Semi-fragile Watermarking for Video Content Authentication Based on Hybrid Feature

Chen Ling[1, 2] Wenjun Zhang[1]

[1] School of Film and Television Technology, Shanghai University
Shanghai 200072, Shanghai, China
lcrex@shu.edu.cn, wjzhang@mail.shu.edu.cn

[2] School of Communication & Information Engineering, Shanghai University
Shanghai 200072, Shanghai, China

Received 26 January 2014; Revised 29 April 2014 ; Accepted 24 June 2014

Abstract. In practical video storage and distribution systems, video sequences are stored and transmitted in a compressed format. During compression, the video frame is transformed from the spatial domain into frequency domain. Therefore, video content authentication methods need to be robust to lossy compression. This paper proposes a novel semi-fragile watermarking video content authentication based on a hybrid feature, consisting of gray threshold and relative total variation edge feature. The watermark is encrypted and embedded into the principal diagonal of 8×8 DCT coefficients. At the receiver side, when a part of the watermarked video is tampered, the proposed approach can locate these tampered areas. The experiment demonstrates the proposed method can distinguish malicious attacks from the legitimate common alterations, such as H.264 lossy compression, Gaussian noise and Gaussian filtering. It has outstanding capability to robust to H.264 compression and to detect malicious attacks. The experiment shows that the proposed method has higher recall and precision than the current approaches.

Keywords: H.264, video watermarking, content authentication, hybrid feature, DCT, Kerckhoffs's principle

1 Introduction

In state-of-the-art network, together with the development of increasingly powerful signal and image processing techniques, digital multimedia data is susceptible to manipulations and alterations using widely available editing tools. Many applications, such as video surveillance, video conferencing, DVD and so on, will meet challenges. So information integrity authentication for multimedia content protection is becoming an important problem in the study of information security [1].

For video content authentication, there are two main methods: digital signatures and digital watermarking. The former is well developed and widely used in industry. However, its shortcoming is that the signature needs extra band-width or a separate secure channel for transmission. Due to the use of a hash function, it is susceptible to failed authentication due to the avalanche effect. It is quite often that exactly one or a few bits of multimedia data change, e.g., due to noise or compression [2-3]. Digital watermarking is a technique about how to hide a special mark into digital multimedia data to protect copyright or verify the integrity of the original data [4-5]. The robust watermarking technology is used to protect copyright while the fragile watermarking, just like the digital signature, is proposed to check integrity and authenticity of digital contents [6].

Videos may be regarded as a series of continuous static images in the time domain. Therefore, video watermarking can be based on static image watermarking. Until now, the static image watermarking technology is more mature. However, video watermarking must have higher requirements except for satisfying static image watermarking' requirements. In practical video storage and distribution systems, video sequences are stored and transmitted in a compressed format. During compression, the video frame is transformed from the spatial domain into frequency domain. Therefore, it needs to be robust to acceptable operations, such as compression and filtering. But in practice, the fragile watermarking is too sensitive to any alteration, including common image processing, so the semi-fragile watermarking technique has been proposed. The semi-fragile watermarking can detect and locate tampered areas. In order to realize this kind of semi-fragile watermarking approach, two aspects should be considered: robust watermarking embedding algorithm and robust feature.

Fridrich and Goljan [7] introduced two techniques for self-embedding an image in itself. These are now two general watermarking categories: spatial domain methods and transform domain methods. Spatial methods embed watermark by changing certain original image pixels directly. For example, watermarks are embedded in the least significant bits (LSB). While transform domain methods change the coefficients of transform domain (e.g. DCT and DWT domain) and distribute the watermark signal energy to all pixels. Qiu et al. [6] proposed a novel H.264 watermarking method. The robust watermarks are embedded into DCT coefficients and fragile ones into motion vectors respectively. Watermarking method provides more payloads without degrading video quality greatly. But the watermark embedded in MVs is fragile and easy to be removed by simply recompression with the same quantization parameter. Chen et al. [8] proposed a H.264 semi-fragile video watermarking system. Watermarks are generated by block sub-band index (number of nonzero AC coefficients) and then to be embedded into the quantized DCT AC coefficients in I frames. Due to the watermark relating to nonzero AC coefficients, it is fragile for common image processing operations. Xu et al. [9] proposed a novel watermarking scheme for H.264 content-based video authentication. They consider the feature of H.264 to generate the spatial tampering watermark using the reliable features extracted from video frame blocks. Then it is embedded into the DCT coefficients in diagonal positions. The method can detect malicious manipulations and allow recompression.

The watermarking scheme can be divided into two parts. The first part is the feature extraction and the other one is the watermark embedding method. The commonest feature is gray threshold version. Tsai et al. [10] proposed multi-resolution image authentication. The watermark is generated by MSB bit planes. However, the gray threshold feature will always fail to detect tampered areas when the gray threshold feature of the falsification is same as the original one. Another feature is the edge. Zhang et al. [11] introduced a semi-fragile image watermarking algorithm. Filtered contour image derived from Canny edge detector is used as image feature to generate a watermark, then it will be embedded into the DWT transform domain. The traditional edge feature has redundancy due to the image texture. It will also fail when the tampered area has many texture details. The third one is dithered feature. Cheddad et al. [12] proposed a solution to resist the noise and a certain extent JPEG compression. Considering the local feature, the dithered feature will be like the gray threshold version. For the watermark embedding procedure, many researches have proved that transform domain methods have robust performance for semi-fragile watermarking methods [13-15].

In this paper, we propose a novel semi-fragile watermarking video content authentication approach. It utilizes a hybrid feature which combines gray threshold feature and relative total variation edge feature. Then the watermark is encrypted and embedded invisibly into the principal diagonal of 8×8 DCT coefficients. Finally, the tampered areas can be located by comparing the extracted watermark and the hybrid feature which is regenerated from the watermarked video. Experiments show the proposed scheme can distinguish malicious attacks from the common legitimate alterations, such as H.264 lossy compression, noise, Gaussian filtering and so on. It meets requirements of video content authentication.

The rest of the paper is organized as follows. In Section 2, the proposed watermark embedding and extraction algorithms are described. In Section 3, experimental result and performance analysis are presented. Finally, the conclusions are drawn in Section 4.

2 Proposed Approach

The proposed hybrid feature semi-fragile watermarking video content authentication approach has two parts: watermark embedding and watermark authentication procedures. The details will be described as follows.

2.1 Watermark Embedding Procedure

2.1.1 Hybrid feature watermark generation

The proposed watermark embedding procedure is shown in Fig. 1. Video sequence is divided into 3 types: I frame, P frame and B frame in H.264 video encoder. I frame uses the intra coding mode and it appears in the video sequence periodically. It only associates with spatial correlations in the image. Therefore I frame stability feature is used for generating watermarking information. Assume that the luminance component of the I-frame is Y, it has N_1 columns and N_2 rows (both N_1 and N_2 are multiples of 8), and total number of pixels is $N = N_1 \times N_2$. $Y(x,y)$ denotes the pixel, where $1 \leq x \leq N_1$ and $1 \leq y \leq N_2$. Each pixels $Y(x,y)$ has the range of gray levels [0, 255]. For a watermarking content authentication algorithm, efficient feature is very important. If the extracted feature can present the main semantic information, it is capable of the resistance to legitimate signal operations. It will be constant if the semantic information does not change. So our hybrid feature focuses on the main semantic information of the video images. The first part is gray threshold feature *GT*. The threshold in this paper is the adaptive median *med*. The gray threshold feature can be calculated as follows:

$$GT = \begin{cases} 1 & if \quad Y(x,y) \geq med \\ 0 & if \quad Y(x,y) < med \end{cases} \qquad (1)$$
$$med = median(Y)$$

where $median(Y)$ is the function to find the median of I-frame Y. We found if the frame is tampered, sometimes the average of the image will change. This changeable average will cause most of watermarks are changed. It is unacceptable in the video content authentication. These modified watermarks will cause many un-tampered areas are detected as tampered ones. Here, we use median instead of average. If the image is modified, the median of the frame will be constant or change a little. It will not cause the authentication failure.

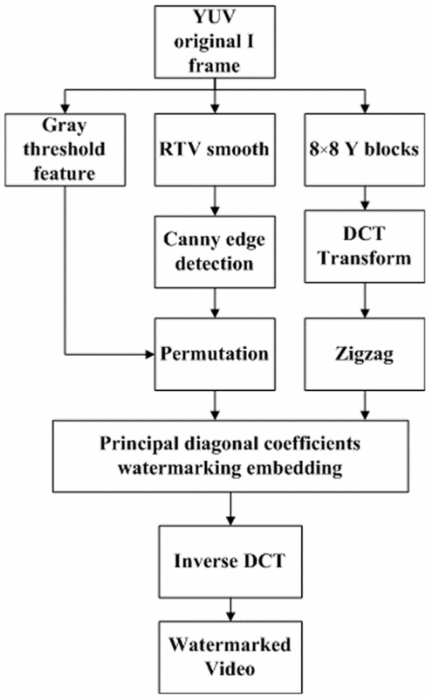

Fig. 1. Block diagram of the watermark embedding procedure.

The other part is the relative total variation (RTV) edge. It is a method to extract structure from texture [14]. Texture usually refers to surface patterns that are similar in appearance and local statistics. In content authentication applications, people may always not pay close attention to what the texture is. For example, it is not important for a video surveillance to distinguish how many leaves in the background, but we are always interested in cars or people on the street. So the texture may not be main semantic information. However, it can be difficulty to remove texture when details are complex and irregular. Representative structure-texture decomposition methods that do not require extensive texture information are those enforcing the total variation (TV) regularizer to preserve large-scale edges. In [14], Li et al. use a general pixel-wise windowed total variation measure and windowed inherent variation to distinguish prominent structures and to remove the saliency texture. They can be written as

$$D_x(p) = \sum_{q \in R(p)} g_{p,q} \cdot \left|(\partial_x S)_q\right|$$
$$D_y(p) = \sum_{q \in R(p)} g_{p,q} \cdot \left|(\partial_y S)_q\right| \qquad (2)$$

$$L_x(p) = \left|\sum_{q \in R(p)} g_{p,q} \cdot (\partial_x S)_q\right|$$
$$L_y(p) = \left|\sum_{q \in R(p)} g_{p,q} \cdot (\partial_y S)_q\right| \qquad (3)$$

Where q belongs to $R(p)$, the rectangular region centered at pixel p. S is the resulting structure image. $D_x(p)$ and $D_y(p)$ are the windowed total variations in the x and y directions for pixel p, which count the absolute spatial difference within the window $R(p)$. And $g_{p,q}$ is a weighting function. $L_x(p)$ and $L_y(p)$ are the windowed inherent variations in the x and y directions for pixel p, which helps distinguish prominent structures from the texture elements, besides $D(p)$. $L(p)$ captures the overall spatial variation. Different from the expression in Eq. (2), it does not incorporate the modulus. So the sum of ∂S depends on whether the gradients in a window are coincident or not, in terms of their directions, because ∂S for one pixel could be either positive or negative. More details of structure extraction from texture, please read Section 3 in [16]. You can get Matlab code from http://www.cse.cuhk.edu.hk/~leojia/projects/texturesep/. In this paper, the structure feature is extracted by RTV edge as follows:

$$Y_{RTV} = RTVsmooth(Y, \lambda, \sigma, sharpness, maxIter) \quad \textbf{(4)}$$

RTVsmooth$(\cdot)$ denotes the RTV smooth function. λ is the parameter to control the degree of smooth. And σ is the parameter specifying the maximum size of texture elements. *sharpness* controls the sharpness of the final results. *maxIter* is the number of iterations. According to experiments, we choose λ=0.01, σ =5, *sharpness*=0.01 and *maxIter*=10. The result Y_{RTV} will remove texture and maintain the principal structure information. Then the edge feature *EG* can be obtained using Canny edge detector.

When the original hybrid feature is generated, the amount of data is too large to embed into the cover image. In this paper, we only consider 8×8 DCT blocks, so two features *GT* and *EG* should be blocked. We just use 2 bit to represent *GT* and *EG*. The blocking functions are as follows:

$$GT_{(i,j)} = \begin{cases} 1 & if \sum_{k=1}^{8\times8} GT_{(i,j)}^{k} \geq \tau_{gt} \\ 0 & if \sum_{k=1}^{8\times8} GT_{(i,j)}^{k} < \tau_{gt} \end{cases} \quad \textbf{(5)}$$

$$EG_{(i,j)} = \begin{cases} 1 & if \sum_{k=1}^{8\times8} EG_{(i,j)}^{k} \geq \tau_{eg} \\ 0 & if \sum_{k=1}^{8\times8} EG_{(i,j)}^{k} < \tau_{eg} \end{cases} \quad \textbf{(6)}$$

where (*i, j*) denotes the indices of nonoverlapping 8×8 blocks. $GT_{(i,j)}^{k}$ and $EG_{(i,j)}^{k}$ are the *k*-th *GT* and *EG* coefficients in the (*i, j*) 8×8 blocks respectively. $GT_{(i,j)}$ and $EG_{(i,j)}$ denote the output *GT* and *EG* feature for each 8×8 blocks. τ_{gt} and τ_{eg} are predefined threshold. In other words, blocking functions make the hybrid feature become 2 bit. After blocking, the size of *GT* and *EG* becomes *N* respectively. Then *GT* and *EG* will compose the hybrid feature *HF*. Here, the 2 bit hybrid feature for each 8×8 DCT blocks. The LSB is gray threshold feature *GT*, and the MSB is the edge feature *EG*. In order to increase the security, the torus automorphism is used to permutate by a secret key, written as

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} (\bmod S) \quad \textbf{(7)}$$

where (*i, j*) is the original position and (*i', j'*) is the new position. *S* is a positive integer about the range of transformation. *k* is the random variable generated by a secret key. Finally, the original feature will be transformed and the watermark is generated.

2.1.2 Watermark Embedding

The input original cover frame *Y* will be segmented into nonoverlapping 8×8 blocks $Y_b(i,j)$. After DCT transform, we choose the principal diagonal coefficients to embed the watermark according to [14]. In other words, the embedding position is from 30 to 41 after zigzag scan. In this way, it has good stability for most attacks. The watermark embedding method is written as follows:

If *wm*=1, then

$$\begin{cases} C_k(u) = C_k(v) + QP, C_k(v) = C_k(u) - QP & if\ C_k(u) < C_k(v) \\ C_k(u) = C_k(u) + QP + s, C_k(v) = C_k(v) - QP - s & if\ C_k(u) = C_k(v) \end{cases} \quad \textbf{(8)}$$

If *wm*=0, then

$$\begin{cases} C_k(u) = C_k(v) - QP, C_k(v) = C_k(u) + QP & if\ C_k(u) > C_k(v) \\ C_k(u) = C_k(u) - QP - s, C_k(v) = C_k(v) + QP + s & if\ C_k(u) = C_k(v) \end{cases} \quad \textbf{(9)}$$

Here C_k denotes the principal diagonal coefficients. *u* and *v* are the embedding position. *s* is a small constant. *u* and *v* are position indices of diagonal DCT coefficients. *QP* is the H.264 quantization parameter. Because the quantized value Y_Q (*x,y*) can be given as

$$Y_Q(x,y) = round(Y(x,y)/QP) \quad \textbf{(10)}$$

where $round(\cdot)$ function rounds a number to the nearest integer. In order to maintain stability, the watermarking embedding adjustment factor should be large enough. If the adjustment factor is larger than *QP*, the watermarking approach will resist to the H.264 compression. So we employ QP as an adjustment factor.

In order to increase the robustness of a watermarking system, error correcting code is used. According to the embedding position *u* and *v*, the proposed method can embed 6 bit watermark in each 8×8 blocks. However, only 2 bits are hybrid feature. So we can embed 4 error correcting bits. Here, (6, 2) repetition code is used. For example, suppose the watermark is $\{01\}$, then the encoded watermark is $\{01|\,01|\,01\}$. In this way, at the receiver side, the watermark extraction will be more robust using majority logic decoding. After embedding watermark, the watermarked DCT block is inverse transformed. The original frame and watermarked frame are shown in Fig. 2(a) and (c). The hybrid feature is described as Fig. 2(b). It shows that the proposed algorithm satisfies perceptual invisibility.

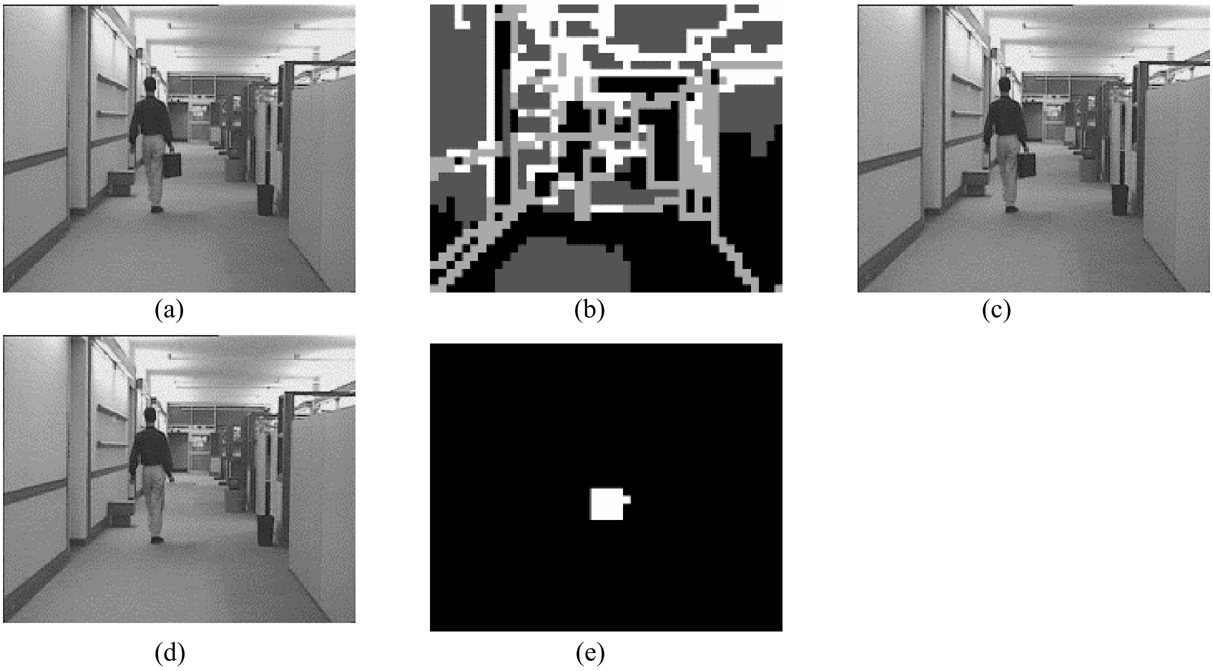

Fig. 2. (a) Original hall frame; (b) Hybrid feature; (c) Watermarked hall frame (PSNR=34.57) (QP=10); (d) Tampered watermarked frame; (e) Tampered area location map (Precision=0.83088, Recall=0.97835).

2.2 Watermark Extraction and Authentication Procedure

The proposed watermark extraction and authentication procedure is shown in Fig. 3. Suppose that an adversary has tampered some regions in a watermarked video with fake information as shown in Fig. 2(d). Once a watermarked video Y_t is input, the luminance component of the I-frame is extracted. The input I-frame will be divided into nonoverlapping 8×8 blocks, the watermark *wm'* will be extracted as follows:

$$\begin{cases} wm' = 1 & if \;\; C_k(u) > C_k(v) \\ wm' = 0 & if \;\; C_k(u) < C_k(v) \\ wm' = -1 & if \;\; C_k(u) = C_k(v) \end{cases} \tag{11}$$

wm' =-1 means the bit has an error. Because the original watermark has 4 bit redundancies, the *wm'* can be corrected by the duplicated information. The watermark will be inverse permutated, and then the extracted hybrid feature *HF'* is gained. The watermarked video Y_t will generate the hybrid feature *HF''* as the watermark embedding procedure. After subtraction, the original tampered area location map *TM* is created. The original tampered area location map often has some isolated points, so it needs post-processing. After the connected domain computation and some small areas removal, the final tampered area location map is generated in Fig. 2(e).

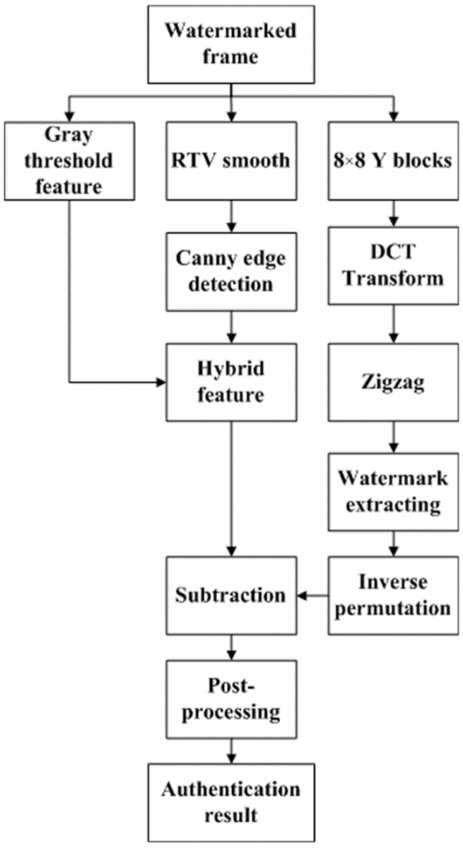

Fig. 3. Block diagram of the watermark extraction and authentication.

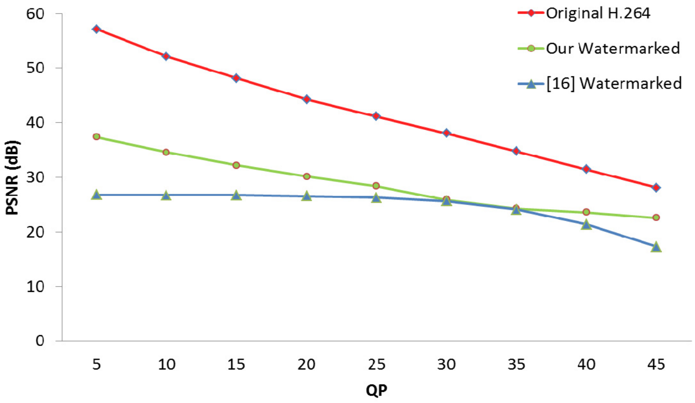

Fig. 4. Experimental result of the PSNRs (dB) of the watermarked with different QP.

3 Experiment Results

For the performance evaluation of our technique, we have conducted comprehensive sets of simulation experiments. Four 4:2:0 CIF YUV format video test sequences, Hall, Bus, Flower and News, are used in these experiments. The Hall video is based on a still camera and moving human. The Bus video is the video of cars on the street and contains more details. The Flower video is a free shooting in the complex environment. The News video represents news on the television which can also be seen as a videoconference. These video sequences are common as a proof in front of a court of law. The video compressed format employed in this paper is H.264. The software codec adopted is H.264 Baseline Codec in [17].

3.1 Imperceptibility Test

The perceptual invisibility can be seen in Fig. 2. An original frame from video Hall is shown in Fig. 2(a). The corresponding watermarked frame is Fig. 2(c). Besides subjective observation, the experimental result of the PSNRs (dB) of the watermarked with different compression quality is illustrated in Fig. 4. The first curve is the original H.264 PSNRs. The second one is our watermarked curve. The third curve is another semi-fragile watermarking algorithm [18]. They show that the proposed method has good perceptual invisibility. One of main reasons to reduce the quality is that our approach uses (6, 2) error correcting code. But this mechanism can increase the robustness.

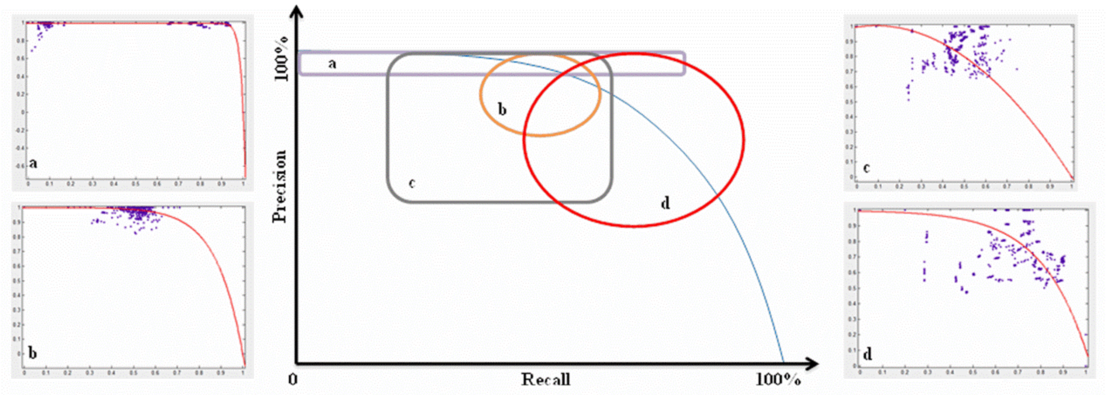

Fig. 5. Distribution of Precision-Recall points. a) Gray threshold feature, (b) edge feature, (c) relationship feature and (d) our proposed hybrid feature.

3.2 Tampering Detection

The most important security issue for authentication watermarking system is the block replacement attacks. The attacker would replace a watermarked block with another block to remove something important in the video. Fig. 2(d) gives a simulation result of the replacement attack. In the original watermarked test sequences Hall, a man with a briefcase is walking in the office in Fig. 2(a). The tampered version is shown in Fig. 2(d), where the briefcase is removed. We can see clearly that the man carried nothing in Fig. 2(d). Our proposed method can locate tampered areas in Fig. 2(e). A considerable amount of work on it has been done. According to Kerckhoffs's principle (i.e. a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.), the security of a good video authentication system should closely rely on the secret key. But less attention to openness and transparency of watermarking algorithm has been paid. In other words, most authentication methods have an assumption that attackers do not know the video has been watermarked and watermarking method. In this paper, suppose the embedding and extraction algorithms are public. The adversary finds the video has been watermarked and may extract the original watermark first, and then tamper the video. Finally, the original watermark will be re-embedded into the tampered frame. In this way, most previous methods are hard to detect. In order to show the excellent performance of the proposed hybrid feature, a Precision-Recall (PR) graph is presented in Fig. 5. We compare with four features: a) gray threshold feature, (b) edge feature (Canny), (c) relationship feature [9] and (d) our proposed hybrid feature. We test 100 frames per four test video sequences with different tampering proportion (10%~100%). Finally, the PR graph of different features is gained respectively in Fig. 5. If the PR point is in the upper right corner, its precision and recall are high. It has good detection performance. As shown in Fig. 5(a) area, gray threshold feature is extreme. The distribution of PR points is in the upper right corner and the upper left corner. It means that it sometimes can detect all tampering regions, and sometimes it will detect nothing. The relationship feature [9] is a feature which is generated by the relationship with some pixels in a block, as described in Eq. (2) in the literature [9]. Its PR points are in the upper. It has good precision performance. However, this feature will miss many tampering areas. The distribution of the edge feature is similar to the relationship one. However, both precision and recall are lower than the latter feature. The distribution of our proposed hybrid feature is in the upper right corner. It always has a stable performance to detect tampering areas.

Table 1 describes comparison results with 4 features: gray threshold feature (GT), edge feature (EG), relationship feature and our proposed hybrid feature. They have the same testing environment: QP=20 H.264 compression and two tampered areas, where the original watermark will be re-embedded. Precision and recall are employed as performance metrics. The subjective evaluation is used as a gauge of its authentication success. “T” denotes two tampered areas have been all located. “F” means tampered areas may be undetected. “F-1” means one of two tampered areas is not found. And “F-2” means both of tampered regions are not detected. According to the results in the Table 1, our proposed method has a more stable property among them. Our proposed method recall is higher than other methods. The detection tampered area in our method is a little bigger than the real tampered area, which covers the real region. So the precision decreases. But it will not miss some tampered areas.

Table 1. Comparison results with two tampered areas and H.264 compression (QP=20).
"T" denotes two tampered areas have been located. "F" denotes the tampered area is missed (-).

Video: Hall	GT	EG	Relationship	Proposed
Precision	0.76834	0.81032	0.7125	0.61279
Recall	0.44493	0.87726	0.35877	0.98741
Subjective evaluation	F-1	T	F-1	T
Video: Bus	GT	EG	Relationship	Proposed
Precision	0	0.74918	0.48549	0.60912
Recall	0	0.35838	0.34225	0.93548
Subjective evaluation	F-2	F-1	T	T
Video: Flower	GT	EG	Relationship	Proposed
Precision	0.72229	0	0.44364	0.70945
Recall	0.96381	0	0.31275	0.7502
Subjective evaluation	T	F-2	F-1	T
Video: News	GT	EG	Relationship	Proposed
Precision	0.84443	0.54115	0.51836	0.67253
Recall	0.48899	0.66381	0.52203	0.93761
Subjective evaluation	F-1	T	T	T

3.3 Robustness to Common Image Processing

In the scheme, the authentication will pass without any malicious attack. The watermarking method should be resistant to some common image processing attacks including recompression, Gaussian noise and filtering. In this paper, we use bit error rate (BER) to measure the robustness as illustrated in Table 2. The hybrid-feature watermark is embedded into the original video (QP=20). Firstly, we consider recompression attack with QP of 10 and 30. The average BER is approximately 0. That means our method can be resistant to recompression. Secondly, Gaussian noise is considered. The white noise of mean zeros and low standard deviance is added. The simulation results achieve the anticipation. If the noise is seen as a kind of texture, RTV will remove it away. So Hybrid feature can resist Gaussian noise. Finally, we examine the robustness of the proposed algorithm to Gaussian filtering. It also has satisfactory results. To sum up, our method can be resistant to other common legitimate alterations, such as recompression, noise and filtering.

Table 2. Robustness to common image processing.

Video (BER)	Recompression(QP=10)	Recompression(QP=30)	Gaussian noise (var=0.0001)	Gaussian noise (var=0.001)	3×3 Gaussian filtering
Hall	0	1.45%	0	2.08%	0
Bus	0	0.76%	0	0.63%	0.76%
Flower	0	0	0	0	0
News	0.82%	0	0	1.83%	0.69%

4 Conclusion

This paper presents a novel semi-fragile watermarking video content authentication using hybrid feature. The feature consists of gray threshold feature and relative total variation edge feature. The watermark is encrypted and embedded into the principal diagonal of 8×8 DCT coefficients. Embedding processing does not degrade the quality of the original video and be perceptually invisible to maintain its protective secrecy. The experiment demonstrates that the proposed method can distinguish malicious attacks from the common legitimate alterations. It is good at resistance to H.264 lossy compression, noise and Gaussian filtering. It has satisfactory performance to detect and locate malicious attacks. The proposed method is based on hybrid feature, which has higher recall. Thus, the method will meet the requirements of video tampered areas self-recovery applications. Self-recovery is a new idea to recover the original principal feature within the tampered areas. Therefore, higher recall is wanted to ensure all of the tampered areas are detected. Our method is very suitable for this new video content authentication application. In addition, the proposed watermarks are based on video contents, which can solve Kerckhoffs's principle problem. Thus it has practical application value.

The hybrid feature approach can resist high lossy compression (i.e. QP is more than 40). However, it still has some problems. First, in order to increase the robustness to lossy compression, error correcting code is used. But this will decrease the image quality. Second, there is too much noise in the image, such high standard deviance Gaussian noise and salt noise, so the authentication will fail. In the next step, this problem should be solved.

Acknowledgement

This work is supported by the PPP-Project, funded by the China Scholarship Council and the Deutscher Akademischer Austausch Dienst (DAAD).

References

[1] X. Li, Y. Shoshan, A. Fish, G. Jullien, O. Yadid-Pecht, “Hardware Implementations of Video Watermarking,” *Information Technologies & Knowledge*, Vol. 3, pp. 103-120, 2009.

[2] J. Fridrich and M. Goljan, “Images with Self-correcting Capabilities,” in *Proceedings of 1999 International Conference on Image Processing (ICIP 99)*, pp. 792-796, 1999.

[3] P. K. Atrey, W. Yan, M. S. Kankanhalli, “A Scalable Signature Scheme for Video Authentication,” *Multimedia Tools and Applications*, Vol. 34, No. 1, pp. 107-135, 2007.

[4] H. S. Wong, Y. R. Chen, J. S. Lee, “An Improved CRT-based Watermarking Scheme with Voting Strategy,” *Journal of Computers*, Vol. 22, No. 3, pp. 67-77, 2011.

[5] H. W. Liao, H. W. Huang, “A Multiple Watermarking Scheme for Gray-level Images Using Visual Cryptography And Integer Wavelet Transform,” *Journal of Computers*, Vol. 22, No. 1, pp. 18-36, 2011.

[6] G. Qiu, P. Marziliano, A. T. Ho, D. He, Q. Sun, “A Hybrid Watermarking Scheme for H. 264/AVC Video,” in *Proceedings of the 17th International Conference on Pattern Recognition (ICPR 2004)*, pp. 865-868, 2004.

[7] J. Fridrich and M. Goljan, “Images with Self-correcting Capabilities,” in *Proceedings of 1999 International Conference on Image Processing (ICIP 99)*, pp. 792-796, 1999.

[8] T. Chen, T. Chen, Y. Lin, Y. Chang, D. Wang, “H. 264 Video Authentication Based on Semi-Fragile Watermarking,” in *Proceedings of IIHMSP'08 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 659-662, 2008.

[9] D. Xu, R. Wang, J. Wang, “A Novel Watermarking Scheme for H. 264/AVC Video Authentication,” *Signal processing: Image Communication*, Vol. 26, No. 6, pp. 267-279, 2011.

[10] P. Tsai, Y. Hu, H. Yeh, W. Shih, “Multi-resolution Image Authentication Watermarking Based on Progressive Image Transmission,” *ISA 2012*, 2012.

[11] D. Zhang, Z. Pan, H. Li, “A Contour-based Semi-fragile Image Watermarking Algorithm in DWT domain,” in *Proceedings of 2010 Second International Workshop on Education Technology and Computer Science (ETCS)*, pp. 228-231, 2010.

[12] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "A Secure and Improved Self-Embedding Algorithm to Combat Digital Document Forgery," *Signal Processing*, Vol. 89, No. 12, pp. 2324-2332, 2009.

[13] S. Roy, X. Li, Y. Shoshan, A. Fish, O. Yadid-Pecht, "Hardware Implementation of a Digital Watermarking System for Video Authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, ID. 5318, 2012.

[14] T. Kuo, Y. Lo, "A Hybrid Scheme of Robust and Fragile Watermarking for H. 264/AVC Video," in *Proceedings of 2010 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, pp. 1-6, 2010.

[15] W. Chen, G. Zhang, G. Liu, "Algorithm Study on Video Watermarking Authentication Based on AVS in Compressed Domain," in *Proceedings of World Automation Congress (WAC)*, pp. 283-287, 2012.

[16] L. Xu, Q. Yan, Y. Xia, J. Jia, "Structure Extraction from Texture via Relative Total Variation," *ACM Transactions on Graphics (TOG)*, Vol. 31, No. 6, pp. 139, 2012.

[17] A. A. Muhit, M. R. Pickering, M. R. Frater, J.F. Arnold, "Video Coding Using Elastic Motion Model and Larger Blocks," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 20, No. 5, pp. 661-672, 2010.

[18] H. Chen, Z. Chen, X. Zeng W. Fan, Z. Xiong, "A Novel Reversible Semi-Fragile Watermarking Algorithm of MPEG-4 Video for Content Authentication," in *Proceedings of Second International Symposium on Intelligent Information Technology Application*, pp. 37-41, 2008.