International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Multibiometric Template Security Based on Fuzzy Behavior

Praveer Tigga[1], Akash Wanjari[2]

[1, 2]Computer Science Engineering (Information Security), DIMAT Raipur, C.G., India

Abstract: ***Biometric authentication has evolved from the disadvantages of ancient means that of authentication. The templates have the danger of outflow of user privacy and system security. Multibiometric templates can jointly has to be protected because it contains info of multiple traits of one person so the danger of outflow of knowledge and intrusion attack will increase, therefore it becomes necessary to guard multiple templates. The objective of this work is to secure the templates before storing it to the information so as to beat the intrusion attack and guarantee users privacy. In this work basically two biometric template were used for the cryptosystem. The functionality of the system comprises of feature extraction where features of individual template extracted after that embedding is done on the various features, codeword generation generates the code for each feature of the template this codeword along with predefined keys and with hashing completes the architecture of the system. Lastly, on analysis with various experiments it is found that our implementation, the genuine accept rate is 99% with lesser security bits.***

Keywords: Fuzzy Biomatric Cryptosystem, Fuzzy Commitment, Fuzzy vault.

1. Introduction

Biometric refers to acknowledge the identity of an individual supported physiological or activity characteristics of the topic [1]. A generic biometric system operates by taking associate input from the user, preprocessing the signal to de noise it to seek out the region of interest, extracting options, and authenticating a personal supported the results of comparison. Biometric example protection is to secure the templates before storing it to the information so as to beat the intrusion attack and guarantee users privacy. Biometric cryptosystem is that the combination of cryptography and biometry to reinforce the protection as misuse of biometric knowledge may be avoided by exploitation cryptosystem.

In fuzzy commitment theme a random secret's generated that is of length L and is employed to index a codeword c that has error tolerance [13]. The hash worth of the secret's additionally hold on. This codeword is then XORed with the example which ends up in an exceedingly secure sketch. throughout authentication a biometric example is given as a input and a replacement codeword is made and additional secret's generated. If the hash worth of each the keys are identical, the person is authentic. In fuzzy vault [14], a polynomial is made and this typically secures the biometric options that are purpose set. Here security entirely depends on the infeasibility of the polynomial reconstructions downside. Protection of multibiometric templet could be a necessity because the run of knowledge will cause intrusion attacks a lot of.[15] essentially templet protection theme is of 2 sorts specifically biometric cryptosystem and have transformation. For feature transformation biohashing is that the example that comes underneath seasoning and seasoning is that the classification of feature transformation.

The planned system[5], for the feature-extraction stage is predicated on feedback path. subsequently feature-refinement is performed thus on improve the matching performance. The Dennis Gabor filter is applied to the input image to boost its quality. This method improves the matching performance of the biometric system. F.Yang [8] have projected a multimodal system taking options of fingerprint, palm print and hand pure mathematics. These life science are taken from the identical image. first off fusion of fingerprint and palm print is performed at matching score level and so matching score fusion between multimodal system and unimodal system i.e. hand pure mathematics is performed. this provides higher results.

F Besbes [7] projected a multimodal system combining finger print and iris. call is taken into account from every modality and so finally combined by "AND" operator. victimization AND operator suggests that if each the conditions are true then solely the result are all over as true. If each the biometric modalities are real then the result are real. Y. J. chin [6] have projected a hybrid temple protection theme that is dole out in three stages. First off feature level fusion is performed. In second stage random feature set is generated and in third stage temple bit string is obtained. This ensures that revocable and heterogeneous templates are generated.

Rest of the paper is organized as follows in section II we discuss about the face recognition through templates. Section III briefs about iris templates and their features. Methodology of the proposed system is discussed in section IV. Experimental study and result analysis have been discussed in the section V. Last section throws light on the conclusion and future scope of the work.

2. Face Recognition Through Template

Recognition is a term that includes several sub-problems. The input of a face recognition system is always an image or video stream. The output is an identification or verification of the subject or subjects that appear in the image or video. A face recognition system as a three step process. 1) Face Detection 2) Feature Extraction 3) Recognition . From this point of view, the Face Detection and Feature Extraction phases could run simultaneously.

Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face. Face detection procedure has many applications like face tracking, pose estimation or compression. The next step -feature extraction- involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not. This phase has other applications like facial feature tracking or emotion recognition. Finally, the system does recognize the face. In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure. This phase uses methods common to many other areas which also do some classification process -sound engineering, data mining et al. These phases can be merged, or new ones could be added. Therefore, we could find many different engineering approaches to a face recognition problem. Face detection and recognition could be performed in tandem, or proceed to an expression analysis before normalizing the face

3. IRIS Recognition Through Template

Biometric ways supported iris pictures area unit believed to permit terribly high accuracy, and there has been an explosion of interest in iris bioscience in recent years. Pupil is that the darkest circular formed space within the eye image. Pupil controls the number of sunshine getting into the attention by dilation and contraction. Iris is circular formed that separates pupil from the sclerotic coat region. Recent authentication systems want secure, quick and correct computing that iris pattern is found to be appropriate. Iris is captured while not co-operation of the topic. This marks the quality of iris recognition conjointly for criminal identification. Iris biometric system involves challenges of automating the system to spot the region of interest, finding helpful feature(s) from the region of interest, matching options once a question comes, maintaining feature sets appreciate each registered subject within the info etc. of these segments area unit freelance analysis areas and forms an authentication system once deployed along.

4. Methodology

The scope of the present analysis from the literature survey and came to understand the way to create a system that might give higher security to the multibiometric templates, therefore we will currently proceed any for implementation section and understand its importance in simulation setting. This work involves extracting the options from totally different biometric attribute i.e. iris and face and so fusing it with random permutation. Finally securing it with biometric cryptosystem. Our work chiefly focuses on securing the biometric templet mistreatment fuzzy extractor by taking 2 biometric traits fingerprint and iris by considering solely the binary values and not purpose set and not mistreatment secret share module as in however mistreatment helper information extraction.

A. Fuzzy Extractor

A secure sketch addresses the matter of error tolerance. it's a (probabilistic) operate outputting a public worth v concerning its biometric input w, that, whereas revealing very little concerning w, permits its precise reconstruction from the other input w0 that's sufficiently shut. the value for this error tolerance is that the appliance can need to work with a lower level of entropy of the input, since business v effectively reduces the entropy of w. However, in an exceedingly smart secure sketch, this reduction are tiny, and w can still have enough entropy to be helpful, though the opposer is aware of v. A secure sketch, however, doesn't address unsimilarity of inputs. A fuzzy extractor addresses each error tolerance and unsimilarity.

B. Fuzzy Commitment

Fuzzy commitment is meant to realize a replacement property referred to as as “fuzziness”. This suggests the commitment theme ought to be resilient to corruption values i.e. given any operate with the input w then the ought to settle for very little variances if the input given at the time of verification i.e. x’ is shut enough to x. In fuzzy commitment theme a random secret's generated that is of length L and is employed to index a codeword c that has error tolerance. The hash price of the secret's additionally hold on. This codeword is then XORed with the model which ends up in an exceedingly secure sketch. throughout authentication a biometric model is given as a input and a replacement codeword is created and additional secret's generated. If the hash price of each the keys square measure identical, the person is authentic.

C. Cryptosytem with Fusion

For securing the templates fuzzy extractor and fuzzy commitment is employed. 1st 2 biometric traits area unit given as input. Options area unit extracted from the traits. The 2 biometric attribute used area unit face and iris. once feature extraction of iris and face embedding algorithms area unit applied thus on create them homogenized. Within the embedding half random fusion is applied. Fusion is that the feature level fusion. Once fusion code generation is being done that is finished by fuzzy extractor that uses fuzzy commitment? Using this, a codeword is generated that is additionally known as helper knowledge. this is often encrypted with a key that is named as a multibiometric secure sketch and hold on within the info in conjunction with the hash worth of the key hash worth is generated victimization md5 (Message Digest 5) . Throughout verification section, once feature extraction of iris and fingerprint, same method is applied. Code is generated and bit error rate is given. within the key generation the key's regenerated and if the hash worth of the key's same then the user is claimed to be real otherwise trickster. This is often the summarization of the full work.

D. Embedding and fusion

The embedding formula transforms a biometric feature illustration into a replacement feature illustration. In our implementation the output illustration ought to be a binary string. In embedding algorithms conversions of the numbers to binary are done. To get a consolidated template, the fusion module combines a collection of undiversified biometric options. Fusion are often classified in three categories.

- Feature level fusion:- once feature extraction the options area unit consolidated.

- Score level fusion:- once matching a similarity score is obtained then the fusion takes place.
- Call level fusion:- during this the resultant vector is classed in a pair of selections either settle for or reject.

E. Codeword Extraction

Fuzzy extractor could be a biometric tool that is employed to get a codeword with the assistance of fuzzy commitment. this can be generated with the assistance of a secure sketch. we've got seen that the "fuzzy-commitment" construction of Juels and Wattenberg [13] supported error correcting codes are often viewed as a (nearly optimal) secure sketch. Then the results area unit applied to convert it into an almost best fuzzy extractor. playacting distance is employed for the development of fuzzy extractor. The output of the codeword extraction is that the solely helper information extraction. As this information is currently shuffled and also the entrant won't be able to observe whose information it's. Fuzzy extractor merely means that planning a system that accepts randomness. In our implementation it accepts until zero.5. Same within the commitment theme. during this additionally theme ought to be resilient to corruption values i.e. given any perform with the input w then the ought to settle for very little variances if the input given at the time of verification i.e. w' is shut enough to w.

F. Key Genration

Key generation is completed to form the sketch safer. Cryptosystem is combined with statistics to confirm a lot of security. The key's binded with the sketch. it's a very important step in biometric cryptosystem. Finally the output of this can be hold on within the information with the hash price of the key. During verification section, the 3 module viz. embedding, fusion and biometric cryptosystem play a vital role. All the modules runs throughout this section, if the key matches then the user is authentic different shammer.

G. Hash Key Genration

In this phase MD5 is used for the generation of the certificate. Key generated in the earlier phase is fed into the MD5 algorithm that generates 128 bit hash key which is uniquely

5. Experimental Setup and Results

Experimental Database available from YALE dataset includes 244 images. Database from Chinese Academy of Sciences' Institute of Automation (CASIA) contains 756 iris images from 216 eyes acquired in an indoor environment. GUI has been designed for the simulation and performance analysis of the system in MATLAB 2014a. First of all features are extracted, embedding algorithm is applied, code word is generated, and during code word generation it shows the bit error rate. Further key is generated. While verifying it shows that key matched or it does not match. We evaluate the trade-off between recognition accuracy and security of the proposed multibiometric cryptosystems in case of the above database, the security of the multibiometric is of 99%.

6. Conclusion

The results obtained by implementing the proposed method to gain accuracy rate and security are upto the mark. We have proposed a feature-level fusion framework for the design of multibiometric cryptosystems that simultaneously protects the multiple templates of a user using a single secure sketch. The feasibility of such a framework has been demonstrated using fuzzy extractor, which is a well-known biometric cryptosystem. We have also proposed random fusion for fusing biometric representations, and a mechanism to impose constraints such as minimum matching requirement for specific modalities in a multibiometric cryptosystem. Experiment is conducted on databases CASIA and YALE. This work demonstrates that it is indeed possible to improve both the matching performance and template security using the multibiometric cryptosystems. While demonstrating we achieved a score of 99%.

References

[1] Y. J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh, "Integrated biometrics template protection technique based on fingerprint and palm print feature level fusion". Expert Systems with Applications, Elsevier, 2014. pp-161-174.

[2] Chi Chen, chaogang Wang, Iengfei Yang, Dongdai Lin, Song Wang, Jiankun Hu "*Optional multibiometric cryptosystem based on fuzzy extractor*", Proceedings of IEEE 2014, 11th International Conference on Fuzzy Systems and Knowledge Discovery. 989-994.

[3] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[4] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proc. Sixth ACM Conf. Computer and Communications Security, Singapore, Nov. 1999, pp. 28–36

[5] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data cryptology ePrint Archive, Tech. Rep. 235, Feb. 2006, A preliminary version of this work appeared in EUROCRYPT 2004

[6] A.K. Jain, K. Nandakumar, A. Nagar, "Biometric Template Security". EURASIP journal on advances in signal processing, 2008

[7] H. Sung, J. Lim, J. Park, and Y. Lee. Iris recognition using collarette boundary localization. In *17th International Conference on PatternRecognition*, volume 4, pages 857–860, 2004

[8] F. Yang, B.MA, "A new mixed mode biometrics information fusion based on fingerprint, hand geometry and palm print". Proceedings 4th International IEEE Conf. Image Graph, 2007, pp- 689-693.

[9] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on Fingerprint identification and iris recognition" in proceedings 3rd International IEEE conf. Inf. Communication technology. ICITA 2008, pp-1-5.

[10] S. Cimato, M. Gamassi, V. Piuri, R. Rassi, and F. Scotti, "Privacy-aware biometrics: Design and Implementation of a multimodal verification system" in proc. IEEE annual conference Computer Security Applications, 2008.

[11] Peng Li, Xin Yang, Hua Qiao b, Kai Cao c, Eryun Liu c, Jie Tian "An effective biometric cryptosystem

combining fingerprints with error correction codes". Expert Systems with Applications, Elsevier, 2012, pp-6562–6574.

[12] Y. J. Chin, T.S. Ong, A.B.J. Teoh, K.O.M. Goh, "Integrated biometrics template protection technique based on fingerprint and palm print feature level fusion". Expert Systems with Applications, Elsevier, 2014. pp-161-174.

[13] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. IEEE 2nd Int. Conf. Biometrics: Theory,Applications, and Systems*, Washington, DC, Sep. 2008.

[14] Abhishek Nagar, Anil k. jain, Karthik nandakumar, IEEE Transaction on Information Forensics and Security, Vol 7, 2012, "Multibiometric Cryptosystems based on feature level fusion".