www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18907-18910

A Survey on Privacy Protected Facial Biometric Verification

Parvathy R[1] , Dhanya Sreedharan[2]
[1]parudeepam@gmail.com, [2] dhanu.sree@gmail.com
Computer Science and Engineering from Kerala Technical University, India

Abstract

Today the use of security cameras or the surveillance cameras has been increased dramatically. Why because the cameras and networks become cheaper and also these cameras provide a feasible amount of security to the society. But the important thing is that the system should achieve two goals: it should perform face recognition for the security purpose and also the system should provide privacy protection for the individuals who are captured in those cameras. In simple words their face image should not browse without permission or it cannot be misused for any other purpose. Many solutions have been proposed to achieve these two in a surveillance system. The first solution was cryptographic encryption and later face scrambling has been proposed. In this paper we discuss about different techniques used for the privacy protection as well as face recognition and also a comparison between these methods are performed to evaluate these techniques.

Keywords: *face scrambling, cryptographic encryption, fuzzy random forest, privacy*

1. Introduction

Biometric recognition system especially face recognition is actually a computer application which has the capability of identifying or recognizing the person from a digital video frame or an image from a video source. Typically this system is implemented in authentication application by means of security cameras or surveillance cameras in public places like bus station, shopping mall etc. It can be compared with other biometric verification system such as fingerprint or eye iris recognition systems. Now a day it becomes popular as a commercial identification and marketing tool.

For security biometric verification systems especially face recognition system has been widely deployed in many authentication applications. Usage of these biometric data raises another serious issue and that is privacy. And hence privacy protection is now one of the challenging central issues in the video surveillance. And we cannot avoid the usage of these cameras because through the help of these security cameras we can reduce the rate of terrorism and attacks thus by benefitting our society. And now actually increase the need of a system which achieve both recognition process as well as protection of private data. In short privacy protection technology is essential in this surveillance society.

As cameras and networking have become cheaper, there has been an explosion in the dissemination of images occurred. In recent years, a number of technological solutions have been proposed for the general problem of privacy protection in images and video, and for face privacy protection in particular. Various methods have been proposed and developed for the protection of privacy based on the prior identification of sensitive regions of interest (ROI) such as human faces. After identifying such regions of interest we perform certain operations on that region in order to assure security and the operations are like biometric encryption, cartooning, scrambling etc.

Biometric encryption is actually a combination of cryptographic techniques and image processing operations to achieve privacy protection. In earlier this method was used for privacy protection in the surveillance cameras. Later face scrambling was proposed and it is considered as

the better one. Scrambling can be simply done by cartooning or masking etc. But the drawback with these methods are the loose of the facial information and thus by face recognition become unsuccessful. It is practically not a good choice to really erase human faces from surveillance videos. Thereafter Arnold Transform is proposed which is a type of recoverable scrambling method. And also it has properties like simplicity and periodicity. Scrambled faces can be easily unscrambled by some manual tries. Actually nowadays advanced automated surveillance systems are installed with online facial biometric verification.

In this paper a detailed study on different methods for privacy protected facial biometric verification is done and also comparisons between these methods are performed.

2. Literature Survey

Due to the increase in demand for security, video surveillance has become widely applied technology in the real world life .And the usage of these technology raises privacy as serious issue. F.Dufaux and T.Ebrahami [1] address the problem of scrambling the regions of interest in a video sequence for the purpose of preserving privacy in video surveillance. They propose an efficient solution based on transform-domain scrambling. More specifically, the sign of selected transform coefficients is pseudo-randomly flipped during encoding. And they address more specifically the two cases of MPEG-4 and Motion JPEG 2000. Simulation results show that the technique can be successfully applied to conceal information in regions of interest in the scene while providing with a good level of security. Furthermore, the scrambling is flexible and allows adjusting the amount of distortion introduced.

S.Hosik, W De Nevve and Y.M.Ro [2] discuss privacy protected surveillance system by makes use of JPEG Extended Range (JPEG XR) and this JPEG XR is used why because it offers a low complexity solution for high resolution images. In this method the working was as follows. Initially face regions are detected and scrambled in the transform domain. The method was able to conceal privacy sensitive face regions with a feasible level of protection.

F. Dufaux [3] proposes a framework to assess the capacity of privacy protection solution of different face recognition algorithms. In order to assess the efficiency of algorithms they perform rigorous experiments with each of them. And in the paper they also introduce privacy protection techniques such as pixelization and blur.

T. Honda, Y. Murukami, Y. Yanagihara, T. Kumaki and T. Fujino [4] develop a paper which proposes an image scrambling method for bit map and JPEG XR formatted images. The method also enables access control by simply providing keys to authorized individuals. The major advantage with the method is that the image's format is retained and hence no special viewer is needed in display only console. And also the experimental results show that the scramble level can be linearly controlled by parameters. They also developed a demo system for describing the working and functionalities and to ensure that this can be implemented with embedded system such as those equipped with surveillance cameras.

A. Melle and J. L. Dugelay [5] propose a novel scrambling procedure for protecting privacy sensitive image regions which encodes the sensitive data in a parametric form, and exploiting the visual information in the remaining part. The data is encrypted with a secret key. Partial knowledge of the secret key reveals a protected version of the original image at variable level of scrambling and the knowledge of full key allows the decryption to a quality level suitable for people identification. To evaluate the proposed method they apply scrambling filter to the AT&T face recognition dataset and measure the resulting quality with an objective metric.

T. Winkler and B. Rinner [6] presents attacks that affect the data privacy in visual sensor networks and proposes privacy promoting security solutions based on opponent detection. In this paper considering the privacy and security mechanism for a heterogeneous wireless visual sensor network (VSN). The network consists of wirelessly communicating cameras and scalar sensors. The sensors

trigger the cameras and provide specific privacy guarantees based on event detection. The network may deploy in one or more zones such as throughout a building and its perimeters.

A. Erdlyi, T. Bart, P. Valet, T. Winkler and B. Rinner [7] presents a resource aware cartooning privacy protection filter which converts raw images into abstracted frames where the privacy revealing details are removed. Cartooning can be applied either to entire images or to pre-selected sensitive regions of interest. The feasibility of this method is demonstrated by its deployment to real world embedded smart cameras. And they also evaluate privacy protection and utility of cartooning with the PEViD dataset and compare it with the two widely used privacy filters blurring and pixelization.

Richard Jiang, Ahmed Bouidane, Danny Crookes, M.Emre Celebi and Hua Liang Wei [8] proposed a method to make feature extraction from scrambled face images. For that a biased random subspace sampling scheme is applied to construct fuzzy decision trees from randomly selected features and fuzzy forest decision using fuzzy memberships is then obtained from combining all fuzzy tree decisions. In the experiment they first estimated the optimal parameters for the construction of the random forest and then applied the optimized model to the benchmark tests using three publically available face datasets.

3. Conclusion

Visual privacy in video based application is now a highly active research area. As the surveillance cameras are widely deployed for security purpose, privacy protection becomes a very challenging task. For privacy protection initial solution was cryptographic encryption which is a combination of cryptographic techniques and digital image processing. Later face scrambling method is proposed and is considered as the better solution since it needs less computational cost than the cryptographic encryption. And also face scrambling does not really hide information. Face scrambling methods are also available in different forms such as masking, cartooning, by Arnold transform, using Fuzzy Forest Learning etc. Among all these face scrambling methods Fuzzy Forest Learning is the best solution since it can perform online facial biometric verification which can be installed in automated surveillance system. And also this method is implemented with three publically available face datasets and the experimental results show that this method is a promising candidate for the emerging privacy related facial biometric applications.

Acknowledgment

I am grateful to my project guide Prof. Dhanya.Sreedharan for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. I am also thankful to all the staff members of the Department.

References

[1]F.Dufaux and T. Ebrahimi, (2006) "Scrambling for video surveillance with privacy," in Proc. Conf. Comput. Vision Pattern Recog. Workshop, Washington.

[2]S.Hosik, W.DeNeve, andY.M.Ro (2011) "Privacy protection in video surveillance systems: Analysis of sub band-adaptive scrambling in JPEG XR," IEEE TRANS. CIRCUITS SYST. VIDEO TECHNOL., VOL. 21, NO. 2.

[3]F. Dufaux (2011) "Video scrambling for privacy protection in video surveillance: Recent results and validation framework," PROC. SPIE, VOL. 8063.

[4] T. Honda, Y. Murakami, Y. Yanagihara, T. Kumaki, and T. Fujino (2013) "Hierarchical image-scrambling method with scramble-level controllability for privacy protection," in Proc. IEEE 56th Int. Midwest Symp. Circuits Syst.

[5]A.MelleandJ.L.Dugelay (2014) "Scrambling faces for privacy protection using background self-similarities," in Proc. IEEE International. Conference for . Image Process.

[6]T.WinklerandB.Rinner (2014) "Security and privacy protection in visual sensor networks: A survey," ACM Computer Surveys, vol. 47.

[7]A. Erdlyi, T. Bart, P. Valet, T. Winkler, and B. Rinner (2014) "Adaptive cartooning for privacy protection in camera networks,"in Proc. Int. Conf. Adv. Video Signal Based Surveillance.

[8]Richard Jiang, Ahmed Bouidane, Danny Crookes, M.Emre Celebi , Hua Liang Wei(2016), "Privacy protected facial biometric verification using fuzzy forest learning,"*IEEE TRANSACTIONS ON FUZZY SYSTEMS*, vol. 24, no. 4

Parvathy R received B.Tech. degree in Computer Science and Engineering from Mahathma Gandhi University, India. Pursuing M.Tech. degree in Computer Science and Engineering from Kerala Technical University, India.

Dhanya Sreedharan received B.Tech. Degree in Computer Science and Engineering from College of Engineering Karunagappally (CUSAT), received M.Tech. Degree in Computer and Information Technology from MS University, India. Currently, She is Assistant Professor at Sree Buddha College Engineering, Kerala University