiyavash, & Lin, 2003; Juels & Sudan, 2002).

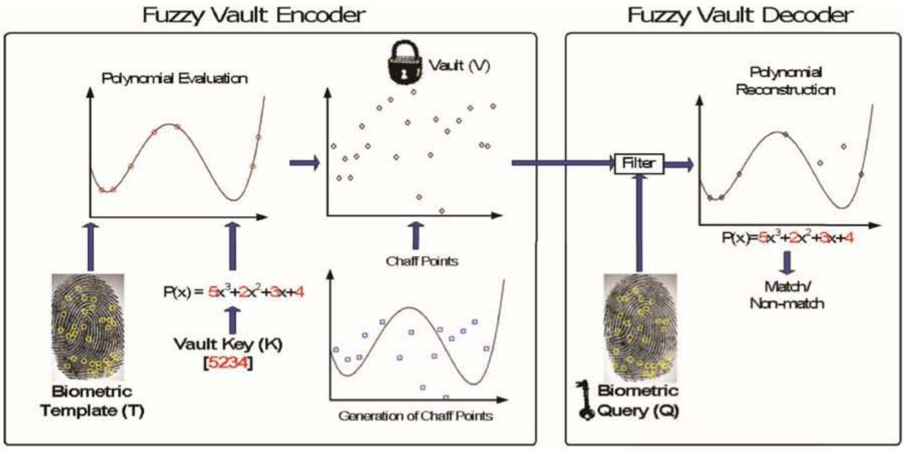
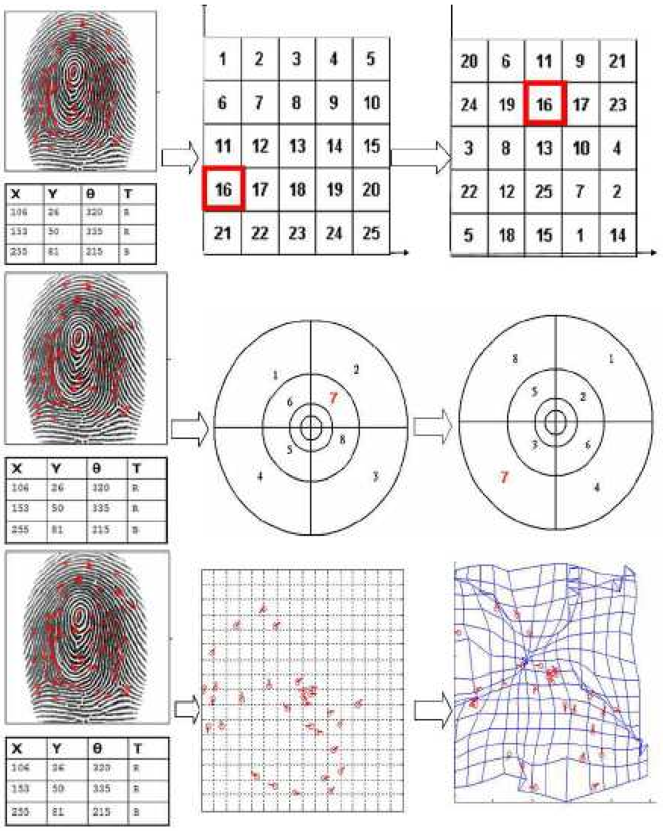


Fig. 2. Fuzzy Vault Scheme for biometric protection

As for the protection minutiae templates, this scheme describes two process (Rathgeb & Uhl, 2011; Juels & Sudan, A Fuzzy Vault Scheme, 2002), the encryption process (enrol) and the decryption process (comparison). To carry out the encryption process, a generalized code word is created, representing the secret *k* and the corresponding polynomial construction *p*. The disorder feature set *A* is evaluated in *p* and a set *q* of chaff points are added to create the protected template *R*. The chaff points are randomly generated noise in coordinate form (x, y) and cannot match the polynomial construction *p*. To check if a biometric feature set *B* contains or has a level of similitude with the set *A,* both sets are overlapped. If the set *B* is substantially overlapped in the set *A,* then the chaff points can be identified and the polynomial construction *p* is obtained by the reconstruction process using the error correcting code.

3.2 CANCELLABLE TEMPLATES

It is the repetition and intentional distortion of a biometric sign based on a non-invertible transformation (Ratha, Connell, & Bolle, 2001). The process is executed every time the authentication or enrollment petition is performed by the biometric system. If a protected minutiae template is compromised during an attack, it is possible to change the transformation function and generate a new protected set of features from the original feature set. This kind of transformation has as advantage that if the protected template is obtained and the transformation function is known, the biometric data cannot be recovered due to the non-invertibility property of the encryption function used. Ratha N. , Connell, Bolle, & Chikkerur (2006); Jain, Nandakimar, & Nagar (2012) present three kinds of transformations, named Cartesian transformations, Radial transformations and Functional transformations, to encrypt fingerprint minutiae template as shown in Figure 3.



X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

20	6	11	9	21
24	19	16	17	23
3	8	13	10	4
22	12	25	7	2
5	18	15	1	14

X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

Fig. 3. Non-invertible minutiae template protection scheme

In the Cartesian transformations, the minutiae are organized and measured in rectangular coordinates. To perform the encryption the fingerprint is divided into cells or rectangular sub -areas and the minutiae are reorganized changing the position (from one cell to another). The transformation is not a permutation, several cells can be mapped into one cell to make the transformation irreversible. The Radial transformation consists on the conversion to polar coordinates and the change of the minutiae between the sectors. The conversion is performed using as reference point the core singularity and the minutiae angles are measured in reference to the orientation. The Functional transformations have restrictive properties to design a cancellable template. The function to encrypt the minutiae data must be globally non-smooth and locally smooth.

3.3 BIOHASHING

It was exclusively applied to the texture feature of a fingerprint extracted using the FingerCode technique (Jain, Prabhakar, Hong, & Prankanti, 1999) as shown in Figure 4:

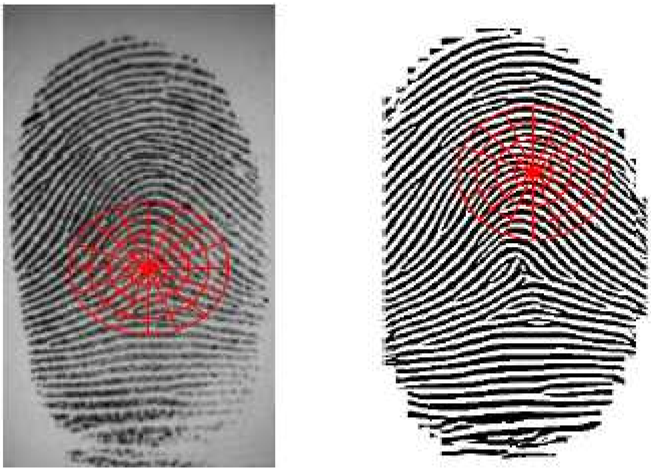


Fig. 4. Finger code extraction from a minutiae in fingerprints

The first approach of this method depended on the core singularity of the fingerprint through which the process is performed. Recent approach translates the center of this method to each minutiae (Belguechi, Rosenberger, & Ait, 2010) allowing the protection of each one and concatenating the result into a resultant string. The process began with the MinuCodes computation, which is the FingerCode process applied to each minutiae and not to a core singularity. For each MinuCode the biohashing is processed as follows:

1. The generation of pseudo-random vector is performed.
2. Gram-Schmidt process is applied to transform the generated vector into an orthonormal set of matrices.
3. The inner product between the biometric feature and the matrices are performed.
4. The result is compared with a threshold calculated with Otsu method.

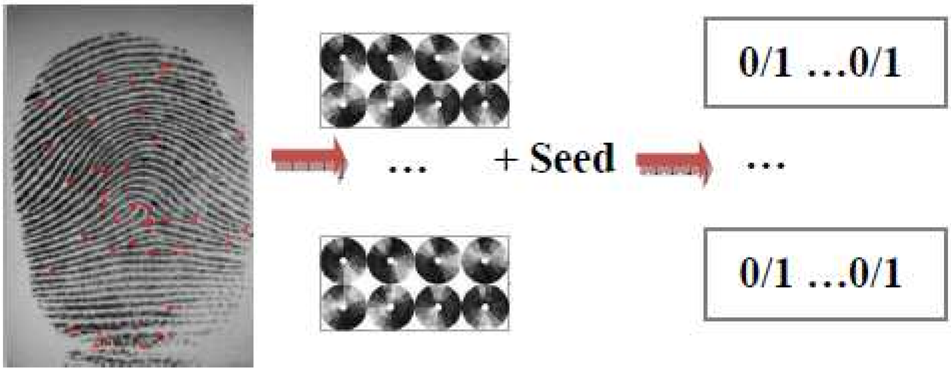


Fig. 5. Biohashing template protection scheme representation from (Belguechi, Rosenberger, & Ait, 2010)

Figure 5 shows how each minutiae is transformed into a FingerCode and then the Biocodes are processed to obtain a string vector. Only the BioCodes are processed to be stored.

4 Conclusion and Future Work

The full or partial leak of information in the biometric template are one of the most important vulnerabilities and security risks in biometric systems. The generalized use of biometric data to identify persons in daily tasks, across public networks with low security level, facilitate the retrieval of minutiae data if it is in plain text. To encrypt the biometric data a few minutiae template protection scheme has been proposed based on cryptographic constructions, named fuzzy vault, cancellable templates and biohashing, allowing better security levels. The alignment schemes analyzed provide an insight about this process and the matching in the protected domain and as future work the vulnerabilities and countermeasures of each cryptographic model will be analyzed to propose a new cryptographic method to encrypt a set of features from the minutiae.

REFERENCES

[1] Ahmad, T. (2013). SHARED SECRET-BASED KEY AND FINGERPRINT BINDING SCHEME. *Kursor Journal*.

[2] Belguechi, R., Rosenberger, C., & Ait, S. (2010). BioHashing for securing fingerprint minutiae templates. 1168-1171. IEEE Computer Society.

[3] Beng Jin, A. T., Chek Ling, D. N., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition Society*. Elsevier.

[4] Boonchaiseree, N., & Areekul, V. (2009). Focal Point Detection Based on Half Concentric Lens Model for Singular Point Extraction in Fingerprint. *Proceedings of International Conference on Biometrics*. IEEE.

[5] Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. (2007). Fingerprint Image Reconstruction from Standard Template. *29(9)*. IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE.

[6] Clancy, C., Kiyavash, N., & Lin, D. J. (2003). Secure SmartcardBased Fingerprint Authentication. Berkeley: ACM.

[7] Dahiya, N., & Kant, C. (2012). Biometrics Security Concerns.

[8] Jain, A. K., Nandakimar, K., & Nagar, A. (2012). Fingerprint Template Protection: From Theory to Practice. 29.

[9] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*.

[10] Jain, A. K., Prabhakar, S., Hong, L., & Prankanti, S. (1999). FingerCode: A Filterbank for FIngerprint Representation and Matching.

[11] Jeffers, J., & Arakala, A. (2006). MINUTIAE-BASED STRUCTURES FOR A FUZZY VAULT. *2006 Biometrics Symposium*.

[12] Jeffers, J., & Arakala, A. (2007). FINGERPRINT ALIGNMENT FOR A MINUTIAE-BASED FUZZY VAULT.

[13] Juels, A., & Sudan, M. (2002). A Fuzzy Vault Scheme. 1-18. Retrieved from MIT Computer Science and Artificial Inteligence Laboratory: http://www.csail.mit.edu/peoplesearch

[14] Juels, A., & Wattenberg, M. (1999). A Fuzzy Commitment Scheme. 28-36.

[15] Juels, A., & Wattenberg, M. (2013). A Fuzzy Commitment Scheme.

[16] Li, J., Yang, X., Tian, J., Shi, P., & Li, P. (2008). Topological Structure-based Alignment for Fingerprint Fuzzy Vault.

[17] Malhotra, S., & Kant, C. (May de 2013). A Novel Approach for securing Biometric Template. *Internal Journal of Advanced Research in Computer Science and Software Engineering*.

[18] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). HandBook of Fingerprint Recognition. Springer.

[19] Poongodi, P., & Betty, P. (January de 2014). A Study on Biometric Template Protection Techniques. *International Journal of Engineering Trends and Technology*.

[20] Prasad, P. S. (June de 2013). Vulnerabilities of Biometric System. *International Journal of Scientific & Engineering Research*.

[21] Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating Cancelable Fingerprint Templates. 561-572.

[22] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM SYSTEMS JOURNAL, 40(3)*.

[23] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM SYSTEMS JOURNAL*. IBM.

[24] Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. (2006). Cancelable Biometrics: A Case Study in Fingerprints. *The 18th International Conference on Pattern Recognition*.

[25] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *Journal on Information Security*. EURASIP.

[26] Sharma, A., & Kumar, N. (2014, April). Encryption of Text Using Fingerprints as Input to Various Algorithms. *International Journal of Science and Research*.

[27] Sonar, J., & Dahad, S. (April de 2014). A Review on Security of Fingerprint Template Using Fingerprint Mixing. *International Journal of Engineering Trends and Technology*.

[28] Zhang, X., Feng, Q., & He, K. (2014). A New Blind Fingerprint Alignment Algorithm used in Biometric Encryption. 231-234.

[29] Zhe, J., & Teoh Beng Jin, A. (2011). Fingerprint Template Protection with Minutia Vicinity Decomposition. *IEEE*.