MedCrave
Step into the World of Research

Biometrics & Biostatistics International Journal

Research Article

Open Access

CrossMark

Biometric: fingerprints protection

Abstract

Biometric template gives a reliable solution to the hassle of user authentication in identity control systems. Numerous biometric technologies have been developed and correctly deployed around the world together with fingerprints, face, iris, palm–print, hand geometry and signature. Fingerprints are the most famous because of their ease of capture, uniqueness and remains over the years, as well as the low fee and maturity of sensors and algorithms. A biometric authentication scheme with template safety this is irreversible against almost all types of adversaries. If a biometric template inside the database of the system of someone is compromised that consequently would mean identity robbery of that individual. Maximum biometric systems which are presently in use, generally use a single biometric trait to set up identity, they may be referred to as uni–modal biometric systems which have some obstacles. Assurance of biometric template is basic for acceptability in light of the potential bargain of framework security and client's protection. Similarly indispensable is examination of the security bestowed by the systems created to ensure the biometric template. A template protection scheme with provable protection and suited popularity overall performance has to this point remained elusive.

Keywords: biometric, template, fingerprints, uni–modal, acceptability

Volume 7 Issue 3 - 2018

Ashish MM,[1] Sinha GR,[2] Patel RP[3]

[1]Department of Electronics & Communication, Chhattisgarh Swami Vivekanand Technical University, India

[2]International Institute of Information Technology National Assessment and Accreditation Council and Commission, India

[3]Department of Physics, Chhattisgarh Swami Vivekanand Technical University, India

Correspondence: Ashish MM, Assistant Professor, Department of Electronics & Communication, Affiliated by AICTE, Professional Institute of Engineering & Technology, State highway 7, Vidhan Sabha Road, Murra, Raipur, Chhattisgarh 493225, Chhattisgarh Swami Vivekanand Technical University, Bhilai (CG), India, Email ashisza@gmail.com

Received: October 19, 2016 | **Published:** May 04, 2018

Introduction

For thousands of years, humans have used body characteristics such as face, voice, gait, and so on to recognize each other. In the mid–19th century, Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using various body measurements i.e. height, length of arms, feet and fingers; to identify criminals. In the late 19th century, this idea was gaining popularity; it was outshine by a far more significant and practical discovery: the distinctiveness of human fingerprints. Traditionally, user authentication is performed based on passwords something you know or tokens e.g. Smartcards something you have. These techniques are inconvenient and less secure since passwords can be forgotten or guessed and the tokens can be lost or stolen. Biometrics, on the other hand, provides a convenient means of authentication as it is based on something you are *t*hat cannot be lost or forgotten. The Government of India is implementing a system to capture and store multiple biometric traits viz. face, fingerprints and iris, from its population of more than 1 billion individuals for the purpose of issuing them a Unique Identification Number (UIN) i.e. Aadhaar Card.[1] A template is the final idea of the overall human identity and its compromise can simply lead to an identity loss. A biometric template is a digital representation of unique characteristics that have been extracted from a biometric sample of an individual. Biometric templates are known to be the identity of a person and these are used during the biometric authentication process, the matching module compares the feature set extracted during authentication with the enrolled templates and generates match scores. The decision module processes these match scores in order to either determine or verify the identity of an individual. The biometrics traits are transformed into templates by using different algorithms. A fingerprint image is typically represented as an unordered set of minutiae, which encodes the location {x,y} and orientation {è} of friction ridge discontinuities. Some well–known examples of template transformation include Bio–Hashing[2] and cancelable biometrics.[3] With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy of biometric technology. Biometric systems are being widely used to achieve reliable user authentication, a significant component in identity management. But biometric systems security is vulnerable to a number of attacks. Jain[4] proposed vulnerability in a biometric system is the leakage of biometric template information, which may lead to serious security and privacy threats. Most of the available template protection techniques fail to meet all the desired requirements of a practical biometric system like revocability, security, privacy, and high matching accuracy. The encoder contains template whose feature is extracted and codeword is appended with a key to obtain helper data. The feature transformation function or biometric cryptosystem for matching fingerprints securely is one of the important but difficult task is the design of a template protection algorithm that quantifies the security provided by the algorithm. There is still no best approach for template protection that completely satisfies the three main requirements of template security–matching, accuracy and revocability. Uludag et al.,[5] presents biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities or into one of two classes–genuine and impostor verification. A biometric system it is also susceptible to various types of threats such as: An intruder may gain access to the system protected by biometrics and peruse sensitive data such as a medical record pertaining to a legitimately enrolled is called as Circumvention, Repudiation, Coercion etc can cause denial of biometric cryptosystems can contribute to template security by supporting biometric matching in secure cryptographic domains. Smart cards are gaining popularity as the medium for storing biometric templates. There is always high risk associated with template misuse, the issue of template security and integrity continues to pose several challenges. Sun et al.,[6] presents Key–Mixed Template (KMT) mixes a user's template with a secret key to generate another form of template which is more secured. In the feature extraction process, the user given secret key should be mixed with the permanently biometric template to form a Key–Mixed–Template (KMT). The mixing function M. can mix the key–determined random vector Vi

and the template Ti as: M(Ti; Vi)=Ti+Vi. The KMT is useful when a user authorized the template is legal. This scheme is mainly designed to deal with the back end attack, spying, and tampering attacks in a certain level and could be adopted by the existing biometric systems to enhance the security of template protection. Auernheimer[7] discuss the design considerations and a prototype for a biometrics i.e. fingerprint based identification and authentication system to support web–based courses. The challenges of marrying fuzzy biometric data with cryptographic techniques that by design is sensitive to small variations using biometrics to streamline Public Key Infrastructure.[5,8] Ignatenko et al.,[9] proposes capacity of biometric enlistment successions free and decided the relating distinguishing proof limit. The exchange off between the limit of a biometric distinguishing proof framework and the capacity space pressure rate required for the biometric layouts. It focuses on recognizable proof of the same biometrics can be utilized for both confirmations what's more, ID purposes and considered biometric recognizable proof frameworks with ensured layouts. The mystery key, recognizable proof what's more; security spillage rates can be acknowledged by biometric distinguishing proof frameworks with ensured layouts that backing confirmation. It gives the idea that the bigger distinguishing proof rates we might want to accomplish, the littler mystery keys we can create and the more biometric data we need to spill. Sheng et al.,[10] states of biometric formats and/or encryption keys, as received in conventional biometrics–based confirmation strategies, has raised a matter of genuine concern. The created plan is utilized to display the client varieties on both single components and highlight subsets with the reason of recouping a substantial number of predictable and discriminative highlight components for key era. The execution of the proposed technique has been assessed on the biometric methodology of manually written marks furthermore, contrasted and existing techniques. The outcomes appear that our technique can convey steady and discriminative keys of high entropy, beating related strategies and can be utilized to create the keys with great consistency, biased, entropy and outflanking related strategies. Li et al.,[11] explains of conventional validation methods for example, passwords and token cards, biometric–based methods offer an accurate, more all inclusive and dependable alternatives for people's verification. It utilizes normal min–entropy or contingent Shannon entropy as the security metric. The difficulty in estimating statistical distribution of biometric features not only hinders the development of better template protection algorithms, but also diminishes the ability to compute the non–invertibility and non–linkability of existing algorithms has been overcome by proposed method.

Materials and methods

The wide arrangement of biometric acknowledgment frameworks over the most recent two decades has raised security concerns with respect to the capacity and utilization of biometric information. As a result, the ISO/IEC 24745 global standard on biometric data security has built up two principle necessities for ensuring biometric formats: irreversibility and unlinkability. Various endeavors have been coordinated to the improvement and examination of irreversible layouts. In any case, there is still no precise quantitative way to dissect the unlinkability of such layouts. The biometric information that is to be secured is loaded into the security machine. It is consequently absolutely critical to ensure the security of the enlisted subjects. Biometric security designs are proposed to guarantee biometric reference data in an irreversible and un–linkable way, while keeping up key structure properties like the exactness or the speed. We live in a world where information are created from a heap of sources, and it is extremely shabby to gather and capacity such information. Notwithstanding, the genuine advantage isn't identified with the information itself, yet with the calculations that are fit for preparing such information in a mediocre slip by time, and to extricate profitable learning from it. In past years, format insurance plans in view of Bloom channels have been acquainted and connected with different biometric attributes. The main substances of any fingerprint used for identification and security manage are the features it possesses.[12] Biometric cryptosystems give solid biometric security at an abnormal state. There are numerous methods that give provable security down to earth reasonable acknowledgment rates. In any case, there stay a few issues and difficulties that are being looked amid the sending of these innovations. The security of the put away biometric format is itself a test. Highlight change strategies and biometric cryptosystems are utilized to address the worries and enhance the general acknowledgment of biometrics. The motivation behind this paper is to give a diagram of various procedures and procedures for securing the biometric formats. Moreover, the paper investigates flow inquire about patterns around there. Biometric layout is typically assaulted by the assailants. Thing is helpless against assaults which cause absence of security. Biometric Security must guarantee Confidentiality, uprightness, accessibility. Diverse sorts of layout security plans like Biometric cryptosystem, Watermarking method, Intelligent approach are accessible. Biometric cryptosystem safely tie an advanced key to biometric or create a key from the biometric bringing about biometric layout insurance. Watermarking approach is the way toward installing one example into another example. Customary methods for individual distinguishing proof like ID cards and passwords are not any more adequate.

Figure 1 show flow–chart of proposed method, the process is started when sample is loaded to system. The sample is sending to feature extraction which comprises of Gabor filtering, binary image transformation, thinning of image ad minutia extraction. The template is created which is a small file derived from the distinctive features of a user's biometric data and used to perform biometric matches. Templates are created to facilitate the Storage and Matching phases during verifications. The template is encrypted by crypto sub code and encrypted template is stored in database. Biometrics is generally utilized as a part of numerous robotized verification frameworks offering a few points of interest over customary verification techniques. Since biometric components are connected with people, their spillage will damage people's security, which can bring about genuine and preceded with issues as the biometric information from a man are fundamental. On verification, sample is loaded to system and previous steps are repeated, for matching sample which is newly encrypted is searched for match from dataset in database. If sample found a message 'Match Found' is displayed and then desired operation is performed and process stops or if no match is found in database a message 'No Match Found' is displayed and process stops.[13–20] Local capabilities worldwide features are traits of the fingerprint that would be visible with the bare eye. They may be the features that are characterized by way of the attributes that seize the global spatial relationships of a fingerprint. Others are kind traces, center and delta areas. The neighborhood features also are known as Minutia points. They're the tiny, precise characteristics of fingerprint ridges which might be used for superb identity. Local features contain the statistics that is in a local area only and invariant with appreciated to international transformation. It's miles possible for two or greater impressions of the equal finger to have identical global capabilities

but nevertheless fluctuate because they've nearby features that are exclusive.

Encryption and decryption functions

Security is the procedure for altering apparent information known to as Plaintext or Message to an unreadable information referred to as Cipher–text or Cryptogram, except for the exception of from whose having the specific knowledge referred to as the Key or method this case. Encryption/decryption method, where the sender utilizes the receiver's subcode files to secure while the recipient utilizes his own private decrypt. This code cannot be retrieved by anyone who expected by one who encrypted it.[21–23]

Gabor filter

A Gabor filter is a linear filter used for edge detection in image process that is called once Dennis Gabor. Gabor filter frequency and orientation representations square measure similar to those of human sensory system, for texture representation and discrimination it has been found to be remarkably acceptable. A sinusoidal plane wave has been modulating a 2D physicist filter that is a Gaussian kernel performs within the special domain. With eight different orientations of physicist filter, features of the fingerprint square measure extracting and square measure combined.[24–30] Where f represents the ridge frequency and the choice of δx^2 and δy^2 determines the form of the filter envelope and conjointly the trade of between enhancement and spurious artifacts.. Fingerprint Recognition Using physicist Filter and Frequency Domain Filtering

$$G(x,y) = exp\left[-\frac{1}{2}\left(\frac{x^2}{\delta x^2}+\frac{y^2}{\delta y^2}\right)\right]\cos(2\pi fx) \qquad (4.1)$$

Mean square error and peak signal to noise ratio

Mean square error (MSE)

It is the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. It is average of the squares of the errors or deviations.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(Y_i^* - Y_i\right)^2 \qquad (4.2)$$

The MSE is the $\frac{1}{n}\sum_{i=1}^{n}(Y)$ mean of the $(Y_i^* - Y_i)$ square of the errors. This is an easily computable quantity for a particular sample and hence is sample–dependent. After filtering of image MSE is approximately equal to 254.

Peak signal to noise ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting or noise signal which affects the fidelity of its representation.

$$PSNR = \text{üüüüüüüü}_{10}(MAX_i) - {}_{10}(MSE)$$

When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using gray–scale with B bits per sample, MAX_i is $2^B - 1$. The Peak Signal–to–Noise Ratio in decibels for ten samples from the database is calculated and represented in form of chart. PSNR for lossy 8–bit image is 30–50dB. Acceptable values of PSNR is between 20–25dB. After applying gabor filter PSNR is approximately equal to 24 dB.

Binarization

Image binarization is the process of turning a grey scale image to a black and white image. In a grayscale image, a pixel will take on 256 completely different intensity values whereas every pixel is allotted to be either black or white in a black and white image. This conversion from gray–scale to black and white is performed by applying a threshold value to the image. In MATLAB, a value of one means that the pixel is white, whereas a value of zero indicates the pixel is black. For a gray–scale image, the pixels are decimal values between zero and one. When a threshold is applied to an image, all pixel values square measure compared to the input threshol.[31] Any pixel values below the threshold are set to 0 and any values greater than the threshold square measure set to 1. By the end of this method, all pixel values inside the image square measure either zero or one, and the image has been converted to binary format.

Thinning

Ridge Thinning is to eliminate the redundant pixels of ridges until the ridges square measure simply one pixel wide. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in every tiny image window (3x3). Finally removes all those marked pixels after many scans. In my testing, such a repetitive, parallel thinning formula has unhealthy potency though it will get associate degree ideal weakened ridge map once enough scans. The advancement of each trace step still has large computation complexness though it will not need the movement of pixel by pixel as in other cutting algorithms.[32,33]

Minutia detection

After the fingerprint ridge cutting, marking minutia points is comparatively straightforward. But it is still not a trivial task as most literatures declared because at least one special case evokes my caution throughout the point marking stage. In general, for each 3x3 window, if the central pixel is one and has specifically three one–value neighbours, then the central pixel is a ridge branch. If the central pixel is one and has solely one one–value neighbour, then the central pixel is a ridge ending.[34–36]

Results and discussion

The biometric template protection set of rules used for fingerprint safety turned into applied in these studies via the use of MATLAB 7.8.0.347 on the Windows 8.1 domestic primary working machine. The experiments have been achieved on an Intel Celeron Dual Core–2.13 GHz processor with 2GB of RAM. The purpose of the fingerprint safety experiments is to the changed algorithm beneath exclusive conditions of data as well as of the effects from the studies with effects from related works to encrypt the fingerprint database from the intruder or attacker whose is threat to the biometric template stored in database DB. The orientation estimation, ridge frequency estimation and Gabor filtering experiments all hired to generate the binary snap shots. The MATLAB's Morphological *bwmorph* operation the use of the 'thin' option became used to generate the thinned image. These results display that the ridge thickness in each of the image has been reduced to its smallest form or skeleton one pixel wide. The minutiae extraction is accomplished by ridge stop & bifurcation estimation.

Figure 3 shows the cipher–text which is generated by

cryptosubcode. Cipher text contains symbols which carry information of biometric template and is stored in database and Figure 4 shows Fingerprint_DB which is encryption (Figure 4).

Despite the fact that extensive headway has been made in security upgrade of biometrics and cryptography over the past decade, much stays to be finished. Since every single biometric methodology has its own shortcomings. It may not be sufficient to give more security that is required for all the applications. Hence, the multi–biometric models and multi variable verification frameworks, plots that all the while secure multi–biometric layouts and various validation variables merit further study. This technique could be easily used for medical or civil identification and verification, both these areas have considerable amount of frauds and miss use of once identity. In case of patient, if is checked by biometric identification there may be less event of missing any treatment by doctors or medics which is the common problem in Indian. This technique can solve issue relating to identity of persons or patients (Figure 5), (Figure 6) & (Table 1).

Table of MSE and PSNR for ten sample of fingerprint taken from DB1 database which is graphically explained in Figure 5 and Figure 6 indicates Mean Square Error (MSE) and Peak Signal to noise Ratio (PSNR) for ten samples in MatLAB.

Table 1 MSE and PSNR for ten sample of fingerprint

Samples of Fingerprints	MSE(Pixels)	PSNR(dB)
1	255	24.0654
2	254.5422	24.1003
3	254.9988	24.0654
4	254.6847	24.0879
5	254.1842	24.1656
6	254.9795	24.0658
7	254.999	24.0654
8	254.9946	24.0655
9	254.7475	24.0697
10	254.9025	24.0671

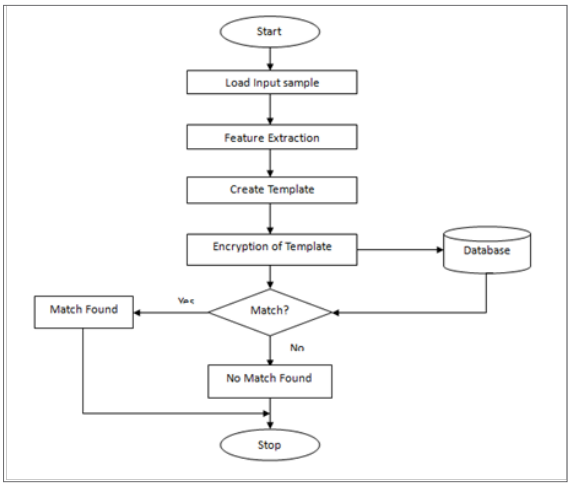

Figure 1 Flow-Chart of proposed fingerprint methodology.

Figure 2 Proposed Method on fingerprint from FVC2004 database DB1. (a) Shows input image or fingerprint from FVC2004 database–Original Image. (b) The filtered output by using Gabor filter. (c) Binary output of picture received from photo processing. (d) Image after Morphological operation thinning of input image.

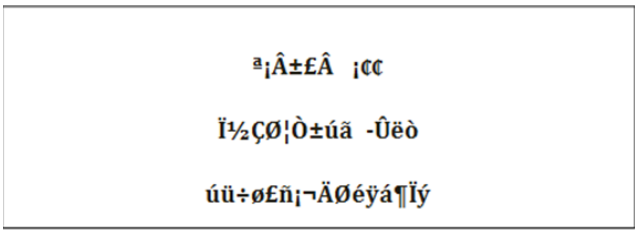

Figure 3 Secured Template.

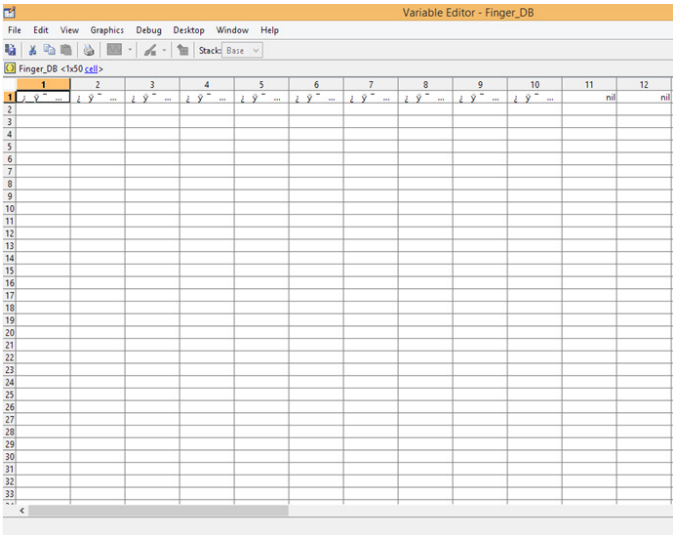

Figure 4 Secured Database.

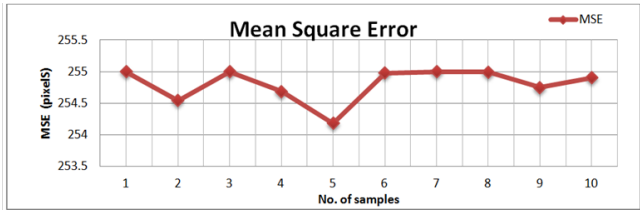

Figure 5 Mean Square Error for ten samples.

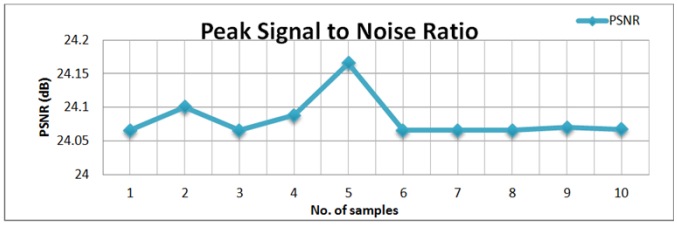

Figure 6 Peak Signal to noise Ratio for ten samples.

Conclusion

This paper discusses the results of the modification of fingerprint template protection algorithm developed and implemented in related research. Some stages of the algorithm were slightly modified for improved performance. For instance Gabor filter processing approach was introduced into the orientation estimation algorithm in place of directly finding ridge end & bifurcation estimation. The results of the experiments conducted for fingerprint template protection, ridge orientation estimation, ridge frequency estimation, Gabor filtering, binarization and thinning on synthetic and real fingerprint images is never revealed by this algorithms. Improved performance is specifically noticed for the modified ridge orientation estimation algorithm. The results obtained from the final stage of thinning show that the connectivity of the image ridge structure has been preserved and improved at each stage. A template protection scheme with provable security and acceptable recognition performance has still remained elusive.

Acknowledgements

None.

Conflicts of interest

Author declares that there is no conflict of interest.

References

1. Jain Anil K. Multibiometric Cryptosystems Based on Feature–Level Fusion. *IEEE Transactions On Information Forensics And Security*. 2012;7(1):255–268.
2. Teoh ABJ, Kar–Ann T, Wai Kuan Y. 2N Discretisation of Bio Phasor in Cancellable Biometrics. *ACM Digital library*. 2007;435–444.
3. Ratha NK, Sharat Chikkerur, Jonathan H Connell. Generating Cancelable Fingerprint Templates. *IEEE Trans on Pattern Analysis and Machine Intelligence*. 2007;29(4):561–572.
4. Jain, Anil K. Biometric Template Security. *Journal on Advances in Signal Processing*. 2008;1–17.
5. Uludag Umut, Anil K, Jain Arun Ross. Biometric Template Security: Challenges and Solutions. *EUSIPCO*. 2005.
6. Shih–Wei Sun, Chun–Shien Lu, Pao–Chi Chang. Biometric Template Protection: A Key–Mixed Template Approach. *Proceeding IEEE International Conference*. 2007;(3):1–3.
7. Auernheimer, Brent. Biometric Authentication for Web–Based Course Examinations. *IEEE Proc. of 38th Hawaii International Conference on System Sciences*. 2005;1–5.
8. Xuebing Zhou, Stephen D, Wolthusen, et al. A Security Analysis of Biometric Template Protection Schemes. *ICIAR*. 2009;(5627):429–438.
9. Sim Hiew Moi, Nazeema Binti, Puteh Saad, et al. Iris Biometric Cryptography for Identity Document. *IEEE Computer Society International Conference of Soft Computing and Pattern Recognition*. 2009;736–741.
10. Abhilasha Bhargav–Spantzel, Anna Squicciarini, and Elisa Bertino. Privacy preserving multi–factor authentication with biometrics. *Conference on Computer and Communications Security*. 2006;63–72.
11. Biometrics deployment for Machine Readable Travel Documents. NTWG; 2004.
12. Yuliang Zheng. Advances in Cryptology–ASIACRYPT. 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, Proceedings, volume 2501 of Lecture Notes in Computer Science. Springer; 2002.
13. Ashish MM, Sinha GR. Biometric Template Protection. *Journal of Biostatistics and Biometric Applications*. 2016;1(2):1–7.
14. Ashish MM, Sinha GR. Biometric Template Protection. *Research Journal of Engineering*. 2016;5(8):1–7.
15. Juels M, Sudan. *A fuzzy vault scheme. Switzerland: Proc of IEEE Int Symp Inform.* Theory, Lausanne; 2002: 408 p.
16. Abhishek Nagar, Karthik Nandakumar, Anil K Jain, et al. Multibiometric Cryptosystems Based on Feature–Level Fusion. *IEEE Xplore digital library*. 2012;7(1):255–268.
17. Anil K Jain, Karthik Nandakumar, Abhishek Nagar, et al. Fingerprint Template Protection: From Theory to Practice. *Security and Privacy in Biometrics*. 2012;1–6.
18. Donny Jacob Ohana, Liza Phillips, Lei Chen, et al. *Fingerprint Biometric Security utilizing Dongle and Solid State Relay Technology.* IEEE Xplore digital library; 2013. p.173–180.
19. Julien Bringer, Hervé Chabanne, Bruno Kindarji, et al. The best of both worlds: Applying secure sketches to cancelable Biometrics. *Science of Computer Programming*. 2008;(74):43–51.
20. Ratha NK, Connell J, Bolle RM, et al. Cancelable biometrics: A case study in fingerprints. *IEEE Computer Society*. 2016;10(10):3–6.
21. Ratha NK, Connell JH, Bolle RM, et al. Enhancing security and privacy in biometrics based authentication systems. *IBM Syst J*. 2001;40(3):614–634.
22. Ratha NK, Chikkerur S, Connell JS, et al. Generating cancelable fingerprint templates. *IEEE Trans Pattern Anal Mach Intel*. 2007;29(4):561–572.
23. Salil Prabhakar, Sharath Pankanti, Anil K Jain, et al. Biometric Recognition: Security and Privacy. *IEEE Security & Privacy*. 2003;99(2):33–42.
24. Nagar Abhishek. *Biometric Template Security.* PhD Dissertation. USA: Michigan: Michigan State University; 2012.
25. Pappu R, Garfinkel SR, Juels A, et al. RFID Privacy: An Overview of Problems and Proposed Solutions. *Electronics & Communication Engineering Journal*. 2005;3(3)3:34–43.
26. Manabe H, Sasaki R, Yamakawa Y, et al. Security Evaluation of Biometrics Authentication. *Electronics & Communication Engineering Journal*. 2009;34–39.
27. Anil K Jain, Karthik Nandakumar, Abhishek Nagar, et al. Biometric Template Security. *Journal on Advances in Signal Processing*.2008;1–17.
28. Feng Hao, Ross Anderson, John Daugman, et al. Combining Crypto with Biometrics Effectively. *IEEE Trans on computers*. 2006;55(9):1081–1088.
29. Karthik Nandakumar, Anil K Jain. Biometric Security and Privacy. *IEEE Signal Processing Magazine*. 2015;32(5):3–9.
30. Anil K Jain, Nandakumar K, Nagar, et al. Biometric Template Security. EURASIP Journal on Advances in Signal Processing. *Advanced Signal Processing and Pattern Recognition Methods for Biometrics*. 2002;7–11.
31. Rane S, Wang Y, Draper SC, et al. Secure Biometrics: Concepts, Authentication Architectures, and Challenges. *IEEE Signal Processing Magazine*. 2013;30(5):51–64.
32. Scheirer WJ, Bishop B, Boult TE, et al. Beyond PKI: The Biocryptographic Key Infrastructure. *IEEE International Workshop on Information Forensics and Security*. 201;1–8.

33. Herschel WJ. Finger–Prints. *Nature*. 1894;51(1308):77–78.

34. O Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*. 2013;91(12):2021–2040.

35. Prabhakar S, Pankanti S, Jain AK, et al. Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy*. 2003;1(2):33–42.

36. Marta Gomez–Barrero, Javier Galbally, Christian Rathgeb, et al. General Framework to Evaluate Unlinkability in Biometric Template Protection Systems. *IEEE Transactions on Information Forensics and Security*. 2017;13(6):1406–1420.