International Journal of Information Processing, 7(4), 11-20, 2013
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Enhancing Template Security of Face Biometrics by Using Edge Detection and Hashing

Manoj Krishnaswamy[a], G. Hemantha Kumar[b]

[a]Research Scholar, Department of Studies in Computer Science, University of Mysore, Mysore,
Contact: manojkrishnaswamy@gmail.com

[b]Professor, Department of Studies in Computer Science, University of Mysore, Mysore.

In this paper we address the issues of using edge detection techniques on facial images to produce cancellable biometric templates and a novel method for template verification against tampering. With increasing use of biometrics, there is a real threat for the conventional systems using face databases, which store images of users in raw and unaltered form. If compromised not only it is irrevocable, but can be misused for cross-matching across different databases. So it is desirable to generate and store revocable templates for the same user in different applications to prevent cross-matching and to enhance security, while maintaining privacy and ethics. By comparing different edge detection methods it has been observed that the edge detection based on the Roberts Cross operator performs consistently well across multiple face datasets, in which the face images have been taken under a variety of conditions. We have proposed a novel scheme using hashing, for extra verification, in order to harden the security of the stored biometric templates.

Keywords : Cancellable Biometrics, Edge Detection, Face Biometrics, Template Security.

1. INTRODUCTION

The dimensions, proportions and physical attributes of a person's face are unique. Biometric facial recognition systems will measure and analyze the overall structure, shape and proportions of the face: Distance between the eyes, nose, mouth, and jaw edges; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, the area surrounding the cheekbones. At enrolment, several pictures are taken of the user's face, with slightly different angles and facial expressions, to allow for more accurate matching. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded. Benefits of face biometric systems being that it is not intrusive, can be done from a distance, even without the user being aware of it (for instance when scanning the entrance to a bank or a high security area). Weaknesses of face biometric systems: Face biometric systems are more suited for authentication than for identification purposes, as it is easy to change the proportion of one's face by wearing a mask, a nose extension, *etc.*. Also, user perceptions / civil liberty: Most people are uncomfortable with having their picture taken. Applications of face biometrics include access to restricted areas and buildings, banks, embassies, military sites, airports, law enforcement.

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancellable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by N K Ratha, J H Connell and R M Bolle [1].

Several methods for generating cancellable biometrics have been proposed. The first fingerprint based cancellable biometric system was

Table 3
Recognition Accuracy of Face Recognition Methods of IFD Dataset and Variants

Accuracy (%) (Recognition Rate)						
Classifier	Dataset					
	IFD	IFD-L	IFD-S	IFD-R	IFD-F	IFD-P
ICA	76.7	76.3	75.4	78.0	75.0	75.0
IPCA	76.7	86.0	86.9	86.0	86.0	86.4
LDA	**91.1**	**89.8**	**89.8**	**89.8**	**89.4**	**89.0**
PCA	76.3	72.0	76.3	75.8	76.7	77.1

Also, by varying the convolution kernel values of the Robert's filter gradient, more cancellable templates can be generated for a particular face image, as discussed for difference of gaussian edge filter by G. Hemantha Kumar and Manoj Krishnaswamy [20].

By storing SHA-256 hash of the stored biometric template and encrypting with AES-256 algorithm (Table 4) we have provided a strong measure against biometric template tampering. SHA-256 hashing and AES-256 cipher can be performed computationally fast (less than a second) and hence can be easily incorporated into existing systems. Although we have assumed that the attacker will not be able to easily gain access on the various levels to compromise the entire system, even in case the entire system was being compromised, the cancellable templates can be re-issued which provides new hash values automatically. Due to the non-invertible nature of the templates there is no worry of misuse of lost data. Other schemes involve calculating the helper data (in our case the ciphered hash value) for each set of biometric templates which becomes time consuming during verification. The time taken to decrypt only once enhances the speed of execution and can be incorporated in systems which require speed as well as security. Useful scenarios for the proposed method could be in real time systems, banking, ATM access, *etc.*.

4. CONCLUSIONS

We have shown that the final filtered images itself can be used for face matching instead of unaltered face images. The results are checked across datasets which encompasses a wide variety of images taken under different conditions as well as different resolutions and image quality. We proposed a novel method for generating cancellable face biometrics and to secure the stored templates in a way which is suitable for integration with current face matching systems with acceptable alterations.

Also, by using fast, proven and standard hashing (SHA-256) and cryptographic (AES-256) methods for data verification, the vault is further enhanced. We discussed their strengths and shortcomings, as well as their relative performance on different databases under a variety of conditions. The approach allows for enhanced template security, privacy and maintaining good ethics in biometric systems. It is important that biometrics based authentication systems are designed to withstand different sources of attacks on the system.

REFERENCES

1. N K Ratha, J H Connell and R M Bolle. Enhancing Security and Privacy in Biometrics-based Authentication Systems, *IBM systems Journal*, 40:614-634, 2001.
2. S Tulyakov, F Farooq and V Govindaraju. Symmetric Hash Functions for Fingerprint Minutiae, *Proc. Int'l Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance*, pages 30–38, 2005.
3. A B J Teoh, A Goh and D C L Ngo. Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs, *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 28(7):1892-1901, 2006.

Table 4
SHA-256 Hash of Cancellable Image Before and After AES-256 Bit Cipher

	Cancellable template
SHA-256 Hash unencrypted in HEX representation:	5BB015B9A86F88AA1C21C47170553C3A3FB0052F35FF B35993D3AA0C43988449
SHA-256 Hash encrypted with AES-256 cipher (key=1234) in HEX representation:	5A8B2D5EDB8D5AEED90F67F2D7868C62DCD1B81E0 D588FB2A00111ABF5736589E649E6514AC256B74532E2 6AE5D369CBFF3715845E7B91C7223A877591082051FF2 94EBA0B0B7632C3C6BE5936A2078DA86487D39CDB2D B41A43FB53A2330F85021AEA394F3E867155979CF3BE7 A037209CDAC7E2D3896A200C89903EE48F36AFAA0F14 9F8A1D07C871537FB86EDB4AC

4. M Savvides, B V K V Kumar and P K Khosla. Corefaces- Robust Shift Invariant PCA based Correlation Filter for Illumination Tolerant Face Recognition, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04)*, 2004.
5. M A Dabbah, W L Woo and S S Dlay. Secure Authentication for Face Recognition, *in Proceedings of IEEE Symposium on Computational Intelligence in Image and Signal Processing, CIISP 2007*, 2007.
6. I Sobel. Neighborhood Coding of Binary Images for Fast Contour Following and General Array Binary Processing, *Compute, Graphics Image process*, pages 127–135, 1987.
7. L G Roberts. Machine Perception of Three Dimensional Solids, In Optical and Electrooptical Information processing, *MIT Press, Cambridge, MA*, 1965.
8. W Frei and C C Chen. Fast Boundary Detection: A Generalization and a New Algorithm, *IEEE Trans. on Computers*, 26(10):988-998, 1977.
9. J M S Prewitt. Object Enhancement and Extraction, in: B.S. Lipkin, A. Rosenfeld (Eds.), *Picture Analysis and Psychopictorics, Academic Press, New York*, 1970.
10. Dodis Y, Ostrovsky R, Reyzin L and Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data, *Tech. Rep. 235, Cryptology ePrint Archive*, 2006.
11. Hao F, Anderson R and Daugman J. Combining Crypto with Biometrics Effectively, *IEEE Transsctions on Computers* , 55(9):1081-1088, 2006.
12. Nandakumar K, Jain A K and Pankanti S. Fingerprint-based Fuzzy Vault: Implementation and Performance, *IEEE Transactions on Inform. Forensics Security* , 2(4):744-757, 2007.
13. Sutcu Y, Li Q and Memon N. Protecting Biometric Templates with Sketch: Theory and practice, *IEEE Transactions on Inform. Forensics Security*, 2(3):503-512, 2007.
14. C T Hsu and J L Wu. Hidden Digital Watermarks in Images, *IEEE Transactions On Image Processing*, 8(1):58–68, 1999.
15. Manvjeet Kaur, Sanjeev Sofat and Deepak Saraswat. Template and Database Security in Biometrics Systems: A Challenging Task, *International Journal of Computer Applications*, 4(5):0975–8887, July 2010.
16. Announcing the ADVANCED ENCRYPTION STANDARD (AES), *Federal Information Processing Standards Publication 197, United States National Institute of Standards and Technology (NIST)*, November 26, 2001, Retrieved October 2, 2012.
17. AT&T Laboratories Cambridge, The Database of Faces, *http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html*
18. Yale Face Database, *http://cvc.yale.edu /projects/yalefaces/yalefaces.html*
19. Vidit Jain, Amitabha Mukherjee. The Indian Face Database, *http://vis-www.cs.umass.edu/∼vidit/IndianFaceDatabase/*
20. G Hemantha Kumar and Manoj Krishnaswamy. Cancellable Face Biometrics Using Image Blurring, *International Journal of Machine Intelligence*, 3(4/5):272, 2011.

Dr. G Hemantha Kumar is currently the Chairman, Department of Studies in Computer Science, University of Mysore, Mysore, India. His Qualifications include B.Sc, B.Ed, M.Sc, Ph.D He was awarded Ph.D in Computer Science from University of Mysore. He has over 200 publications in all leading international and national journals as well as conferences.His current research interest includes Numerical Techniques, Digital Image Processing, Pattern Recognition and Multimodal Biometrics.

Manoj Krishnaswamy is a Research Scholar, Department of Studies in Computer Science, University of Mysore, Mysore, India. His Qualifications include BE in Computer Science from RVCE (BU) and MTech. in Computer Science from MVJCE (VTU). His current research interest includes Image Processing, Biometrics and Template Security.