Cancelable knuckle template generation based on LBP-CNN

Avantika Singh[1], Shreya Hasmukh Patel[2], and Aditya Nigam[1]

[1] Indian Institute of Technology Mandi, India,
d16027@students.iitmandi.ac.in,aditya@iitmandi.ac.in
[2] Indian Institute of Technology Jodhpur, India, hasmukh.1@iitj.ac.in

Abstract. Security is a prime issue whenever biometric templates are stored in centralized databases. Templates are highly susceptible to varied security and privacy attacks. Unlike passwords, biometric traits are permanently unrecoverable if lost once. In this paper efforts have been made to generate cancelable knuckle print templates. To the best of our knowledge, this is the first attempt for generating secure template for this biometric-trait. Here for learning feature representation of a biometric sample, local binary pattern based CNN is used. The experimental results are evaluated on PolyU FKP knuckle database and demonstrate high performance. The proposed protected template is resilient to various privacy attacks as well as it satisfies one important criteria of cancelable biometrics i.e. revocability.

Keywords: cancelable biometrics · knuckle-print · bio-hashing.

1 Introduction

Among the three major personnel security mechanisms, which are based on either password, token or biometric scheme, appears to be insufficient in addressing the challenges of identity frauds. Passwords and pins are easily forgotten or cracked, whereas biometric traits suffer from the privacy assault and non-revocable issues. It simply means, if a biometric is compromised, it is rendered worthless, just like a password or pin. In such circumstances, replacement of a biometric trait with new template is not reasonable, as a person has only limited set of biometric samples. To address these critical issues, the concept of cancelable biometrics was emerged few years back that replaces the raw biometric template as a mixture of user-defined random values with biometric features [2, 7]. Nevertheless, biometric modalities have been proved to carry unique biological information of an individual than any of the conventional passwords or token based methods. Although the use of biometrics is always problem specific but the good performance of finger knuckle print represents a recent trend in this field [3]. The convex shape lines and creases on finger dorsal surface are very distinctive to everyone and easily collectible using low-resolution imaging cameras [6].

Major Concerns and Contribution : The major open issues in knuckle biometrics are the lack of robustness against outdoor illumination, low image

quality, inconsistent ROI segmentation and poor matching between weaker texture regions. Also, no commercial usage of finger knuckle biometric is available till the date. To the best of our knowledge, this is the first time efforts are made to introduce knuckle modality as cancelable biometric template, where the biometric features of a finger knuckle are modified using a well known Bio-hashing technique.

2 Proposed Architecture

Local binary patterns have been widely used in the past in variety of image processing applications and surprisingly have shown tremendous success in the face recognition area. In our work we have used local binary convolution neural networks as proposed by [5] for feature extraction. The main reason for chosing this kind of convolution is its ability to reduce large number of learnable parameters in comparison to the standard convolution layer. Thus this kind of convolution can work pretty well if we have limited data set at our disposal as the case with most of the biometric applications. Our proposed architecture is shown in Fig.1. The detailed description of the LBP based CNN that is used in

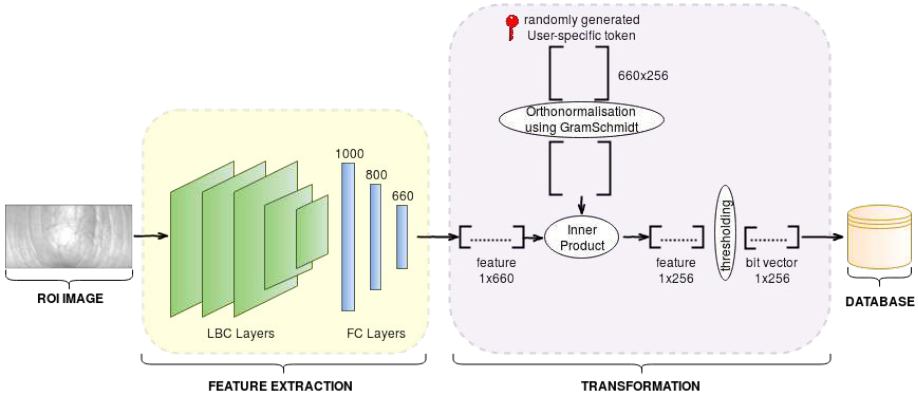

Fig. 1. Proposed architecture framework

our work is shown in Table 1. We have used Adam optimizer with learning rate 0.001 and all the implementations has been done on Intel (R) Xenon(R) CPU E5-2630 V4 and NVIDIA Tesla K40C GPU card with 12 GB on card RAM.

2.1 Cancelable knuckle template generation

Once the feature vector corresponding to a particular subject is obtained from LBP-CNN, they are transformed using the biohashing [4] technique to generate

Table 1. LBP based CNN architecture

Layer	**No of Filters**	**Size of Filters**
Conv1	8	3*3
Conv2	16	3*3
Conv3	32	3*3
Conv4	64	3*3
Maxpooling(2*2)		
Conv5	128	3*3
Maxpooling(2*2)		
Fully Connected -1000		
Fully Connected- 800		
Fully Connected-660		

cancelable knuckle template. Under this technique a user specific key is used to generate pseudo-random vectors, which are further transformed into orthonormal sets by applying Gram-Schmidt process. Then the inner product of the feature vector with the orthonormal set is computed. After that the resultant is further thresholded to generate bit-vector representation which is our cancelable template and stored in database. During authentication phase, the query image is processed through the same architecture to generate bit-vector representation which is compared with the templates stored in the databases using Euclidean distance to get the genuine match.

3 Testing Protocol and Results

To evaluate the proposed architecture, a state-of-the-art PolyU FKP database [1] which contains total $7,920$ images from 660 different fingers, has been used. We have used first 6 images for training the network and rest 6 images for testing. We have also augmented our training dataset using various parameters like rotation, brightness, zooming and distortion. By doing so, a total of 46 images are generated corresponding to each image. In this way we have total $1,82,160$ training images. Thus, we have obtained $3,960$ genuine and $26,09,640$ impostor matchings in our experimentation. In order to generate genuine score, matching is performed between an image of a subject with all other images of the same subject. On the other hand imposter score is generated by comparing an image of each subject against the images of all other subjects. The Genuine Vs Impostor score distribution graph is depicted in Fig. 2 that shows genuine and imposters are well separated with each other which is the prime requirement of any biometric based application. In this experiment, the performance comes out to be very superior i.e. FAR= 0.125 and FRR= 0.212.

4 Conclusion

In this paper, we proposed a cancelable knuckle template which is inspired from LBP-CNN and bio-hashing. Experimental results show exceptional performance

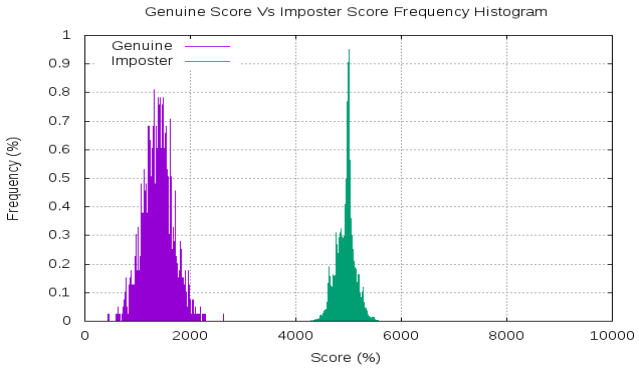

Fig. 2. Genuine vs imposter score graph

on PolyU FKP dataset. Finally, the proposed technique can potentially be extended to other biometric modalities also. Cancelable multi-biometrics is an emerging area. In future we will try to design effective non-invertible transformations for multiple biometric modalities.

References

1. Finger-knuckle-print polyu. http://www.comp.polyu.edu.hk/biometrics (2009)
2. Cho, S., Teoh, A.B.J.: Face template protection via random permutation maxout transform. In: Proceedings of the 2017 International Conference on Biometrics Engineering and Application. pp. 21–27. ACM (2017)
3. Jaswal, G., Kaul, A., Nath, R.: Knuckle print biometrics and fusion schemes–overview, challenges, and solutions. ACM Computing Surveys (CSUR) **49**(2), 34 (2016)
4. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition **37**(11), 2245–2255 (2004)
5. Juefei-Xu, F., Boddeti, V.N., Savvides, M.: Local binary convolutional neural networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition,CVPR. pp. 4284–4293 (2017)
6. Kumar, A., Xu, Z.: Personal identification using minor knuckle patterns from palm dorsal surface. IEEE Transactions on Information Forensics and Security **11**(10), 2338–2348 (2016)
7. Lai, Y.L., Jin, Z., Teoh, A.B.J., Goi, B.M., Yap, W.S., Chai, T.Y., Rathgeb, C.: Cancellable iris template generation based on indexing-first-one hashing. Pattern Recognition **64**, 105–117 (2017)