http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (7): 1476-1482, 2010
ISSN 1812-5638

Quantization based Semi-fragile Watermarking Scheme for H.264 Video

[1]Yong Zhang, [2]Zhe-Ming Lu and [3]Dong-Ning Zhao
[1]ATR National Defense Technology Key Laboratory, School of Information Engineering,
Shenzhen University, Shenzhen, 518060, China
[2]School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, China
[3]Shenzhen Xitoy Science and Technology Co., Ltd, Shenzhen, 518060, China

Abstract: Although, many fragile video watermarking techniques have been proposed as an effective solution to content authentication problems, they cannot effectively distinguish between legal attacks and illegal attacks. In order to solve this problem, this paper proposes a novel semi-fragile video watermarking algorithm for H.264 video. Traditional fragile video watermarking methods often select the motion vectors as the embedding positions, while our scheme adopt the intra-prediction residuals after Integer DCT (Discrete Cosine Transform) and quantization to be embedding locations. During the watermark embedding process, we modify the standard H.264 quantizer and we embed the watermark based on the dither modulation technique in order to extract the watermark blindly. In the watermark extraction process, this paper adopts a threshold to distinguish between illegal attacks and legal attacks performed on the video clip. Experimental results demonstrate the effectiveness and feasibility of the proposed algorithm and the proposed scheme can survive legal recompression operations and recognize illegal filtering operations.

Key words: Content authentication, semi-fragile video watermarking, intra-prediction, integer DCT, H.264, quantization

INTRODUCTION

The explosive development of computer and Internet technologies has brought both opportunities and challenges to the multimedia industry. The possibility of lossless and unlimited copies of digital contents is a major obstacle from the owner's viewpoint for entering the digital world. Copy protection, copyright protection and content authentication have therefore been the three most important issues in the digital world. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Over the last decade, digital watermarking (Niu *et al*., 2000a, b; Lu *et al*., 2000; Lu and Sun, 2000; Fiaidhi and Mohammed, 2003; Qureshi and Tao, 2006) has been presented to complement cryptographic processes. Digital watermarking is the process of embedding information into a digital image (Niu *et al*., 2000a), audio (Yan *et al*., 2006) or video (Wang *et al*., 2005) in a way that is difficult to remove. If the signal is losslessly copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time (Wang *et al*., 2009a, b; Lu *et al*., 2003b, 2005). In general, there are two types of digital watermarks addressed in the existing literature, visible and invisible watermarks. A visible watermark (Luo *et al*., 2007; Pan *et al*., 2007; Lu *et al*., 2003b) typically contains a visible message or a company logo indicating the ownership of the image. On the other hand, the invisibly watermarked digital content appears visually very similar to the original. In literatures, the invisible watermark gains relatively more attention compared with visible watermarks. The invisible watermark may be intended for widespread applications. One application of watermarking is in copyright protection systems (Niu *et al*., 2000b; Lu *et al*., 2003c; Wang *et al*., 2005; Khan *et al*., 2008), which are intended to prevent or deter unauthorized copying of digital media. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark can be retrieved from the copy and the source of the distribution is known. Content authentication with fragile watermarks (Lu *et al*., 2003a) is another application branch of invisible watermarking. The illegal changes in the watermarked media may change the watermark accordingly such that we can know whether the media is authentic or not and further determine where, is altered. Annotation of digital

Corresponding Author: Zhe-Ming Lu, Teaching Building 5, Yuquan Campus, Zhejiang University, 38 ZheDa Road, Hangzhou 310027, People's Republic of China Tel/Fax:+86-571-87951589

photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself. It is also possible to use hidden embedded information as a means of covert communication (Lu and Li, 2006) between individuals.

With the rapid development of digital video processing technology, it becomes easier and easier to produce, copy, download, edit and transmit digital video. The authenticity and integrality of digital video products or evidences have been oppugned, thus content authentication or information forensics for digital video has become a hotspot in the content security field. Under this circumstance, digital video watermarking has been proposed as an important branch of digital watermarking. The research on video watermarking algorithms seems to be quite rare and most of early ones are extensions of still image watermarking algorithms. A large proportion of the proposed video watermarking algorithms are implemented in the uncompressed domain (Wang *et al*., 2005), namely the watermark is embedded in the raw video sequence and the watermarked sequence is consequently compressed for storage or transmission. The disadvantages of raw-domain video watermarking are: (1) the watermark extraction process is quite computation demanding; (2) the embedded watermark will be affected by lossy compression operations. On the contrary, in compressed domain video watermark algorithms, the watermark is directly embedded into the compressed stream and completely decoding is not necessary in watermark extraction. As a result, the compressed domain watermarking algorithm (Noorkami and Mersereau, 2005; Wang *et al*., 2009b) is much more feasible than those uncompressed domain ones. Most of compressed domain video watermarking algorithms are designed for copyright protection with robust watermarks. Noorkami and Mersereau (2005) proposed a low complexity scheme that embed one bit watermark in one of the quantized AC coefficients in each macroblock of I frames. Wu and Wang (2005) presented a blind watermarking algorithm that embeds the watermark in I frames. This scheme can survive H.264 compression attacks, but it requires the decompression operation during watermark embedding. Zhang and Ho (2005) proposed to embed gray-level images into the H.264 video. The idea is realized by encoding the sign of the diagonal coefficients in each 4×4 DCT block. This algorithm shows good robustness, high capacity and nice visual quality.

Recently, several fragile video watermarking algorithms have been proposed to embed watermarks in different positions using different schemes for different purposes. Park *et al.* (2002) proposed an invertible semi-fragile watermarking algorithm that uses a hash function to authenticate the video content, but it is not designed for H.264 but for MPEG-2. Qiu *et al.* (2004) proposed a hybrid watermarking scheme that embeds a robust watermark in the quantized DCT coefficients and a fragile watermark in the motion vectors and it is actually a multipurpose watermarking algorithm with multiple watermarks. Fragile watermarks are embedded in compressed video streams for error detection, not for content authentication (Chen *et al*., 2003). We think that the watermarking scheme in the compressed domain that cannot survive recompression attacks makes no sense, thus the proposed method recognizes the recompression attacks as legal attacks and other common attacks as illegal attacks. Based on above state-of-the art of fragile video watermarking, here we propose a novel semi-fragile video watermarking algorithm based on a modified H.264 quantizer. Our scheme is blind, which means we don't require the original video to extract the watermark from the watermarked video. In addition, our method can distinguish between illegal attacks and legal attacks performed on the video clip.

PROPOSED SCHEME

Traditional fragile video watermarking methods often select the motion vectors as the embedding positions, our scheme adopt the intra-prediction residuals after Integer DCT (Discrete Cosine Transform) and quantization to be embedding locations. During the watermark embedding process, we modify the standard H.264 quantizer and we embed the watermark based on the dither modulation technique in order to extract the watermark blindly. In the watermark extraction process, we adopts a threshold to distinguish between illegal attacks and legal attacks performed on the video clip. Here, we first introduce the H.264/AVC standard and then we present our modified H.264 quantizer for watermark embedding. We then introduce the dither modulation principle used in the watermark embedding process. Finally, we describe our watermark embedding and extraction steps.

H.264/AVC: H.264/AVC is the latest block-oriented motion-compensation-based codec standard developed by the ITU-T Video Coding Experts Group together with the ISO/IEC Moving Picture Experts Group (MPEG) and it was the product of a partnership effort known as the Joint Video Team (JVT). The ITU-T H.264 standard and the ISO/IEC MPEG-4 AVC standard are jointly maintained so that they have identical technical content. H.264 is used in such applications as Blu-ray Disc, videos from YouTube and the iTunes Store, DVB broadcast, direct-broadcast satellite television service, cable television services and real-time videoconferencing.

H.264/AVC/MPEG-4 Part 10 contains a number of new features that allow it to compress video much more effectively than older standards and to provide more flexibility for application to a wide variety of network environments. With regard to multi-picture inter-picture prediction, it uses previously-encoded pictures as references in a much more flexible way than in past standards and it employs variable block-size motion compensation (VBSMC) with block sizes as large as 16×16 and as small as 4×4 and it can obtain quarter-pixel precision for motion compensation. It uses weighted prediction, allowing an encoder to specify the use of a scaling and offset when performing motion compensation and providing a significant benefit in performance in special cases-such as fade-to-black, fade-in and cross-fade transitions. It adopts spatial prediction from the edges of neighboring blocks for intra coding, rather than the DC-only prediction found in MPEG-2 Part 2 and the transform coefficient prediction found in H.263v2 and MPEG-4 Part 2. With regard to new transform design features, it uses an exact-match integer 4×4 spatial block transform, allowing precise placement of residual signals with little of the ringing often found with prior codec designs and it also adopts an exact-match integer 8×8 spatial block transform, allowing highly correlated regions to be compressed more efficiently than with the 4×4 transform. Furthermore, it can perform adaptive encoder selection between the 4×4 and 8×8 transform block sizes for the integer transform operation. With regard to its quantization design, it adopts logarithmic step size control for easier bit rate management by encoders and simplified inverse-quantization scaling and frequency-customized quantization scaling matrices are selected by the encoder for perceptual-based quantization optimization.

Modified H.264 quantizer: In order to make the watermarking scheme robust to the legitimate video codec attack, we must find a way to embed watermarks in the low frequency of I frames. In general, if we embed the watermark into low-frequency DCT coefficients directly, it will result in two problems. One is that some of the watermarked low-frequency coefficients may be quantized later; the other is that embedding directly into low-frequency coefficients would extremely affect the visual quality. On the other hand, if we embed the watermark directly into high-frequency DCT coefficients, the watermark would be so fragile that it cannot survive the video codec attack, thus we cannot distinguish between legal and illegal attacks. Therefore, this paper proposes a scheme which takes the H.264 quantization characteristics into account during watermark embedding. The watermark is embedded still into low-frequency DCT coefficients, but not directly.

First, we briefly introduce the principle and mechanism of the H.264 quantizer (Richardson, 2003). In nature, the H.264 quantizer is improved from the classic quantizer whose expression is as follows:

$$Z_{ij} = \text{round}\left(Y_{ij} / Q_{step}\right) \qquad (1)$$

where, Z_{ij} denotes the quantized coefficient, Y_{ij} denotes the coefficient to be quantized, Q_{step} denotes the quantization step that varies from position to position and round () denotes the rounding off operation. Since the H.264 standard adopts the integer DCT, the coefficient matrix should be introduced in the quantizer, the Eq. 1 is therefore changed as:

$$Z_{ij} = \text{round}\left(W_{ij} \times \text{MF} / Q_{step}\right) \qquad (2)$$

where, W_{ij} denotes the coefficient to be quantized, MF denotes the corresponding value in coefficient matrix.

In present study, in order to implement Eq. 2 only with multiplication and shifting operations, Eq. 2 is further improved as follows:

$$\left|Z_{ij}\right| = \left(\left|W_{ij}\right| \times \text{MF} + f\right) >> \text{qbits} \qquad (3)$$

$$\text{sgn}\left(Z_{ij}\right) = \text{sgn}\left(W_{ij}\right) \qquad (4)$$

where, >>qbits means 0.5^{qbits}, f denotes the residual value and sgn () denotes the sign function. In general H.264 encoder configuration parameters, the quantization step is expressed as QP, which can be converted into qbits and vice versa. Therefore, we only need to alter the encoder configuration parameter QP to enhance the quantization level. Generally, the default QP value is 16. In this paper, the watermark is embedded into low frequency coefficients with the QP value 32. Since, the quantization step for watermark embedding is larger than that for the re-encoding attack, the watermark information can be preserved. Therefore, the watermark is robust to common video codec attacks but fragile to illegal attacks.

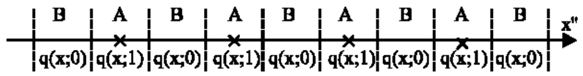

Fig. 1: The principle of dither modulation

The dither modulation principle: In order to extract the watermark blindly, we must design a watermarking scheme whose extraction process can be performed without the original video. Here, we adopt the dither modulation technique (Chen and Wornell, 2001) to embed the watermark in the video. The main idea of dither modulation is to quantize the original carrier data x to different quantization intervals according to the watermark information. Then we can detect the watermark bits according to the corresponding quantization intervals of carrier data in the x axis as illustrated in Fig. 1. If the quantized coefficient is in Interval A, then the watermark bit is 1; otherwise, if it is in Interval B, then the watermark bit is 0.

We embed a bit watermark into one of the AC coefficients after the 4×4 Integer DCT and quantization with dither modulation. The 16 coefficients can be denoted as Eq. 5:

$$Y_{(s,t)} = \bigcup_{k=0}^{15}\{Y_{(s,t)}(k)\} \quad 1 \le s \le M/4, 1 \le t \le N/4 \tag{5}$$

Here, the elements $Y_{(s,t)}(k)$ of $Y_{(s,t)}$ are in the Zig-Zag order and (s,t) means the two-dimensional coordinates of the DCT block in the frame. Assume that the watermark to be embedded is denoted as W(s,t) ∈ {0, 1}, the dither modulation process can then be described as follow:

Step 1: Divide the number axis into two kinds of intervals denoted as Interval A and Interval B according to the quantization step, as shown in Fig. 1

Step 2: Calculate the quotient m and remainder r of $Y_{(s,t)}(k)$ divided by the quantization step:

$$m = \text{floor}(Y_{(s,t)}(k)/\Delta + 0.5) \tag{6}$$

$$r = Y_{(s,t)}(k) - m\Delta \tag{7}$$

Step 3: Perform the dither modulation on $Y_{(s,t)}(k)$ according to the watermarking bit (0 or 1). There are four cases:

Case 1: If $Y_{(s,t)}(k) \ge 0$ and W(s,t) = 1:

$$Y'_{(s,t)}(k) = \begin{cases} 2k\Delta & \text{if } m = 2k \\ 2k\Delta + 2\Delta & \text{if } m = 2k+1 \text{ and } r \ge 0 \\ 2k\Delta & \text{if } m = 2k+1 \text{ and } r < 0 \end{cases} \tag{8}$$

Case 2: If $Y_{(s,t)}(k) \ge 0$ and W(s,t) = 0:

$$Y'_{(s,t)}(k) = \begin{cases} 2k\Delta + \Delta & \text{if } m = 2k \text{ and } r \ge 0 \\ 2k\Delta - \Delta & \text{if } m = 2k \text{ and } r < 0 \\ (2k+1)\Delta & \text{if } m = 2k+1 \end{cases} \tag{9}$$

Case 3: If $Y_{(s,t)}(k) < 0$ and W(s,t) = 1:

$$Y'_{(s,t)}(k) = \begin{cases} -2k\Delta & \text{if } m = -2k \\ -2k\Delta & \text{if } m = -(2k+1) \text{ and } r \ge 0 \\ -2k\Delta - 2\Delta & \text{if } m = -(2k+1) \text{ and } r < 0 \end{cases} \tag{10}$$

Case 4: If $Y_{(s,t)}(k) < 0$ and W(s,t) = 0

$$Y'_{(s,t)}(k) = \begin{cases} -2k\Delta + \Delta & \text{if } m = -2k \text{ and } r \ge 0 \\ -2k\Delta - \Delta & \text{if } m = -2k \text{ and } r < 0 \\ -(2k+1)\Delta & \text{if } m = -(2k+1) \end{cases} \tag{11}$$

where, the quantization step Δcan control the robustness of the embedded watermark. The larger the step Δis, the higher the robustness is and vice versa. Meanwhile, we can see that the maximum error caused by dither modulation is Δ.

Step 4: We extract the watermark as follows:

$$m = \text{floor}(Y'_{(s,t)}(k)/\Delta + 0.5) \tag{12}$$

If m is odd, then the watermark bit is 0. If m is even, then the watermark bit is 1. In this paper, we should meet the fragility to illegal video attack, so we set Δ =1.

Watermark embedding and extracting: Taking the video quality, the bit rate and human eyes' visually optimized mode into account (Watson, 1993), we perform a large number of experiments on coefficient selection and the results show that the third coefficient of the 4×4 DCT block in the Zig-Zag order is the optimal location to embed watermarks. Based on above descriptions, our proposed embedding procedure can be described as follows:

Step 1: Before embedding, we enhance the quantization step QP to make the embedded watermark robust to legal attacks such as recompression

Step 2: During the embedding process, we adopt the dither modulation with the step 1 to make the embedded watermark fragile to illegal attacks such as averaging filtering, Gaussian low-pass filtering, Laplacian filtering, linear motion filtering, median filtering, adding noises and scale zooming

Step 3: After embedding, we choose the best prediction model to achieve a balance between the video quality and the bit rate

The extraction procedure is the reverse process of the embedding procedure as follows:

Step 1: First, we decode the video streams and find the corresponding coefficient before inverse quantization

Step 2: Then, we determine which quantization interval of dither modulation the coefficient belongs to and get the watermark information

Step 3: Finally, we piece the watermark bits into a binary image and calculate the error rate of the extracted watermark

EXPERIMENTAL RESULTS

In experiments, the video sequence used in this paper is the standard Foreman testing sequence whose frame size is 352×288. Its macroblock and subblock sizes are 16×16 and 4×4, respectively. We embed one bit watermark information in each subblock, thus the total number of bits embedded is 6336, i.e., the embedding capacity is 6336 bits. In order to show the experimental result more intuitively, we adopt a binary image whose size is 88×72 = 6336 as the watermark to be embedded. Figure 2a shows the example original I frame and Fig. 2b shows the I frame after watermark embedding. Figure 3a shows the original watermark and Fig. 3b shows the extracted watermark without attacking, whose error rate is 0.55%.

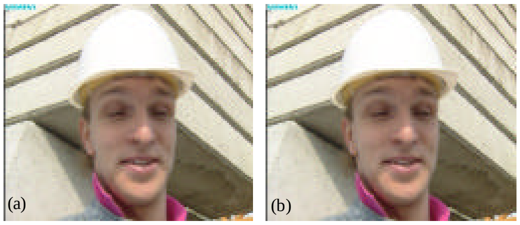

Fig. 2: Original and watermarked frames. (a) original frame and (b) watermarked frame

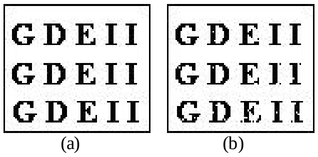

Fig. 3: (a, b) Original and extracted watermarks without attacking

In this study, we view the recompression attack as a legal attack, because the compressed-domain video will make no sense if it cannot survive the recompression operation. If someone encodes the video after decoding it without any processing, it should not be treated as a legal attack. In this experiment, the video will be encoded and decoded repeatedly, during which we will extract watermarks. The flow chart is shown in Fig. 4:

The experiment data is shown in Fig. 5, where, Fig. 5a-d are the watermarks extracted after once, twice, third, quartic recompression attacks, respectively. Figure 5e is the watermark extracted without any attack and Fig. 5f shows the original watermark. Table 1 shows the error rate of the extracted watermarks accordingly.

We cannot see from the data that the error rate of extracted watermarking is increased with increasing recompression times. After enough recompression operations, the error rate will become steady and less than some typical threshold 1.43%. The reason is that the pixel residuals will be integer multiple of quantification step after enough recompression operations. In other word, there is no extra space for compression, so there is no change.

Table 1: Watermarking error rates of several runs

Recompression times	0	1	2	3	4
Error Rate (%)	0.55	1.41	1.42	1.42	1.42
Picture label	(e)	(a)	(b)	(c)	(d)

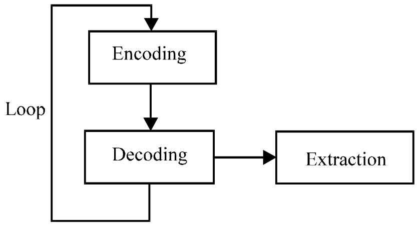

Fig. 4: The flow chart of the recompression operation

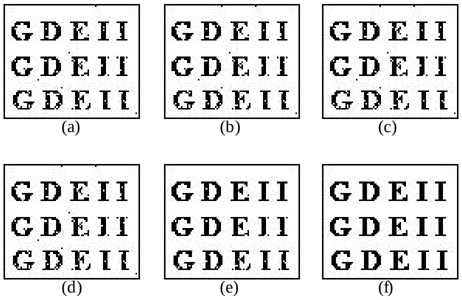

Fig. 5: (a-f) The extracted watermarks under the recompression attacks

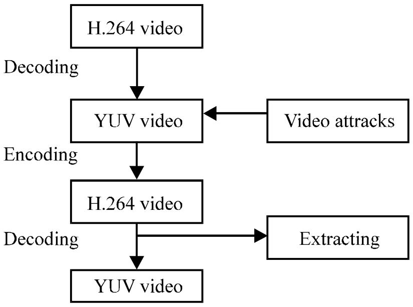

Fig. 6: The flow chart of illegal attacks

Table 2: Obtained error rates (%) after various kinds of attacks

Attack type	Recompression	Averaging filtering	Gaussian lowpass	Laplacian filtering
Error rate	1.42	80.38	1.64	8.90
Picture label	(a)	(b)	(c)	(d)
Attack type	Motion filtering	Median filtering	Adding noise	Scale zooming
Error rate	79.15	44.26	5.46	81.20
Picture label	(e)	(f)	(g)	(h)

As described above, the embedded watermark should have different responses to legal and illegal attacks, which can be seen from the error rate of extracted watermarking. We have tried several representative video attacks, such as averaging filtering, Gaussian low-pass filtering, Laplacian filtering, linear motion filtering, median filtering, adding noise and scale zooming. We extract watermarks after the video attacks above and the attacks are implemented by standard functions in Matlab7.0. The flow chart is given in Fig. 6. After experiment, we obtain their error rates in Table 2 and the extracted watermarks from the watermarked video under recompression, averaging filtering, Gaussian lowpass filtering, Laplacian filtering, motion filtering, median filtering, adding noise and scale zooming are shown in Fig. 7a-h, respectively.

We can see from the experiment that, the embedded watermark is sensitive to averaging filtering, Laplacian filtering, linear motion filtering, median filtering, adding noise and scale zooming. The reason is that the H.264 standard adopts the mechanism of encoding the residuals after intra-frame prediction while other encoding methods do not have. So, it is sensitive to pixel-level disturbance. The watermark is the least sensitive to Gaussian low-pass filtering. The main reason is that we embed the watermarking into low frequency part of the I frame image in order to resist the recompression attack. So, it is not sensitive to low-pass filtering. But we can still distinguish the low-pass filtering and recompression operations from the data carefully. Here we have tried every types of Gaussian low-pass filtering with different template sizes and sigma deviation values and we find 1.64% is the maximum error rate.

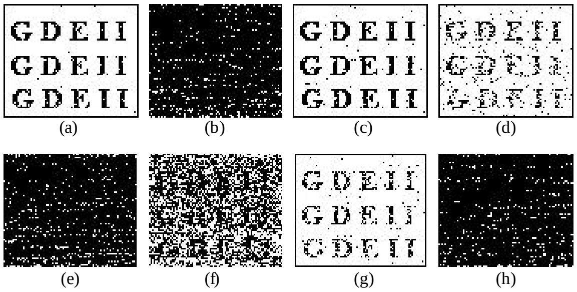

Fig. 7: (a-h) The extracted watermarks after various illegal attacks

We can see from the above experiments that, the error rate of the embedded watermark to legal attacks is no more than 1.43% and the error rate to illegal attacks is no less than 1.64%. So we can define the threshold as any value between 1.43 and 1.64%. Here we define it as 1.43%. The significance of the threshold is: if the error rate after video processing is less than the threshold, then we can judge that there are no illegal attacks on it; otherwise, if the error rate is more than the threshold, then we can judge that it must be attacked by some illegal attack.

CONCLUSIONS

In this study, we propose a fragile video watermarking algorithm based on the modified H.264 quantizer with the dither modulation technique. The watermark is embedded by modifying the residuals after DCT and quantization. We adopt the dither modulation to achieve the property of blind extraction. The quantizer is modified to embed the watermark into low frequency coefficients of each I frame image. The Lagrangian optimization function is adopted to achieve a balance between video quality and bit rate. Significantly, the proposed watermarking method can distinguish illegal attacks and legal attacks by the error rate of extracted watermark effectively.

ACKNOWLEDGMENTS

This study was supported by the Science and Technology Program of Shenzhen Government (Project No. JC200903120097A), the Scientific Research Foundation of Harbin Institute of Technology (Project Number: HIT.2003.52).

REFERENCES

Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans. Inform. Theory, 47: 1423-1443.

Chen, M.H., Y. He and R.L. Lagendijk, 2003. A fragile watermark error detection scheme for wireless video communications. IEEE Trans. Multimedia, 7: 956-958.

Fiaidhi, J.A.W. and S.M.A. Mohammed, 2003. Towards developing watermarking standards for collaborative e-learning systems. Inform. Technol. J., 2: 30-34.

Khan, A., X. Niu and Z. Yong, 2008. A robust framework for protecting computation results of mobile agents. Inform. Technol. J., 7: 24-31.

Lu, Z.M. and S.H. Sun, 2000. Digital image watermarking technique based on vector quantisation. Electronics Lett., 36: 303-305.

Lu, Z.M., J.S. Pan and S.H. Sun, 2000. VQ-based digital image watermarking method. Electronics Lett., 36: 1201-1202.

Lu Z.M., C.H. Liu and D.G. Xu, 2003a. Semi-fragile image watermarking method based on index constrained vector quantization. Electronics Lett., 39: 35-36.

Lu, Z.M., H.T. Wu, D.G. Xu and S.H. Sun, 2003b. A multipurpose image watermarking method for copyright notification and protection. IEICE Trans. Inform. Syst., E86-D: 1931-1933.

Lu, Z.M., W. Xing, D.G. Xu and S.H. Sun, 2003c. Digital image watermarking method based on vector quantization with labeled codewords. IEICE Trans. Inform. Syst., 86: 2786-2789.

Lu, Z.M., D.G. Xu and S.H. Sun, 2005. Multipurpose image watermarking algorithm based on multistage vector quantization. IEEE Trans. Image Process., 14: 822-831.

Lu, Z.M. and S.Z. Li, 2006. Multipurpose watermarking algorithm for secret communication. Chinese J. Electronics, 15: 79-84.

Luo, H., J.S. Pan and Z.M. Lu, 2007. Content adaptive visible watermarking during ordered dithering. IEICE Trans. Inform. Syst., 90: 1113-1116.

Niu, X.M., Z.M. Lu and S.H. Sun, 2000a. Digital watermarking of still images with gray-level digital watermarks. IEEE Trans. Consumer Electronics, 46: 137-145.

Niu, X.M., Z.M. Lu and S.H. Sun, 2000b. Digital image watermarking based on multiresolution decomposition. IEE Electronics Lett., 36: 1108-1110.

Noorkami, M. and R.M. Mersereau, 2005. Compressed-domain video watermarking for H.264. Proceedings of the IEEE International Conference on Image Processing, Sept. 11-14, Atlanta, Genoa, Italy, pp: 890-893.

Pan, J.S., H. Luo and Z.M. Lu, 2007. Visible watermarking for halftone images. IEICE Trans. Fundamentals Electronics Commun. Comput. Sci., E90-A: 1487-1490.

Park, J.Y., J.H. Lim, G.S. Kim and C.S. Won, 2002. Invertible semi-fragile watermarking algorithm distinguishing MPEG-2 compression from malicious manipulation. Proceedings of the International Conference on Consumer Electronics, June 18-20, IEEE Computer Society, pp: 18-19.

Qiu, G., P. Marziliano, A.T.S. Ho, D. He and Q. Sun, 2004. A hybrid watermarking scheme for H.264/AVC video. Proceedings of the 17th International Conference on Pattern Recognition, Aug. 23-26, Nanyang Technol. Univ., Singapore, pp: 865-868.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Richardson, I.E.G., 2003. H.264 and MPEG-4 Video Compression. John Wiley and Sons, New York, ISBN: 0-470-84837-5.

Wang, H.X., Z.M. Lu, J.S. Pan and S.H. Sun, 2005. Robust blind video watermarking with adaptive embedding mechanism. Int. J. Innovative Comput. Inform. Control, 1: 247-259.

Wang, H.X., Z.M. Lu, Y.N. Li and S.H. Sun, 2009a. A compressed domain multipurpose video watermarking algorithm using vector quantization. Int. J. Innovative Comput. Inform. Control, 5: 1441-1450.

Wang, Y.G., Z.M. Lu, F. Liang and Y. Zheng, 2009b. Robust dual watermarking algorithm for AVS video. Signal Process. Image Commun., 24: 333-344.

Watson, A.B., 1993. DCT quantization matrices visually optimized for individual images. Proceedings of the SPIE International Conference Human Vision, Visual Processing and Digital Display, Feb. 01, San Jose, CA, USA., pp: 202-216.

Wu, G.Z. and Y.J. Wang, 2005. Robust watermark embedding/detection algorithm for H.264. J. Electronics Imaging., 14: 013-013.

Yan, B., Z.M. Lu and S.H. Sun, 2006. Security of autoregressive speech watermarking model under guessing attack. IEEE Trans. Inform. Forensics Security, 1: 386-390.

Zhang, J. and A.T.S. Ho, 2005. Robust digital image-in-video watermarking for the emerging H.264/AVC standard. Proceedings of the IEEE Workshop on Signal Processing Systems Design and Implementation, Nov. 2-4, Nanyang Technol. Univ., Singapore, pp: 657-662.