PRIVACY REGION PROTECTION FOR H.264/AVC BY ENCRYPTING THE INTRA PREDICTION MODES WITHOUT DRIFT ERROR IN I FRAMES

Yongsheng Wang, Máire O'Neill, Fatih Kurugollu

Center for Secure Information Technologies (CSIT), Queen's University, Belfast, BT3 9DT, UK
Email: ywang26@qub.ac.uk, m.oneill@ecit.qub.ac.uk, f.kurugollu@qub.ac.uk

ABSTRACT

While video surveillance systems have become ubiquitous in our daily life, this has also brought some serious privacy concerns. Therefore, recent research in this area has included a focus on privacy region protection. Existing video scrambling techniques are being applied to specific regions of interest in a video while the background is left unchanged. In this paper, a new method involving the encryption of intra prediction modes (IPM) is proposed for privacy region protection without drift error in I frames. Compared with a previous technique that uses encryption of IPM, the proposed method offers savings in the bitrate overhead. To enhance the scrambling effect for the privacy region, the proposed method can support the combination of IPM with encryption of the sign bits of nonzero quantized transform coefficients in the privacy region. Experimental results and analysis based on H.264/AVC were carried out and verify the effectiveness of the proposed method.

Index Terms— Privacy region protection, video scrambling, intra prediction modes, drift error, bitrate overhead

1. INTRODUCTION

Video surveillance systems are widely deployed in modern society to help counteract anti-social behaviour and, indeed, possible terrorist threats. While society is enjoying the benefits of the security provided by monitoring important public and/or private infrastructures, the privacy protection of people has become a significant concern. Therefore, in the past few years, significant research has been conducted into the application of existing video scrambling techniques to protect specific privacy regions in video, such as people's faces.

Dufaux and Ebrahimi [1] first proposed to encrypt the sign bits of nonzero AC transform coefficients of blocks in the privacy region for MPEG-4 and Motion JPEG 2000. The encrypted video can be decoded as normal, but without decryption, the privacy region remains scrambled while the rest of each frame, the non-privacy region, is left clear. An MB-type decision mechanism is employed to hinder the drift error caused by inter prediction, which means that the macroblock in the current frame, collocated with a MB in the privacy region of reference frames, is always intra coded. The authors extended their technique to the codestream-domain of MPEG-4 [2]. The compressed video stream is firstly parsed and then the corresponding sign bits of AC transform coefficients are encrypted as described above. In [3], their technique was further extended to H.264/AVC. The Flexible Macroblock Ordering (FMO) mechanism of H.264/AVC [4] [5] [6] is utilized to indicate which macroblocks belong to the privacy region and prevent drift error due to intra prediction from the privacy region to the non-privacy region. The MB-type decision mechanism is also adopted to eliminate drift error due to inter prediction. Choi *et al.* [7] discussed the drift error when applying selective encryption for privacy region protection in H.264/AVC and introduced some new approaches. In order to prevent drift error due to intra prediction, the intra prediction modes of blocks to the right and bottom of the privacy region are modified without prediction from the privacy region. The same MB-type mechanism as that used in [1] [2] is also adopted. In addition, the privacy region in reference frames can not be used to predict blocks in the non-privacy region and their motion vectors. At the same time, Tong *et al.* [8] proposed some similar solutions to avoid drift error when applying different selective encryption methods to privacy regions based on H.264/AVC. They proposed two techniques, Mode Restricted Intra Prediction (MRIP) for intra prediction and Search Window Restricted Motion Estimation (SWRME) for inter prediction, to remove drift error when encrypting the sign bits of nonzero transform coefficients. They also proposed to forbid the use of the intra 4x4 prediction modes of blocks to the right and bottom of the privacy region when encrypting the intra prediction modes in the privacy region. In addition, a binary mask (one bit per MB) is employed to indicate the privacy region without using the slice group separation [5] [6] as used in FMO. The bitrate overhead incurred by the binary mask was addressed in [9]. Dai *et al.* [10] extended the work in [8] by introducing the Boundary Strength Restricted Deblocking Filter (BSRDF) to further remove drift error. Compared with the work in [3], the methods in [8] and [10] have significantly improved the bitrate overhead while preventing drift error. However, this work only focuses on encrypting the sign bits of nonzero transform coefficients.

In this paper, a new method to assist with encryption

of the intra prediction modes in the privacy region is proposed, which offers improved bitrate overhead savings over the method in [8] while ensuring no drift error in the I frames.

The rest of this paper is arranged as follows. In Section 2, the existing MRIP and Improved MRIP [8] are explained, and the proposed method to help with the encryption of the intra prediction modes in the privacy region is demonstrated. In Section 3, experimental results show that the proposed method can effectively save more bitrate overhead while still ensuring no drift error. Finally, conclusions are given in Section 4.

2. ENCRYPTING INTRA PREDICTION MODES IN THE PRIVACY REGION

Directly encrypting the intra prediction modes (IPM) [11] in the privacy region of a video frame will result in drift error in the non-privacy region located to the right and bottom of the privacy region, as shown in Fig. 1. Thus, additional processing is required to prevent such drift error. Before demonstrating the proposed method involving encryption of the intra prediction modes in the privacy region, two existing related methods, MRIP and Improved MRIP, are first explained.

Fig. 1. Drift error in one frame of 'foreman'.

2.1. Mode Restricted Intra Prediction (MRIP)

MRIP was proposed separately by Tong *et al.* [8] and Choi *et al.* [7]. In H.264/AVC, an intra encoded macroblock may be encoded into the intra 4x4 prediction mode or the intra 16x16 prediction mode. There are nine intra 4x4 prediction modes and four intra 16x16 prediction modes. The fundamental idea in the above technique is to restrict the possible intra prediction modes for blocks around the boundary of the privacy region. As shown in Fig. 2, for a block, C, around the boundary of the privacy region, some of the nine intra 4x4 prediction modes are forbidden according to whether or not its adjacent top (T), left (L), top-left (TL) and top-right (TR) blocks are

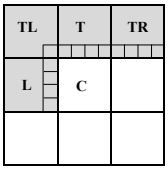

Fig. 2. The adjacent blocks that may affect the current block by intra prediction.

located in the privacy region. The forbidden intra 4x4 prediction modes are listed in Table 1. In particular, if both the top and left block of the current block, C, belong to the privacy region, all nine intra 4x4 prediction modes are forbidden and the current block is coded in IPCM (Intra Pulse Code Modulation) which does not need any prediction from its adjacent blocks. This is also the case for 16x16 intra prediction. Table 2 lists forbidden modes for the 16x16 block according to its neighbouring block position relative to the privacy region.

Table 1. The forbidden intra 4x4 prediction modes of a 4x4 block if its adjacent block is within the privacy region

Position	The forbidden intra prediction modes
T	DC, Diagonal down left, Diagonal down right, Vertical left, Vertical right and Horizontal down
L	Horizontal, DC, Diagonal down right, Vertical right, Horizontal down and Horizontal up
TL	DC, Diagonal down right, Vertical right and Horizontal down
TR	Diagonal down left and Vertical right

Table 2. The forbidden intra prediction modes of a 16x16 block if its adjacent block is within the privacy region

Position	The forbidden 16x16 intra prediction modes
T	Vertical, DC and Plane
L	Horizontal, DC and Plane
TL	Plane
TR	None

2.2. Improved MRIP for Encryption of IPM

MRIP was designed to prevent the drift error caused by intra prediction when encrypting the sign bits of nonzero quantized DCT coefficients. In [8], Tong *et al.* proposed the scrambling of the intra prediction modes (similar to the method in [11]) in the privacy region and they also presented an improved MRIP to prevent the corresponding drift error. To encode the intra 4x4 prediction modes of the current block, C, its most probable intra prediction mode will be the smaller of the two intra 4x4 prediction modes of its neighbouring top and left blocks, T and L. If either of these is not encoded by the intra 4x4 prediction mode, the most probable intra 4x4 mode is set to the DC prediction mode. If the best intra 4x4 prediction mode for optimizing the distortion [5] equals the most probable one, a flag bit 'prev_intra4x4_pred_mode' is sent with a value of '1'; otherwise, the flag bit is set to '0' and a 3-bit parameter 'rem_intra4x4_pred_mode' is sent. If the most probable intra 4x4 prediction mode is greater than the best mode, the value of 'rem_intra4x4_pred_mode' equals the best mode; otherwise, it is set to the best mode minus 1. Because the intra 4x4 prediction mode of the current block is coded according to the most probable mode which is predicted from the coded modes of the two neighbouring blocks (top and left), after encrypting the intra prediction modes of blocks in the privacy region, the intra prediction modes of blocks to the right and bottom of the privacy region are very likely to be decoded

incorrectly. Tong *et al.* [8] proposed to forbid the intra 4x4 prediction mode for blocks if their left or top block is in the privacy region. In all other cases, Table 1 and 2 are still used.

2.3. Proposed Method: Re-encoding IPMs around The Boundary

Generally, a macroblock which is encoded in the intra 4x4 prediction mode has more texture and if encoded in other modes, like the intra 16x16 prediction mode or IPCM, the compression performance will be reduced and the resulting bitrate overhead will increase. Thus, a new mechanism is proposed in this paper to encrypt the intra prediction modes in the privacy region without preventing the use of the intra 4x4 prediction mode for the blocks around the boundary. Each of the intra 4x4 prediction modes of the blocks within the privacy region can be scrambled by XORing with three random bits, generated by a secure stream cipher. When encoding the intra 4x4 prediction mode of a block around the boundary, if any one of its adjacent top and left blocks is located in the privacy region, the most probable prediction mode should be calculated from the encrypted intra 4x4 prediction modes of the two neighbouring blocks. Then the two parameters, 'prev_intra4x4_pred_mode' and 'rem_intra4x4_pred_mode' are sent in the normal way. Figure. 3 shows an example of the proposed mechanism. Assuming that the block above the current block has an intra 4x4 prediction mode of 5 and belongs to the privacy region and that the block to the left has an intra 4x4 prediction mode of 4 and is not within the privacy region, three parameters (α, β, γ) are used to indicate the information for the encoding of each block. Here, θ is the best intra 4x4 prediction mode, α is the corresponding most probable intra prediction mode, and the two parameters, β and γ, represent 'prev_intra4x4_pred_mode' and 'rem_intra4x4_pred_mode', respectively. Given that the intra 4x4 prediction mode of the current block (which is located around the boundary of the privacy region) is 3, the intra prediction mode of its top block is encrypted to 1 as shown in Fig. 3(b). Without any special processing in the decoding procedure, the current block's intra prediction mode will be incorrectly decoded as 4 (Fig. 3(c)) and further more, this error is likely to propagate into subsequent blocks. Thus, to prevent this after encrypting the top block's IPM, the intra prediction mode of the current block should be re-encoded again according to the encrypted intra prediction mode. As shown in Fig. 3(d), the re-encoded intra prediction mode can be decoded correctly according to the encrypted adjacent IPMs. This means that the decoding error that typically results when encrypting IPM will not happen. When decryption is needed, the intra 4x4 prediction modes of blocks around the boundary should be decoded according to the encrypted adjacent IPMs.

2.4. Combination with SNC

As mentioned in Section 1, most previous work on privacy region protection only involve encryption of the sign bits of nonzero quantized transform coefficients, referred to as SNC. On its own, this technique can not provide a strong scrambling effect. As shown in Fig. 4, the face region in the 1st and 15th frames of 'foreman' in the CIF resolution is encrypted by SNC. But it is clear that the scrambling effect is not enough to conceal full face. Thus, in this work the SNC and IPM methods are combined to enhance the scrambling effect of the privacy region if required. The resulting effective scrambling effect will be shown in the next section.

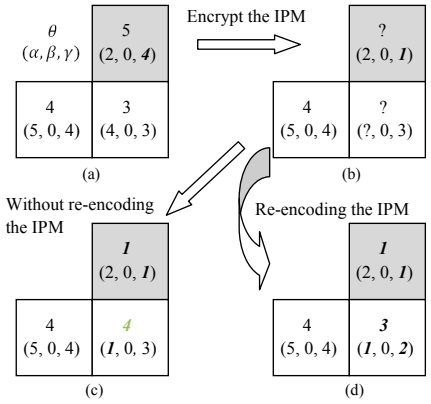

Fig. 3. An example of re-encoding the intra 4x4 prediction mode of a block around the boundary of the privacy region.

(a) The 1st frame (b) the 15th frame

Fig. 4. The 1st and 15th frames of 'foreman' only with SNC for the privacy region protection.

3. EXPERIMENTAL ANALYSIS

Experiments were conducted based on the JM 17.2 [12] reference software. A stream cipher, 'Rabbit' [13], is used to generate the random bit sequence required during the scrambling process. Three test sequences, 'foreman', 'road' and 'hall', in CIF resolution are chosen to evaluate the proposed method for the baseline profile. To provide a better scrambling effect, the combination of IPM and SNC is used to evaluate the proposed method, compared with the work of Tong *et al.* [8]. The privacy region is assumed to be known and signaled on a MB basis.

3.1. Bitrate Overhead

The first 30 frames of 'foreman' and 'road', and the second 30 frames of 'hall' from the 31st frame to the 60th frame, are encoded in the baseline profile. (In the first 30 frames

of 'hall', the moving people which forms the privacy region, does not appear or only appears partially, thus the second 30 frames are used.) Different quantization parameters (QP) are set. The bitrate overhead is defined as the difference between the bitrate when privacy region protection is applied and the bitrate without privacy region protection. In Table 3, the bitrate overheads using the proposed re-encoding method described in this paper, and the previous work by Tong *et al.* [8], are compared. In Table 3, all frames are intra coded. It is clear that for different QP values, the proposed method can offer bitrate overhead savings over the previous work. In Fig. 5, the intra period is set to different values and the bitrate overhead savings are plotted. Here, SWRME [8] [10] is adopted to prevent drift error for inter prediction. With the increase of the intra period, the saving in bitrate overhead is decreased. This is because the proposed method only works for the intra prediction modes. The saving in bitrate overhead is highly dependent on the number of I frames in the sequence.

Table 3. The bitrate overhead using the proposed method and the technique by Tong *et al.* [8] with all frames intra coded

QP	Bitrate Overhead (kb/s)					
	Proposal Method			Tong *et al.* [8]		
	foreman	road	hall	foreman	road	hall
12	129.960	77.880	105.312	195.120	117.872	157.328
18	143.856	92.448	112.976	201.704	129.192	156.776
24	152.688	96.160	122.208	197.696	124.120	154.648
30	152.616	96.592	122.016	182.336	113.216	147.152
36	150.280	95.136	119.480	163.336	103.192	135.968

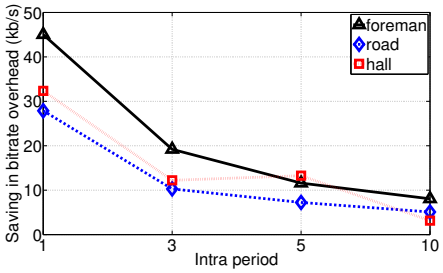

Fig. 5. The bitrate overhead savings for different values of the intra period with QP=24.

3.2. The Scrambling Effect

As mentioned in Section 2.4, solely using SNC for privacy region protection can not provide a strong scrambling effect. Thus, it is better to apply IPM and SNC together to enhance the scrambling effect for the privacy region. The proposed method makes this combination feasible with a relatively low bitrate overhead. Drift error is also completely prevented in the I frames. Fig. 6 shows the 1st and 15th frames in the 'foreman' sequence. Compared with the two corresponding frames in Fig. 4, it is clear that the scrambling effect is very effectively improved to conceal the face. In Fig. 7, the 15th frame of 'road' and the 40th frame of 'hall', are also shown to verify the enhanced scrambling effect.

(a) The 1st frame (b) the 15th frame

Fig. 6. The 1st and 15th frames of 'foreman' with IPM+SNC for the privacy region protection.

(a) The 15th frame of 'road' encrypted by IPM+SNC. (b) The 15th frame of 'road' encrypted by SNC.

(c) The 40th frame of 'hall' encrypted by IPM+SNC. (d) The 40th frame of 'hall' encrypted by SNC.

Fig. 7. Example of the scrambling effect: the 15th frame of 'road' and the 40th frame of 'hall'.

4. CONCLUSIONS

In this paper, a new method is proposed to address the drift error that occurs when encrypting the intra prediction modes (IPM) in the privacy region of a video. Most existing work on privacy region protection only involves the encryption of the nonzero transform coefficients. Some recent research has advanced techniques to remove drift error caused by prediction from the privacy region to the non-privacy region. Tong *et al.* [8] proposed to forbid the intra 4x4 prediction modes when applying IPM in privacy region protection. Compared to this previous research, a re-encoding mechanism is proposed in this paper to re-encode the intra prediction modes of blocks around the boundary of the privacy region according to the encrypted intra prediction modes of blocks in the privacy region. This makes the combination of IPM and SNC for privacy region protection feasible while still preventing drift error, and also enhancing the scrambling effect. Experimental results show that the proposed method can offer bitrate overhead savings over the previous technique proposed by Tong *et al.* [8]. The enhanced scrambling effect of the privacy region is also verified.

5. REFERENCES

[1] F. Dufaux and T. Ebrahimi, "Scrambling for Video Surveillance with Privacy," *Proceedings of IEEE Workshop on Computer Vision and Pattern Recognition*, 2006, pp. 160–167.

[2] 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, 2008.

[3] F. Dufaux and T. Ebrahimi, "H.264/AVC Video Scrambling for Privacy Protection," *Proceedings of 15th IEEE International Conference on Image Processing*, 2008, pp. 1688–1691.

[4] ITU-T REC. H.264 ISO/IEC 14496-10:2010, "Advanced Video Coding for Generic Audio-visual Services," 2010.

[5] I. Richardson, "The H.264 Advanced Video Compression Standard," Wiley, 2010.

[6] F. Lambert, W.D. Neve, Y. Dhondt, and R.V. Walle, "Flexible Macroblock Ordering in H. 264/AVC," *Journal of Visual Communication and Image Representation*, vol. 17, no. 2, pp. 358–375, 2006.

[7] S. Choi, G. Kim and J. Han, "On the Challenges of Applying Selective Encryption on Region-of-Interest in H. 264 Video Coding," *Proceedings of 15th IEEE International Conference on Computer Science and its Applications*, 2009, pp. 1–5.

[8] L. Tong, F. Dai, Y. Zhang, and J. Li, "Restricted H.264/AVC Video Coding for Privacy Region Scrambling," *Proceedings of 17th IEEE International Conference on Image Processing*, 2010, pp. 2089–2092.

[9] Y. Wang, M. O'Neill, and F. Kurugollu, "Adaptive binary mask for privacy region protection," *Proceedings of IEEE International Symposium on Circuit and Systems* , 2012, pp. 1127–1130.

[10] F. Dai, L. Tong, Y. Zhang, and J. Li, "Restricted H.264/AVC Video Coding for Privacy Protected Video Scrambling," *Journal of Visual Communication and Image Representation*, vol. 22, no. 6, pp. 479–490, 2011.

[11] J. Ahn, H. Shim, B. Jeon and I. Choi, "Digital Video Scrambling Method Using Intra Prediction Mode," *Advances in Multimedia Information Processing PCM2004, Springer, LNCS*, vol. 3333, pp. 386-393.

[12] JM reference software, ver. 17.2, `http://iphome.hhi.de/suehring/tml`, Apr. 2011.

[13] M. Boesgaard, M. Vesterager, T. Christensen and E. Zenner, "The Stream Cipher Rabbit," available via `http://www.ecrypt.eu.org/stream/p3ciphers/rabbit/rabbit_p3.pdf`, 2011.