Research Journal of Engineering Sciences E- ISSN 2278 – 9472
Vol. **5(8),** 1-7, August **(2016)** *Res. J. Engineering Sci.*

Biometric Template Protection

M.M. Ashish[1*] and G.R. Sinha[2]
[1]Department of Electronics & Communication, Shri Shankaracharaya Group of Institutions, Shri Shankaracharaya Technical Campus, Junmani, Bhilai, Chhattisgarh, India
[2]Shri Shankaracharaya Group of Institutions, Shri Shankaracharaya Technical Campus, Junmani, Bhilai, Chhattisgarh, India
ashisza@gmail.com

Available online at: www.isca.in, www.isca.me
Received 4th May 2016, revised 11th August 2016, accepted 20th August 2016

Abstract

Biometric template offers a dependable approach to the trouble of user authentication in identity management structures. Various biometric technologies were developed and effectively deployed around the arena which includes fingerprints, face, iris, palm-print, hand geometry and signature. Fingerprints are the most popular due to their ease of capture, forte and patience through the years, as well as the low cost of sensors and algorithms. A biometric authentication scheme with template protection this is irreversible in opposition to almost all types of adversaries. If a biometric template inside the database of the device of someone is compromised that consequently might imply identification robbery of that man or woman. Most biometric systems which are presently in use, generally use a single biometric trait to set up identity, they're called uni-modal biometric structures that have a few obstacles. A template protection scheme with provable safety and acceptable reputation overall performance has to date remained elusive.

Keywords: Biometric, Template, Authentication, Fingerprints, Unimodal.

Introduction

For hundreds of years, human beings have used frame characteristics including fingerprint, face, voice, and gait to recognize every other. In mid nineteenth century, Alphonse Bertillon, leader of the crook identification division of the police department in Paris, developed after which practiced the idea of using numerous body measurements i.e. peak, duration of palms, toes and hands; to pick out criminals. Within the past due 19th century, this idea changed into gaining reputation; it becomes outshine by using a far more full-size and practical discovery: the distinctiveness of human fingerprints. Soon after this discovery, many essential law-enforcement departments interested in the idea of criminal's fingerprints and storing them in databases first of all in card documents. Later, police received the potential to pick up leftover normally fragmentary, fingerprints from crime scenes usually known as latent and fit them with fingerprints in the database to decide criminal's identities. Biometrics first came into enormous use for law-enforcement and legal functions identification of criminals and safety clearances for personnel in touchy jobs, paternity determinations, forensics, advantageous identifications of convicts and prisoners and so on. These days many civilian[1] and personal-zone applications are more and more the use of biometrics to establish private reputation.

With the improvement of techniques to system biometric trends in actual time, biometrics is used as a way of user authentication in programs including laptop log-in or having access to a building. Historically, person authentication is finished primarily based on passwords (something you realize) or tokens e.g. Smartcards (something you've got). Those strategies are inconvenient and much less at ease given that passwords can be forgotten or guessed and the tokens may be lost or stolen. Biometrics, however, provides a handy way of authentication as it's far based on something you are that cannot be lost or forgotten. Currently, biometric primarily based recognition structures are being drastically utilized in a wide variety of programs spanning governmental, forensic, safety and industrial sectors. The authorities of India is imposing a device to capture and shop a couple of biometric traits face, fingerprints and iris from its populace of greater than 1 billion people for the reason of issuing them a completely unique identification number (UIN) i.e. Addar Card. A standard biometric system incorporates of several modules. The sensor module acquires the uncooked biometric information of a character within the form of a photograph, video, audio or some different signal. The feature extraction module operates on the biometric sign and extracts a salient set of capabilities to represent the signal; in the course of consumer enrolment the extracted function set, categorized with the consumer's identity, is stored within the biometric device and is called a template. The matching module compares the function set extracted during authentication with the enrolled templates and generates healthy rankings[1]. The choice module methods those fit scores on the way to either determine or affirm the identity of an individual.

In all these attacks but the maximum tough and of extreme importance is the attack at the template database. A template safety is guaranteed if the transformation feature is non-invertible even if recognized to the attacker. A few famous examples of template transformation encompass Bio-Hashing[2]

and cancelable biometrics[3]. A biometric template is a digital illustration of unique traits which have been extracted from a biometric sample of a person. A template is the very last concept of the general human identification and its compromise can certainly cause an identity loss. Biometric templates are regarded to be the identification of someone and those are used at some point of the biometric authentication manner. With the sizeable deployment of biometric systems in various packages, there are increasing concerns approximately the security and privateers of biometric era. Public popularity of biometrics generation will depend on the potential of machine designers to demonstrate that these structures are strong, have low mistakes charges, and are tamper evidence.

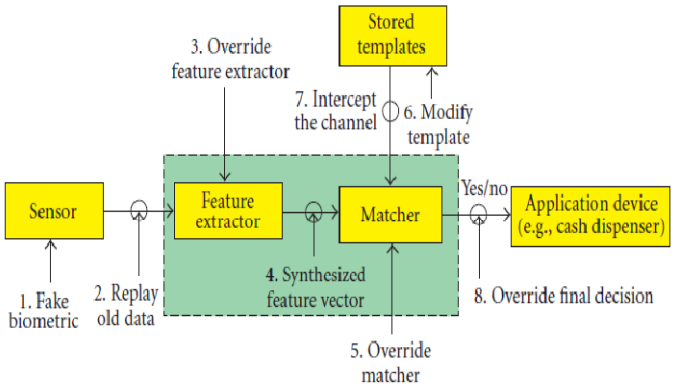

Figure-1
Vulnerabilities in a biometric machine[3]

Literature Review: Jain et al.[4] proposed vulnerability in a biometric machine is the leakage of biometric template records, which may additionally result in extreme safety and privacy threats. maximum of the to be had template protection strategies fail to satisfy all of the preferred requirements of a sensible biometric device like revocability, protection, privatives, and high matching accuracy. Due to variations in finger placement and strain applied at the sensor, there are two fundamental challenges in any fingerprint template protection scheme. First of all robotically align or sign up the fingerprints received all through enrollment and matching, without revealing excessive information about the features which uniquely signify a fingerprint. Secondly, we want to pick out the best representation scheme that captures maximum of the discriminatory facts, however is exceptionally invariant to adjustments in finger placement. The encoder carries template whose characteristic is extracted and codeword is appended with a key to achieve helper records. This helper fact is used for interpreting a template having question, feature is extracted from fingerprint and codeword is matched and get entry to be permitted or rejected to consumer. Specific implementations of three extraordinary template protection schemes on a not unusual fingerprint database were supplied to illustrate the problems concerning matching accuracy and template security. There is no best approach for template protection that completely satisfies main requirements of template security – matching, accuracy and revocability.

Uludag et al.[5] affords biometric gadget can be considered as a pattern reputation gadget whose characteristic is to classify a biometric sign into considered one of numerous identities or into one among classes - real and impostor verification. A biometric system it is also liable to diverse sorts of threats which include: an intruder may additionally benefit access to the system blanketed by using biometrics and peruse touchy statistics along with a scientific document touching on a legitimately enrolled is referred to as Circumvention. Repudiation manner a legitimate user i.e. bank clerk might also get right of entry to the centers offered through an utility and then declare that an intruder had circumvented the machine for his interest and deny responsibility by way of claiming stolen biometric facts. An outsider obtains the raw biometric information of user to get right of entry to the gadget. The latent fingerprints of a consumer can be lifted from an item by way of an interloper and used to reconstruct a virtual or bodily of person's finger is called Circumvention. A character with wide incredible-consumer privileges i.e. administrator may deliberately modify system parameters to permit attacks with the aid of an interloper such assault is referred to as Collusion. An impostor might also force a valid consumer e.g. gunpoint to furnish him access of the device then this is stated to be Coercion. Denial of service does takes place while an attacker may additionally weigh down machine assets to the point where legitimate users desiring get entry to could be refused provider. For instance, a server that processes get admission to requests may be flooded with a large wide variety of bogus requests, thereby overloading its computational sources and stopping legitimate requests from being processed.

The importance of adopting watermarking and steganography concepts is to decorate the safety of biometric templates. Biometric cryptosystems can make a contribution to template safety with the aid of assisting biometric matching in relaxed cryptographic domain names. Smart playing cards are gaining popularity as the medium for storing biometric templates. The amount of available reminiscence will increase more than 64-KByte EEPROM. There is always high threat related to template misuse, the problem of template protection and integrity continues to pose several challenges.

Sun et al.[6] offers Key-mixed Template (KMT) mixes a person's template with a secret key to generate every other shape of template that's more secured. The biometric template is been combined with a secret key to save you the returned stop assault, spying and tampering attack for a cross fit assault. Inside the feature extraction method, the person given secret key should be blended with the permanently biometric template to form a Key-blended-Template (KMT). The integration feature M (.) can mix the key-decided random vector Vi and the template Ti as: M (Ti; Vi) = Ti + Vi. The KMT is useful while a user authorized the template is legal. The key for exclusive databases ought to be set to be distinct by using the identical consumer. Let us say there are exceptional carriers incorporate two one-of-a-kind databases DB1 and DB2. Inside the

enrollment phase, the distinct key-blended-template KMT1 and KMT2 are correspondingly saved in DB1 and DB2. Think that an attacker successfully carried out a returned give up assault, snoop or tampering assault from DB1 and going to DB2 for authentication. This technique will no longer suit KMT1 for KMT2 in database DB2. Consequently, the cross in shape attack can't be successful while an authentic person who owns the permanently biometric and a secret key can achieve the robustness against the lower back stop attack, snooping, and tampering assault. Because the number of attackers in returned stop attack is restrained, involvement from specific attackers should no longer be as clean because the known plaintext attack in cryptography and extra secured than it. The key and KMT generation are the additional essential operations, which may be incorporated to the prevailing biometric structures without difficulty. This scheme is mainly designed to address the back stop assault, spying, and tampering attacks in a positive degree and might be followed via the present biometric structures to decorate the security of template safety.

Auernheimer et al.[7] discuss the layout issues and a prototype for a biometrics i.e. fingerprint primarily based identification and authentication machine to help internet-based totally publications. A typical method to identifying college students proceeding to take an online examination is to reserve a pc lab and lease a proctor to test scholar identification playing cards. Proctor may be bribed and identity cards may be forged or greater often forgotten. Within the case of a student's impostor taking an exam, the consumer is actively seeking to souse borrow his or her identification. BioAPI is intended to offer an excessive-level regularly occurring biometric authentication model; one applicable for any shape of biometric technology. It covers the primary functions of Enrollment, Verification, and identity, and consists of a database interface to allow a biometric provider issuer (BSP) to manage the identification populace for optimum performance. The biometrics may be most beneficial to on line college as identification, not as authentication however to increase a biometric authentication system useful for on-line education, well matched with college way of life and tolerance for risk and modestly demanding to present procedures. This scheme hopes to decrease possibilities for social engineering exploits.

Nandakumar et al.[8] proposed a cryptography scheme to reap facts security, the principle challenges in cryptosystems is to maintain the secrecy of the cryptographic keys. Even though biometric authentication may be used to make sure that simplest the lawful consumer has access to the name of the game keys, a biometric system itself is vulnerable to a number of threats via intruder. It presents a computerized implementation of the fuzzy vault scheme primarily based on fingerprint trivialities as fuzzy vault shops simplest a converted model of the template, aligning the question fingerprint with the template is a hard undertaking. The keys are typically saved in an ease vicinity e.g., tamper-resistant hardware and password-primarily based authentication is usually used for controlling get right of entry to cryptographic keys Fuzzy vault[9]. It proposes implementation a completely computerized and practical fuzzy vault machine based totally on fingerprint minutiae that may without problems at ease secrets and techniques consisting of 128-bits AES encryption keys. the principle task within the implementation of a fingerprint-based totally fuzzy vault is the alignment of the query with the converted template saved in the vault and to cope with versions in the biometric statistics along with the ability to paintings with unstructured sets, that is generally encountered in biometrics and makes the fuzzy vault scheme a promising answer for biometric cryptosystems. Those attributes may also be included into the bushy vault framework. The addition of latest attributes will not increase the number of feasible chaff points which can introduced to the vault however additionally decrease the decoding complexity for actual users and decrease the false errors fee. The dilemma of the fuzzy vault framework is its dependence on chaff factors to reap safety so fuzzy structures that don't contain chaff points can be taken into consideration.

Nagar et al.[10] offers an implementation of characteristic-degree fusion framework using two well-known biometric cryptosystems, viz. fuzzy vault and fuzzy dedication. It has certain analysis of the transaction between matching accuracy and security in multi-biometric cryptosystems based totally on unique databases one actual and one digital multimodal database. The database contains three most popular biometric modalities viz. fingerprint, iris and face[11]. Experimental outcomes show that both the multi-biometric cryptosystems proposed right here have higher protection and matching performance compared to uni-biometric opposite numbers. Non-invertibility to relaxed template, it ought to be computationally difficult to find a biometric feature set to be able to match with the given template and Revocability to at ease templates generated from the equal biometric records, it have to be computationally difficult to perceive that they are derived from the identical records or reap the unique biometric information. It consciousness on the biometric cryptosystem approach for multi-biometric template protection to well-known biometric cryptosystems i.e. fuzzy vault and fuzzy dedication are available for securing exclusive forms of biometric functions and relatively clean to research the safety of a comfy caricature by controlling on the characteristics of mistakes correcting codes[11]. It characteristic-level fusion framework for multi-biometric cryptosystems that includes three primary modules: embedding algorithm, fusion module and biometric cryptosystem.

There some crucial problems that might be investigated similarly: Embedding schemes for remodeling one biometric illustration into some other, at the same time as preserving the discriminative strength of the authentic illustration; a higher feature fusion scheme to generate a compact multi-biometric template that retains maximum of the facts content inside the individual templates; techniques to enhance the safety evaluation by means of as it should be modeling the biometric characteristic distributions; and evaluation of the proposed cryptosystem on large multimodal databases. The difficulty of a

multi-biometric system is that it's far viable for an adversary to get successfully authenticated by using spoofing only a subset of the concerned biometric developments. An easy way to satisfy this requirement is to do not forget the given biometric function vector i.e. minutiae set as a primary representation and derive the secondary representation by making use of a noninvertible transformation.

Ohana et al.[12] provides an alternative to biometric authentication cellular phones use a password, PIN, or visual pattern to secure the Smartphone. With those styles of safety methods being used, there's lot vulnerability. Biometric security systems have been researched for decades. A few cellular manufacturers have implemented fingerprint scanners into their telephones, inclusive of the contemporary Motorola and the old Fujitsu F505i[13]. Fingerprint reputation might also seem to be a bit more comfy because a fingerprint is extremely specific and hard to mimic. It turned into conducted using an outside USB optical fingerprint sensor and the use country wide Institute of requirements and technology Biometric picture software. 2D code affords an extra effective safety protocol and QR codes are extra reliable and secure. It proposes a blended technique of each fingerprint and voice reputation for biometric authentication. The concept at the back of this studies changed into that 3 seconds become coded into the mobile phone's database the use of a VOCODER. Once the voice was digitized, new enter was as compared to preceding recordings for verification. A phoneme is the smallest unit of sound to shape differences among utterances. A phoneme is likewise very precise and therefore most effective a small component ought to be recorded for reference. In assessment to unbiased authentication systems consisting of face, fingerprint, and voice popularity, different strategies were proposed to involve all three and extra. Gait recognition essentially verifies authentication routinely through the manner someone walks. In instances in which a user isn't walking, a PIN could be required instead. This approach is unobtrusive because it is continually recording and amassing statistics without the person having to make any bodily inputs. For gait reputation to achieve success, three techniques were used: device vision primarily based, ground Sensor. Biometric authentication standards should be applied to save you intrusions and robbery in opposition to cell gadgets.

To shield these vital belongings, a gadget other than PIN or password verification should be used due to the fact cellular telephones are misplaced or stolen on an everyday foundation. The biometric authentication is a higher alternative even though must be mixed with other generation to create better protection. Most people of faces, voices, and fingerprints are not duplicated until replicated, best bad component to organic and physiological identification is that biometric patterns cannot be revoked. It approach biological key can't be changed or altered, if a protection device containing biometric keys changed into breached, identity theft and different identity crimes should arise. Many special independent techniques, replications of faces, voices, and fingerprints may be used to obtain authorization illegally. In other words, if a mobile telephone is only protected by biometrics, it is able to still be resold and used as soon as its miles wiped smooth. A few impartial commercial enterprise proprietors even want to take cell telephones and flash them underneath every other issuer to get right of entry to a marketplace that isn't commonly to be had. It is critical to observe that this utility may be applied for any tool that requires strength. If the gadget is separated from its strength source and any other energy source can't be duplicated without a key or hardware protection tool, the gadget may be futile.

Bringer et al.[13] proposed of cancelable biometrics and cozy sketches were added with the cause to guard privatizes of biometric templates while retaining the potential to healthy this covered records against a reference photo. It's far to carry out an irreversible transformation over pix and to make matching over converted photo. A drawback of this method is that for biometrics using an identical set of rules counting on some complicated characteristics despite the fact that cancelable biometrics[14] were added with similar objectives to biometric secure sketches, i.e. to restrict the privations threats rose via biometric authentication, the strategies are incredibly adverse. The concept is to transform biometric records with an irreversible transformation and to carry out the matching immediately on the transformed information. The gain pointed out[14-16] is the functionality of using current characteristic extraction and matching algorithms. However, the principle disadvantage is that, with classical matching algorithms, the overall performance quick decreases when the transformation breaks the structure of biometrics.

Prabhakar et al.[17] speak approximately a biometric system of a pattern-recognition gadget acknowledges a person primarily based on a function vector derived from a selected physiological or behavioral feature that the individual possesses. Relying on the application context, a biometric machine commonly operates in one among two modes: verification or identity. In verification mode, the machine validates a person's identification by means of comparing the captured biometric characteristic with the individual's biometric template, which is pre saved inside the system database. In place of launching a brute-force assault, a hacker might use a very precise goal and present the device with a duplicate of a known man or woman's biometric pattern. InterGov reports that insiders commit approximately 80 percent of all cybercrimes an evaluation primarily based best on stated safety breaches. The man or woman breaching the system's protection very likely knows a licensed user personally, can acquire a pattern biometric i.e. a latent fingerprint & can make a duplicate such as a three-dimensional mildew of the fingerprint and gift it to the biometric machine. A personal reputation gadget design ought to include many biometric and non biometric additives. Biometric-based structures also have boundaries with detrimental implications for a system's protection. The accuracy of present day biometric structures isn't best, and tricky spoofing attacks can defeat a practical biometric device.

Even the evolution of biometric era has overcome some of those limitations, it is vital to understand that foolproof non-public recognition structures truly do not exist—and perhaps in no way will. Protection is a threat-control strategy that identifies controls, eliminates, or minimizes unsure occasions that can adversely have an effect on system sources and statistics assets. A system's security requirements depend upon the application's necessities of the hazard mode and the value-advantage analysis.

Methodology

The biometric information that is to be secured is loaded into the security machine. The main substances of any fingerprint used for identification and security manage are the features it possesses. The functions exhibit orientation from fingerprint to fingerprint and they may be labeled into global and 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. International functions consist of ridge sample, type, orientation, spatial frequency, curvature, position and matter. 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 2 or greater impressions of the equal finger to have identical global capabilities but nevertheless fluctuate because they've nearby features that are exclusive.

Function Extraction: The photograph is filtered by the usage of Gabor Filters to discard redundant channels for grey image. The photo is modified to binary shape and Morphological operations on binary photo the use of operation 'skinny' which remove pixels so that an object without holes shrinks to a minimally connected stroke, and an object with holes shrinks to a hoop halfway among the maintain and outer boundary. Minutiae extraction is performed via ridge stop finding & bifurcation finding.

Encryption: In encryption based techniques, the biometric template is encrypted the use of key, likely derived from a password, for the duration of enrolment. On this paper a new approach of string re-arrangement is implemented to at ease the template. During authentication, the stored information is decrypted the usage of the corresponding decryption key and is matched with the captured query. For the reason that encryption key may be discarded after constructing the comfortable template, the adversary might not be able to update the present encrypted templates even supposing he steals the decryption key. the primary barriers of encryption primarily based strategies is insecure key control for the reason that decryption secret's exposed to the machine for the duration of each try to authenticate and thus may be without problems stolen by using the adversary. The advantage is that any sophisticated matching process may be hired thereby maintaining the matching accuracy.

Template transformation: The template is transformed the use of the user's password and at some point of authentication, the query is also converted using the equal password before being matched with the transformed template. the main advantage of template transformation techniques is that if the person transforms his biometric on a separate private device and sends only the transformed template to the biometric machine, the unique biometric is never revealed inside the device. This is because the transformation generally ends in a lack of discriminative statistics available in the biometric records.

Database Enrollment: The template stored in facts base is transformed to encrypted shape that's simplest retrieved via decryption process best known to user & mere symbols for different. The statistics base stores values of templates in form of cipher text.

ª¡Â±£Â ¡¢¢

Ï½ÇØ¦Ò±úã -Ûëò

úü÷ø£ñ¡¬ÄØéÿá¶Ïý

Figure-2
Encrypted information in Database

Matching: The template authentication is finished by consumer transforms & biometric on a separate private tool and sends most effective the transformed template to the biometric device, the authentic biometric is by no means revealed within the gadget and therefore biometric template stays safe.

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 eight.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. 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 'skinny' 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(a)

Figure-3(b)

Figure-3(c)

Figure-3(d)

Figure-3(a) is the chosen fingerprint from FVC2004 fingerprint database DB1. Figure-3(b) is the filtered output by using Gabor filter. Figure-3(c) is binary output of picture received from photo processing. Figure-3(d) is image after Morphological operation the use of the 'skinny' recognized thinning of photo.

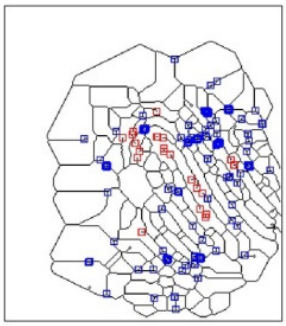

Figure-4
Minutiae Extraction

Figure-4 shows Minutiae extraction is done by ridge end finding & bifurcation finding. This operation remove pixels from Morphological processed thin image so that an object without holes shrinks to a minimally connected stroke, and an object with holes shrinks to a ring halfway between the hold and outer boundary & Figure-5 shows Matching of fingerprint with saved secured template in database.

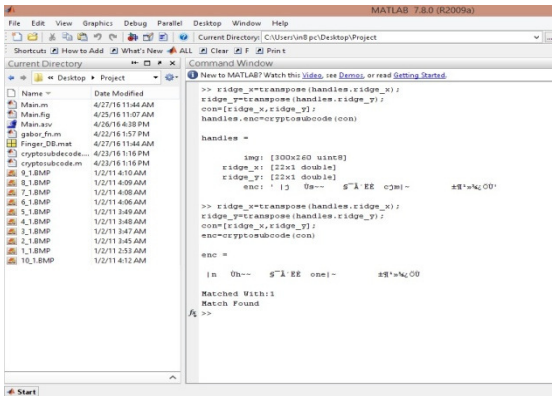

Figure-5
Matching of fingerprint

Conclusion

This paper discusses the results of the change of fingerprint template safety algorithm advanced and applied in related research and few levels of the algorithm were slightly changed for improved overall performance. For instance Gabor filter processing approach becomes brought into the orientation estimation algorithm in area of at once finding ridge end & bifurcation estimation. The effects of the experiments performed for fingerprint template safety, ridge orientation estimation, ridge frequency estimation, Gabor filtering, binary image processing and thinning on actual fingerprint data is by found out by this algorithm. The consequences acquired from the very last level of thinning display that the connectivity of the image ridge structure has been preserved and progressed at each level. A template safety scheme with provable protection and suitable recognition performance has nevertheless remained elusive.

References

1. Nagar Abhishek, Karthik Nandakumar and Jain Anil K. (2012). Multibiometric Cryptosystems Based on Feature-Level Fusion. IEEE Transactions on Information Forensics And Security, 7(1), 255-268, ISBN: 1556-6013.

2. Teoh A.B.J., Toh K.A. and Yip W.K. (2007). 2N Discretisation of BioPhasor in Cancellable Biometrics. Proc. Second Intl. Conf. on Biometrics, Seoul, South Korea, 435-444.

3. Ratha N.K., Chikkerur S., Connell and Bolle J.H. (2007). Generating Cancelable Fingerprint Templates. *IEEE Trans on Pattern Analysis and Machine Intelligence*, 29(4), 561-572.

4. Jain Anil K., Nandakumar Karthik and Nagar Abhishek (2007). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, Hindawi Publishing Corporation, 2008, Article ID 579416, 2-8, doi:10.1155/2008/579416.

5. Ross Arun, Umut Uludag and Anil K. Jain (2005). Biometric Template Security: Challenges and Solutions. Signal Processing Conference, 2005, 13th European http://biometrics.cse.msu.edu.

6. Shih-Wei Sun, Chun-Shien Lu and Pao-Chi Chang. (2007). Biometric Template Protection: A Key-Mixed Template Approach. Proceeding IEEE International Conference, Ch3, pp1-3, ISBN :1-4244-0763X/07, http://vaplab.ee.ncu.edu.twenglishpcchangpdfc75.

7. Brent Auernheimer and Max J. Tsai. (2005). Biometric Authentication for Web-Based Course Examinations. IEEE Proc. of 38th Hawaii International Conference on System Sciences, 1-5.

8. Karthik Nandakumar, Jain Anil K. and Pankanti. Sharath (2007). Fingerprint-Based Fuzzy Vault: Implementation

and Performance. *IEEE Trans. On Information Forensics and Security*, 2(4), 744-751.

9. Juels and Sudan M. (2002). A fuzzy vault scheme. Proc. of IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, 408.

10. Nagar Abhishek, Nandakumar Karthik and Jain Anil K. (2012). Multibiometric Cryptosystems Based on Feature-Level Fusion. IEEE Trans. On Information Forensics and Security, 7(1), 255-268.

11. Jain Anil K., Nandakumar Karthik and Nagar Abhishek (2012). Fingerprint Template Protection: From Theory to Practice, Security and Privacy in Biometrics. P. Campisi edition, Springer, 1-6.

12. Ohana Donny Jacob, Phillips Liza and Chen. Lei (2013). Fingerprint Biometric Security utilizing Dongle and Solid State Relay Technology. IEEE Security and Privacy Workshops, 173-180, DOI 10.1109/SPW.2013.19.

13. Bringer Julien, Chabanne Hervé and Kindarji Bruno (2008). The best of both worlds: Applying secure sketches to cancelable Biometrics. Science of Computer Programming, (74) 43-51, http://www.ac.els-cdn.comS01676423080012631-s2.0-S0167642308001263-main.pdf.

14. Ratha N.K., Connell J., Bolle R.M. and Chikkerur S. (2006). Cancelable Biometrics: A case study in fingerprints. IEEE Computer Society, ICPR (4), 3-6.

15. Ratha N.K., Connell J.H. and Bolle R.M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.*, 40(3), 614-634.

16. Ratha N.K., Chikkerur S., Connell J.H. and Bolle R.M. (2007). Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4), 561-572.

17. Prabhakar Salil, Pankanti Sharath and Jain. Anil K. (2003). Biometric Recognition: Security and Privacy. IEEE Security & Privacy, 540-7993/03.

18. Nagar Abhishek (2012). Biometric Template Security. Ph.D Dissertation. Michigan State University.

19. Pappu R., Garfinkel S.L. and Juels A. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions. *Electronics & Communication Engineering Journal*, 34-43.

20. Manabe H., Sasaki R., Yamakawa Y. and Sasamoto T. (2009). Security Evaluation of Biometrics Authentications for cellular phones. *Electronics & Communication Engineering Journal*, 34-39

21. Jain Anil K., Nandakumar Karthik, and Nagar. Abhishek (2008). Biometric Template Security. Hindawi Publishing Corporation, *EURASIP Journal on Advances in Signal Processing*.

22. Hao Feng, Anderson Ross and Daugman. John (2006). Combining Crypto with Biometrics Effectively. IEEE Trans on computers, 55(9), 1081- 1088.

23. Nandakumar Karthik and Jain. Anil K. (2015). Biometric Template Protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), 88-100.

24. Jain A.K., Nandakumar K. and Nagar A. (2012). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing*, Special Issue on Advanced Signal Processing and Pattern Recognition Methods for Biometrics, 7-11.

25. Rane S., Wang Y., Draper S.C. and Ishwar P. (2013). Secure Biometrics: Concepts, Authentication Architectures, and Challenges. *IEEE Signal Processing Magazine*, 30(5), 51–64.

26. Scheirer W.J., Bishop B. and Boult T.E. (2010). Beyond PKI: The Biocryptographic Key Infrastructure. IEEE International Workshop on Information Forensics and Security, 1-8.

27. Herschel W.J. (1894). Finger-Prints. *Nature*, 51(1308), 77-78.

28. O'Gorman L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

29. Prabhakar S., Pankanti S. and Jain A.K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy*, 1(2), 33-42.