Encoder/Decoder for Privacy Protection Video with Privacy Region Detection and Scrambling

Feng Dai, Dongming Zhang, and Jintao Li

Advanced Computing Research Laboratory, Beijing Key Laboratory of Mobile
Computing and Pervasive Device, Institute of Computing Technology,
Chinese Academy of Sciences, Beijing, 100190, China
{fdai,dmzhang,jtli}@ict.ac.cn

Abstract. Privacy region scrambling is an effective method to protect privacy information in videos. In this paper, we present an encoder/decoder system for privacy protection video. On the encoder side, the privacy region in video is automatically extracted and scrambled while encoding. On the decoder side, users can exactly restore the original video with a legitimate key otherwise only non-privacy part can be decoded correctly but the privacy regions are encrypted.

Keywords: private protection, video scrambling, privacy region detection.

1 Introduction

With the rapid development of information technology and people's widespread concern about public safety, video surveillance systems have penetrated into all aspects of our lives. However, incessant monitoring makes people begin to pay more attention to personal privacy. Privacy region scrambling is one of the major technologies for private protection video [1]. Generally, the scrambling process is driven by a key. Anyone without the key can only see non-privacy region with the privacy region scrambled. When necessary, descrambler can exactly restore the original video with a legitimate key.

Encoder of privacy protection video mainly involves three parts: privacy region extraction, privacy region scrambling and video coding. Face or motion detection methods are commonly used to extract private regions. And the detected region is scrambling either before video coding or during video coding.

2 Encoder for Privacy Protection Video

Fig.1 illustrates the framework of the proposed Encoder of privacy protection Video. There are mainly three parts of the system. First, by utilizing data generated during video encoding, the privacy region is extracted. Then the detected regions are directly protected by quantized coefficients scrambling. To prevent drift error, a coding restricted scheme is employed.

S. Li et al. (Eds.): MMM 2013, Part II, LNCS 7733, pp. 525–527, 2013.

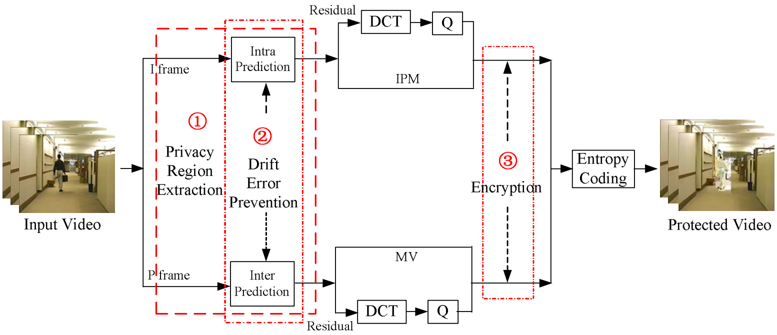

Fig. 1. Encoder for Privacy Protection Video

2.1 Motion Detection with Encoding Information

Motion is important information in video, which is critical for privacy protection. So moving objects are detected and protected in our system. In privacy protection video, video encoding is very time consuming [2] and all process must be finished in real time with additional motion detection. So fast motion detection must be adopted. Different from pixel domain detection and compressed domain detection, we proposed motion detection with encoding information. This method can extract moving objects directly during video encoding, so the computation time is reduced, which is attractive for real-time applications.

2.2 Transform Domain Scrambling

After obtaining the privacy regions, transform domain scrambling is applied to data related to these regions. The random sign inversion method is used in our system. In encoder, a pseudorandom number generator (PRNG) initialized by a key is used to produce random number sequences. Then the sign of quantized coefficients (defined as $qC[i]$, i=0…15) of each 4×4 block in privacy region is pseudo-randomly flipped for each i as follows:

$$qC[i]=\begin{cases}-qC[i] & random\_bits=1\\ +qC[i] & otherwise\end{cases} \tag{1}$$

2.3 Drift Error Prevention

To improve coding efficiency while preventing drift error, mode restricted intra prediction (MRIP) and search window restricted motion estimation (SWRME) are proposed in our early work [3].

2.4 Decoder for Privacy Protection Video

Because the video bitstream is compliant with video coding standard, it can be displayed by a standard decoder but the privacy region scrambled. If we want to decode the whole original image, the encoded video must be decoded by the specific video decoder. Anyone without the key can only see non-privacy data with the privacy region scrambled. Authorized users can exactly restore the original video with a legitimate key.

3 Demonstration

Fig.2 illustrates the encoder/decoder of private protection video user interface. Firstly, we choose a video to encrypt and input a key, then click the "encrypt" button, and the private region will be scrambled while the video encoding. Fig.2(a) shows the decoded image with the right key and Fig.2(b) shows the scrambled image with a wrong key.

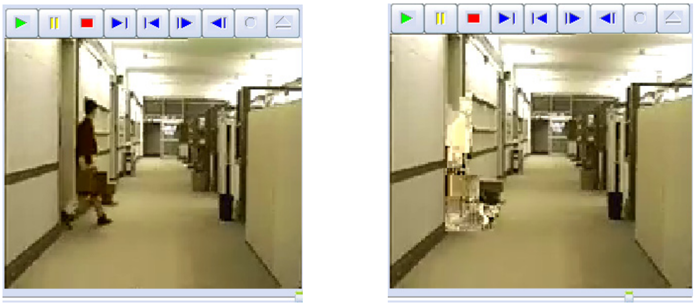

Fig. 2. (a) Decoded image with the right key (b) Scrambled image with a wrong key

Acknowledgments. This work is supported by National Nature Science Foundation of China (61102101, 61272323), National Key Technology Research and Development Program of China (2012BAH06B01).

References

1. Dufaux, F., Ebrahimi, T.: Scrambling for Privacy Protection in Video Surveillance Systems. IEEE Trans. Circuits and Systems for Video Technology 18, 1168–1174 (2008)
2. Zhang, Y., Yan, C., Dai, F., Ma, Y.: Efficient Parallel Framework for H.264/AVC Deblocking Filter on Many-core Platform. IEEE Trans. on Multimedia 14, 510–524 (2012)
3. Tong, L., Dai, F., Zhang, Y., Li, J.: Prediction restricted H.264/AVC video scrambling for privacy protection. Institution of Engineering and Technology Electronics Letters 46, 47–49 (2010)