A Study on Face Masking Scheme in Video Surveillance System

Dongchil Kim
Smart Media Research Center
Korea Electronics Technology Institute
Seoul, Korea
dckim@keti.re.kr

Sungjoo Park
Smart Media Research Center
Korea Electronics Technology Institute
Seoul, Korea
bpark@keti.re.kr

***Abstract*—**In this paper, we analyze face masking schemes in the video surveillance system for protecting the personal privacy from videos acquired by CCTV cameras. Existing face masking schemes have a problem that the face of humans can be identified because face masking setting values cannot be applied as an appropriate value. Through implementation results, we found optimal values for face masking to perfectly protect the personal privacy.

Keywords—face masking; video surveillance system; personal privacy;

I. INTRODUCTION

Video surveillance systems are increasingly installed and utilized for the crime prevention, the traffic surveillance, and the facility management. The video surveillance system consists of IP cameras, video and metadata transmission devices, video storage devices, video analysis devices, and video display devices [1]. In recent years, the video quality of IP cameras is progressing beyond HD to Full HD. As a result, the accuracy of human face recognition using IP camera is significantly increasing. However, existing face masking schemes have a problem that the face of humans can be identified because face masking setting values cannot be applied as an appropriate value [2-3]. To solve these problems, we analyze face masking schemes that are used to protect the personal privacy in the video surveillance system. Although the face masking scheme is applied to the face of humans since the face masking setting value cannot be applied to the appropriate value, the face recognition is possible and the personal privacy cannot be protected. In this paper, we found optimal values for the face masking of humans to perfectly protect the personal privacy through experiments using face recognition Application Programming Interfaces (APIs).

The rest of this paper is organized as follows. Section II provides an overview of existing face masking schemes. Section III describes the results of face masking analysis, and Section IV provides the concluding remarks.

II. RELATED WORKS

Figure 1 shows that the face masking procedure in the video surveillance system. First, the human identification method identifies the human from videos acquired from CCTV cameras and detects the face of humans. The face detection method is a key process that needs to be performed before the face masking. The face detection method can be classified into Knowledge, Template-matching, Feature, Appearance, Hybrid, and Deep Learning-based methods. The face tracking method is an essential technique with the face detection and is used to avoid repetitive operations on the same human. Then, the face masking method is used to mask the face of humans. Face masking methods are blurring, pixelization, removal/ transformation, and encryption [4].

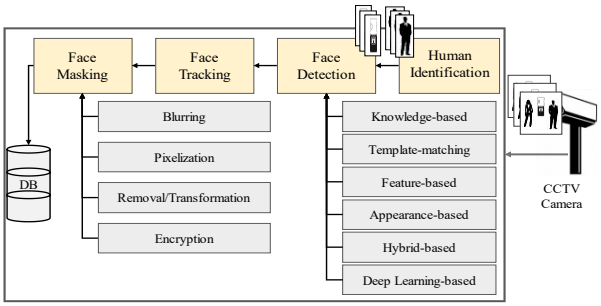


Fig. 1. Face masking procedure in the video surveillance system.

A. Blurring method

The blurring method blurs the face of humans making it difficult to identify the face. As a typical method for blurring, the image is blurred by adjusting the variance value (σ) of the Gaussian low-pass filter. This blurring method is simpler and easier to implement than other masking methods, but once masked images cannot be completely restored to the original image.

B. Plexelization(mosaic) method

The pixelization method blurs the face of humans by replacing the block size (B × B) with the same brightness value using the average value of the block. This method is a technique commonly used in television news and the documentary and is used to keep anonymity by covering the faces of suspects, witnesses, or ordinary people. However, the disadvantage of the plexelization method is that the integration of the pixels over time can partially recover the concealed information.

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (2014-3-00077, Development of global multi-target tracking and event prediction techniques based on real-time large-scale video analysis)

C. *Removal/Transformation method*

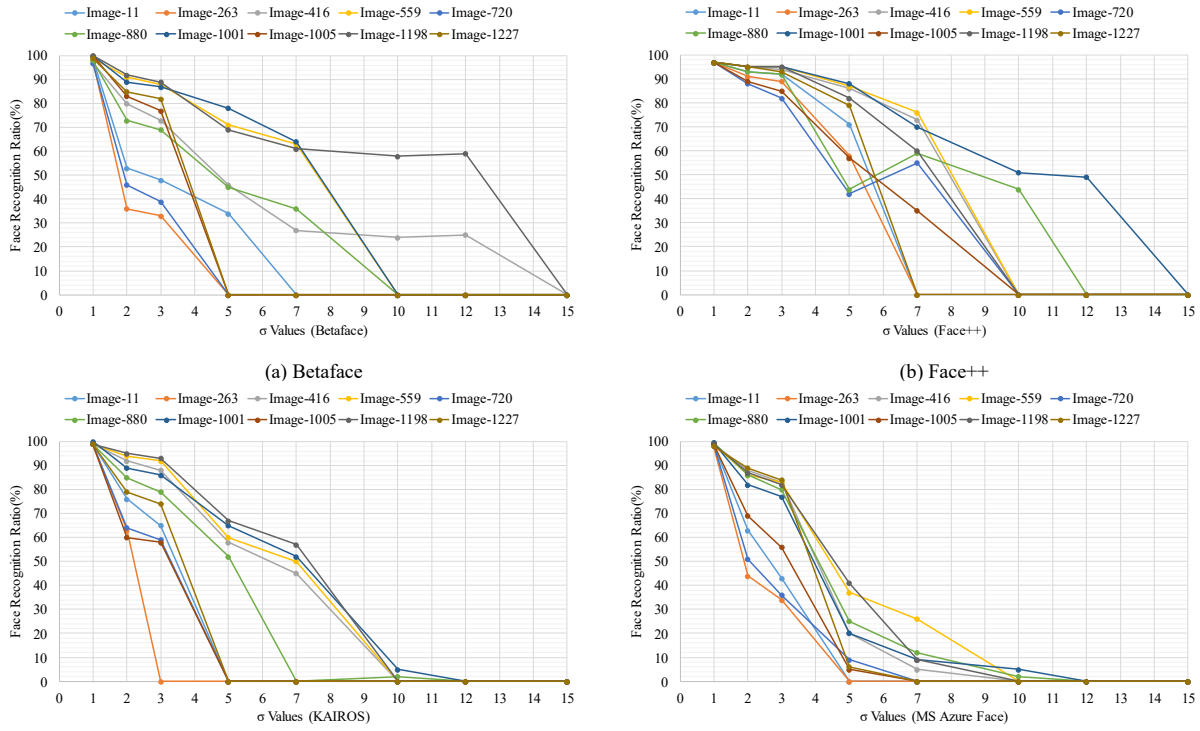
The removal/transformation completely removes or modifies the face region from the image after detecting the face of humans for perfectly protecting the personal privacy [5].

D. *Encryption method*

Even though the video surveillance system protects the personal privacy by making it difficult to identify the face of humans through the blurring, plexelization, and the removal/transformation methods, there is a situation where the face is to be restored to the original image. The scrambling scheme in MPEG-4 uses an encryption key to encrypt the private face image and only the authorized administrator uses the encryption key to unmask [6]. The image can be reconstructed to the original image by using the scrambling scheme. In addition, the strength of the scrambling can be adjusted, so that it can be used for simple monitoring purposes and for accurate person estimation applications. However, since encryption keys for scrambling can be leaked, additional security is required. In order to protect the face of humans in H.264 video, Flexible Macroblock Ordering (FMO) is used [7]. The FMO scheme has seven matching types. FMO type 2 is used for the encryption of Region of Interest (ROI), but it suffers only from a rectangular area, and thus it cannot express an irregular face area well. In general, FMO type 6 is mainly used. The FMO scheme can encode a specific face region in real time and decode it according to the needs of the currently used CCTV standard format.

III. Analysis of Face Masking Scheme

In order to find appropriate setting values for perfect face masking, we experimented with the face recognition rate according to face masking setting values using the face recognition API. We used Betaface [8], Face ++ [9], KAIROS [10] and Microsoft Azure Face [11] for the face recognition API. Betaface is software for the recognition and the face analysis that runs on Windows and Linux. It also supports common image formats, live video streams, and video file formats. Betaface uses 22 basic face points to crop the face region and then uses 101 advanced face points to detect faces. Especially, Betaface supports face similarity judgment as well as sex, age, smile, skin color, face, hair color detection. Face ++ provides services for the face detection, recognition, and analysis in applications. Using computer vision and data mining technology, three core vision services as sensing, recognition, and analysis can be provided, and face recognition can detect age, sex, glasses, and race. KAIROS provides services for the face detection, face recognition, and analysis through computer vision and machine learning. It also detects emotional detections (joy, surprise, sadness, fear, anger, and nervousness) and age, gender, interest, glance, flicker, wearing glasses, and race in the face. MS Azure Face provides cloud-based face detection and face recognition services. It can detect up to 64 human faces. Similar to other methods, emotion detection and recognition of race, sex, and age are possible. We use Face Detection Data Set and Benchmark Home (FDDB) for the experiment [11]. FDDB includes various face poses and occlusion, face data of various sizes.



(a) Betaface

(b) Face++

(c) KAIROS

(d) MS Azure Face

Fig. 2. Face recognition rate according to variations of σ values.

A. *Comparison of the face recognition with variation of σ value*

Figure 2 shows the comparison between the original image and the face image after changing σ values from 0 to 15. Experimental results show that σ value should be set to 15 or more in order not to recognize the face of humans in all systems.

B. *Comparison of the face recognition with variation of block size*

Figure 3 shows the comparison between original image and face recognition after varying the block size of 10 face images from 0 to 15. Experimental results show that when face masking is performed through the pixelization after detecting the face area, the block size must be set to 15 or more so that the face cannot be recognized.

IV. Conclusion

In this paper, we found appropriate values for applying face masking to perfectly protect the personal privacy in the video surveillance system. Through face recognition experiments, appropriate values for blurring and pixelization were derived when applying the face masking. Experimental results show that σ value is set to more than 15 and the block size is set to more than 15 to perfectly protect the face of humans.

References

[1] S. Park, U. Park, and D. Kim, "Depth image-based object segmentation scheme for improving human action recognition," Proceedings of International Conference on Electronics, Information, and Communication, pp. 387-389, Jan. 2018.

[2] H. Moon and S. Pan, "The analysis of de-identification for privacy protection in intelligent video surveillance system," Journal of Korean Institute of Information Technology, Vol. 9, No. 7, pp. 189-200, Jul. 2011.

[3] D. Kim and S. Park "Face masking technology in the intelligent video surveillance system," TTA Journal, Vol. 171, pp. 36-41, Jun. 2017.

[4] M. Yang, D. Kriegman and N. Ahuja, "Detecting faces in images: a survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp. 34-58, Aug. 2002.

[5] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. Nayar, "Face swapping: automatically replacing faces in photographs", ACM Transactions on Graphics, pp. 1672-1675, Aug. 2008.

[6] F. Dufaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 18, No. 8, pp. 1168-1174, Jul. 2008.

[7] F. Peng, X. Zhu, and M. Long, "An ROI privacy protection scheme for H.264 video based on FMO and Chaos", IEEE Transactions on Information Forensics and Security, Vol. 8, No.10, pp. 1688-1699, Apr. 2013.

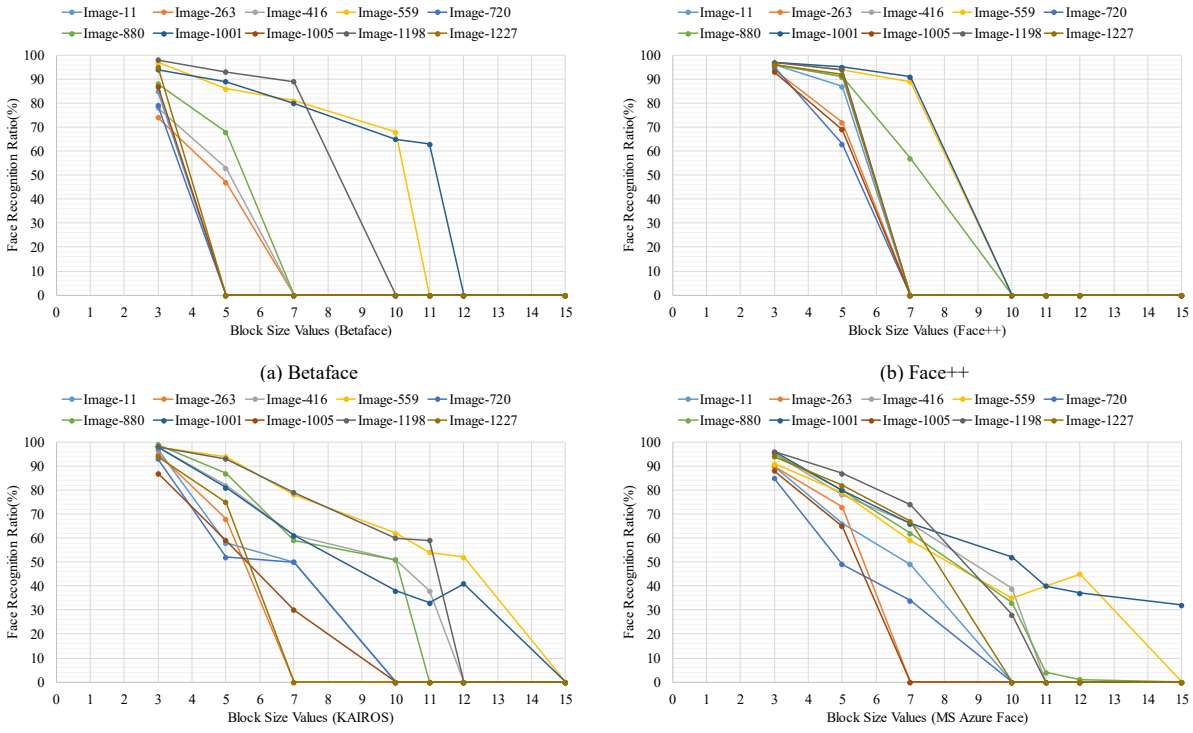
[8] Betaface, "https://www.betafaceapi.com/wpa/"

[9] Face++, "https://www.faceplusplus.com/"

[10] KAIROS, "https://www.kairos.com/"

Microsoft Azure Face, "https://azure.microsoft.com/ko-kr/services/cognitive-services/face/"

[11] V. Jain, Vidit, and E. Learned-Miller, "FDDB: a benchmark for face detection in unconstrained settings", University of Massachusetts, Technical Report, UM-CS2010-009, 2010.



(a) Betaface (b) Face++

(c) KAIROS (d) MS Azure Face

Fig. 3. Face recognition rate according to variation of block sizes.