

# Digital Authentication and Verification in MPEG-4 Fine-granular Scalability Video Using Bit-Plane Watermarking

**Chun-Ching Wang**  
Electrical Engineering  
Department,  
National Changhua  
University of Education,  
Changhua, Taiwan

**\*Yih-Chuan Lin**  
Computer Science and  
Information Engineering  
Department,  
National Formosa  
University, Yun-Lin,  
Taiwan

**Shu-Chung Yi**  
Graduate Institute of  
Integrated Circuit  
Design  
National Changhua  
University of Education,  
Changhua, Taiwan

**Po-Yu Chen**  
Electrical Engineering  
Department,  
National Changhua  
University of Education,  
Changhua, Taiwan

**Abstract**—This paper proposes a content authentication scheme for MPEG-4 FGS (fine-granular scalability) video based on digital fragile watermarking using Bitplane-Coding Watermarking (BCW). In embedding procedure, the watermark information is embedded into every  $8 \times 8$  block of residual bit-planes in the enhancement layer while encoding to MPEG-4 FGS video stream. The watermark bit is modulated by modifying a specified bit in each  $8 \times 8$  bit-plane such that the even/odd value of the total number of “1” bits can meet the corresponding watermark information. In extracting procedure, the embedded signal can be detected from each block of residual bit-planes by judging the total number of “1” bits in the block is even or odd. The detected signal is used to localize errors and claim ownership of the video content by decoding it to copyrights information. It is worth mention that we use run-length coding steps to select the optimal position for embedding watermark information in order to increase the coding efficiency. Experimental results are presented validating the effectiveness of the proposed approach. It is found that our proposed method needs no complicated computation. Furthermore, we found that the compression ratio is increasing due to the selection of optimal position for imposing the watermark.

**Keywords:** MPEG-4, FGS, content authentication, digital watermarking, bit-plane.

## 1 Introduction

Digital watermarking [1-6] is a scheme for embedding watermarking information into multimedia, which can be later extracted for a variety of purposes including identification and/or authentication purposes. This issue is becoming increasingly important due to the proliferation of multimedia contents on the Internet and in electronic commerce. The watermarking technique can be either fragile [1-3] or robust watermarking [4-6] relying on the

desire of the application. The fragile watermarking scheme can detect any modification made to the multimedia and indicate the specific locations that have been modified. Any modification would be resulted in a corresponding error in the watermark. If the content was not watermarked, or if the watermarked content is lost, the watermark extraction algorithm will reflect the multimedia that resembles random noise. The robust watermarking is verifying the validity of copyright by detecting watermark. The watermarking should satisfy at least two conditions such as the transparency and robustness to protect copyrights of multimedia data. The watermark signal should cause minimal degradation of the host data in order to be imperceptible, and it should be robust against various kinds of manipulations or corruptions for the multimedia data.

The newly adopted MPEG-4 fine granularity scalability (FGS) video coding standard [7-10] has received tremendous attentions because it has ability to adapt to the network bandwidth variation. MPEG-4 FGS encodes video sequences into two bit streams: a non-scalable motion-compensated base layer and a fine-granular-scalable enhancement layer. The base layer is a video sequence at the lower bound of a bit-rate range. The enhancement layer encodes the difference between the reconstructed sequence and the original sequence from the base layer in a scalable manner to offer a range of bit rates for the sequence. However, it is fairly easy to modify the video stream captured by the video camera, e.g. mask out of specific event or person, a system for proving authenticity and integrity of video streams is needed. This paper presents such a system based on digital signatures embedded in the video stream. Our concept provides a method for proving authenticity and integrity of MPEG-4 FGS digital video streams. In addition, the watermarked MPEG-4 FGS stream can be played by the ordinary MPEG-4 FGS decoder, because this scheme does not violate MPEG-4 FGS encoding standards. For more detailed information can refer [7-10]

The rest of this paper is organized as follows. Section 2 briefly reviews the basic concepts of watermarking and

MPEG-4 FGS coding. The bitplane-coding watermarking algorithm is presented in section 3. The resulting performance evaluation and comparison are described in section 4. Finally, conclusion is made in section 5.

## 2 Proposed Watermark Embedding

In this paper, the watermark information is embedded into the enhancement layer of MPEG-4 FGS to detect the integrity of video stream. Since fragile watermarking has extremely low resistance for various attacks, the extracted watermark signal fairly easy lose its completeness when multimedia content is modified or changed by a pirate or hacker. Thus, the multimedia can be determined where it has been changed or modified illegally according to the completeness of extracted watermark. In this paper, we propose a BCW (Bitplane-Coding Watermarking) algorithm to add watermark information to the residual bit-planes of enhancement layer. The BCW is very simple and effective. In embedding procedure, the watermark information is embedded into every  $8 \times 8$  block of residual bit-planes in the enhancement layer while encoding to MPEG-4 FGS video stream. The watermark bit is modulated by modifying a specified bit that is selected from each  $8 \times 8$  bit-plane such that the even/odd value of the total number of “1” bits can meet the corresponding watermark information. We propose a run-length-selection method to determine the specified position of each block in residual frame for embedding the watermark bit. The specified bit is then modified by the corresponding watermark bit. Due to employing the run-length-selection method, our proposed watermarking not only achieves an efficient and simple watermarking method but also obtains a better performance for the run-length coding. From extracted watermark, we can detect the completeness of multimedia content. The main reasons for hiding watermark into enhancement layers is that minimal degradation of the host data can be imperceptible as the watermark signal is inserted into the enhancement layer. Comparing with the base layers, these enhancement layer video stream data has less effect to the whole video quality. Therefore, we develop the bit-plane-watermarking method in the enhancement layer.

## 3 Bitplane-Coding Watermarking

### 3.1 MPEG-4 FGS Encoder with Information Embedding Scheme

The basic idea in MPEG-4 FGS is to encode a video sequence into a non-scalable base layer and a scalable enhancement layer. The base layer is typically encoded at a very low bit rate. The FGS profile is used to obtain the enhancement layer to achieve optimized video quality with a single stream for a wide range of bit rates. More precisely, each frame’s residue, i.e., the difference between the

original frame and the corresponding frame reconstructed from the base layer is encoded for the enhancement layer in a scalable manner: DCT coefficients of the residue are compressed bit-plane wise from the most significant bit to the least significant bit. Figure 1 illustrates the proposed MPEG-4 FGS encoder with information embedding scheme using BCW algorithm. Let  $w_i$  denote the  $i$ -th watermark bit and  $T_j$  denote the total number of “1” bits in the  $j$ -th  $8 \times 8$  bit-plane. We want to embed the watermark  $w_i$  into the  $k$ -th specified bit  $B_k$  in  $j$ -th bitplane, the detail of embedding watermarking can be described as follows. First, we choose the specified bit ( $k$ -th bit) in the  $j$ -th bitplane by the proposed run-length-selection algorithm for embedding  $i$ -th watermark bit. The run-length-selection algorithm can determine a specified bit for embedding watermark in  $8 \times 8$  residue bit-plane and obtaining an optimal coding efficiency in run-length coding. The detail of run-length-selection algorithm will be described in next subsection. If  $w_i$  is “1”, then  $T_j$  will be enforced to be as an odd value. Similarly, if  $w_i$  is “0”, then  $T_j$  will be enforced to be as an even value. That is, the specified bit  $B_k$  can be modified as  $B'_k$  by the following expression.

$$B'_k = \begin{cases} 0 & \text{if } w_i \oplus E(T_j) = 0 \\ 1 & \text{if } w_i \oplus E(T_j) = 1 \end{cases} \quad (1)$$

where  $E(T_j) = (T_j + 1) \bmod 2$ , and “ $\oplus$ ” denote exclusive OR operation.

### 3.2 Run-Length-Selection Algorithm

The reason for choosing the bit of  $8 \times 8$  residue bit-plane for embedding watermark can be described as follows. In the embedding procedure, the chosen bit may increase the length of run-length coding such that coding efficiency for MPEG-4 FGS will increase. In the enhancement layer FGS coding, after zigzag scanning applied in the  $8 \times 8$  residue bit-plane, the run-length symbols (RUN, EOP) is obtained. The RUN value of (RUN, EOP) means the run-length, and the EOP indicates whether the end bit is achieved or not. That is, if the value of EOP is “1”, it means that the coding of the bit-plane is completed. Otherwise, the coding of the bit-plane is not completed. In the special case of bit-plane are all zero, it is processed by using special coding for ALL ZERO. As described above, an  $8 \times 8$  bit-plane may have one or more than one (RUN, EOP) except ALL ZERO.

To achieve the goal of increasing the coding efficiency of MPEG-4 FGS, we choose the specified bit for embedding watermark signal such that the new RUN value is the biggest run-length among all (RUN, EOP) in the same block when the specified bit is modified. Fig. 2 shows an example of run-length-coding algorithm for hiding watermark. Fig 2(a) shows the block data before and after the watermark bit is embedded, respectively. Before the watermark bit is embedded, the run-length is (8, 0), (13, 0), (18, 0), (10, 1). After the watermark bit is embedded, the

run-length sequences are (8, 0), (32, 0), (10, 1). In Fig 2(a), the 2<sup>nd</sup> “1” bit is chosen to be changed as ‘0’ based on the run-length-coding, hence the recalculated (RUN, EOP) are (8, 0), (32, 0), (10, 1), which is the optimal run-length coding after modifying watermarking bit. Therefore, the high compression rate can be achieved by run-length-coding algorithm. Fig 2(b) shows the block data after embedding watermark.

### 3.3 MPEG-4 FGS decoder with information extracting scheme

Fig 3 illustrates the schematic diagram for extracting watermark. If  $E(T_j)$  is 1, the extracted watermarking data is “1”. Otherwise, if  $E(T_j)$  is 0, the extracted watermarking data is “0”. The equation for extracting watermark can be expressed as following:

$$w_i = \begin{cases} 0 & \text{if } E(T_j) = 1 \\ 1 & \text{if } E(T_j) = 0 \end{cases} \quad (3)$$

where  $w_i$  ( $i=0, 1, 2, 3, \dots$ ) is the  $i$ -th data of watermark. In the proposed watermark extracting, the received EL stream with watermarking data can be decoded to bit planes through VLD at receiver end. After that, watermarking can be easily extracted by Eq.(2), as detailed illustration of Fig 3. Our watermark extracting algorithm is very easy, only needs the calculating of bit 1, and needs not to memorize the position of watermarking data. Hence, it is suitable for developing watermarking technique in the fine-granularity-scalability video stream transmission. Fig. 4 shows an example of extracting watermark from the blocks of residual bit-plane.

## 4 Experiment Results

To demonstrate the effectiveness of our development, the computer simulation was performed. The test sequences, Mobile, Bus, Akiyo, and Foreman, are selected in our experiment to cover a variety of video characteristics. The performance evaluation of the proposed BCW algorithm includes watermarked video quality, attacking test and compression rate. We describe these simulations as follows.

### ● Watermarked Video Quality

To prove the watermarked video is an acceptable quality, we employ the PSNR to estimate the differences between original video and watermarked video. The PSNR is expressed by

$$PSNR = 10 \log_{10} \frac{255^2}{\left(\frac{1}{M \times N}\right) \sum_{i=0}^M \sum_{j=0}^N (\alpha_{ij} - \beta_{ij})^2} \text{ dB} \quad (4)$$

where  $M, N$  are the length and width of the video frame, respectively.  $\alpha_{ij}$  and  $\beta_{ij}$  denote the pixel value of original video frame and watermarked video frame respectively.

The original watermark is binary image of size 40×40 shown in Fig. 5. Consider a block residing in the LSB with size of 8×8 in the MPEG-4 FGS coding. We want to insert an original watermark bit into this block to form a watermarked block. Note that the number of bits of original watermark needs not the same number as blocks of LSB. In our example, we form the embedded watermark by tiling the original watermark, i.e., periodically replicating to the desired size. Then the quality experiment of watermarked video is evaluated by Eq.(3). Fig 6 illustrates the comparisons of frames with and without bitplane-coding watermarking. Fig. 6(a) is the frame without BCW with PSNR of 44, and Fig. 6(b) is the frame employing BCW with PSNR of 43.35dB. No noticeable artifacts can be observed. Fig 7 shows the PSNR of certain continuous frames of “Bus” video sequences. It is found that the quality of watermarked video does not change a lot and is still in the acceptable range of vision.

### ● Attacking Test

A good authentication watermarking can detect and localize any change to the video, including changes in frame rate, video size or related video object. If the watermarked video is attacked by frame removing, and then the watermark extracting procedure is applied on the attacked video, the procedure returns a false alarm to indicate that the video content becomes incomplete. Also, if one change the size of watermarked video and then one applies the watermark extraction procedure on this resized video, the procedure returns an output that resembles random noise, meaning a false alarm. Similarly, if one modifies certain related video object, then the procedure will output a false alarm. Fig. 8 describes some experimental results of attacking test.

### ● Compression Rate

Table 1 shows improvement of compression rate with and without BCW algorithm. The result indicates that the proposed algorithm may really increase compression rate. This is a significant contribution in the watermarking issue.

## 5 Conclusion

In this paper, we propose a simple and effective bitplane-coding watermarking technique, which not only provides a significant solution for the authentication of MPEG-4 FGS video sequence but also improves the coding efficiency. The proposed algorithm needs no complicated computations while hiding or extracting watermark. In our watermarking scheme, each bit-plane is watermarked using a smart run-length-selection such that the longest run-length can be obtained. Due to its structural simplicity, the proposed coding technique can be easily mapped onto a high-speed, low-complexity, and low-power circuit design.

Performance evaluation reveals that our development outperforms the MPEG-4 FGS based bitplane-coding watermarking by degrading the PSNR in about 1.8 dB on average. However, the quality of watermarked video is acceptable for the naked eyes and the compression rate may further increases.

## References

- [1] Ping Wah Wong and Nasir Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification", *IEEE Trans. on Image Processing*, Vol. 10, No. 10, Oct. 2001, pp. 1593-1601.
- [2] C.-T. Li, "Digital fragile watermarking scheme for authentication of JPEG images", *IEE Proc.-Vis. Image Signal Processing*, Vol. 151, No. 6, December 2004, pp. 460-466.
- [3] Min Wu and Bede Liu, "Watermarking for image authentication", *IEEE Conference on Image Processing*, 1998, pp.437-441.
- [4] Xia-Mu Niu; Zhe-Ming Lu; Sheng-He Sun, "Digital watermarking of still images with gray-level digital watermarks", *IEEE Trans. on Consumer Electronics*, Vol. 46, Issue: 1, Feb., 2000, pp.137 – 145.
- [5] C. Hsu and J. Wu, "Hidden digital watermarks in images," *IEEE Trans. on Image Processing*, Vol. 8, No. 1, Jan., 1999, pp.58-68.
- [6] K. Hashida and A. Shiozaki, "A method of embedding robust watermarks into digital color images," *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*. Vol. E81-A, No.10,1998, pp.2133-2137.
- [7] Hayder M. Radha, Member, Mihaela van der Schaar, and Yingwei Chen, "The MPEG-4 fine-grained scalable video coding method for multimedia streaming over IP" *IEEE Trans. on Multimedia*, Vol. 3, No. 1, Mar., 2001, pp. 53-68.
- [8] Weiping Li, "Overview of fine granularity scalability in MPEG-4 video standard" , *IEEE Transactions on Circuits and Systems for Video Technology*, Vol.11, No.3, Mar., 2001, pp. 332-344.
- [9] M. van der Schaar, Y. Chen, and H. Radha, "Embedded DCT and wavelet methods for fine granular scalable video: Analysis and comparison," in *IVCP 2000, Proc. SPIE*, vol. 2974, Jan. 2000, pp. 643–653.
- [10] "International Standard" ISO/ICE 14496-2:2001/Amd. 2:2002(E).

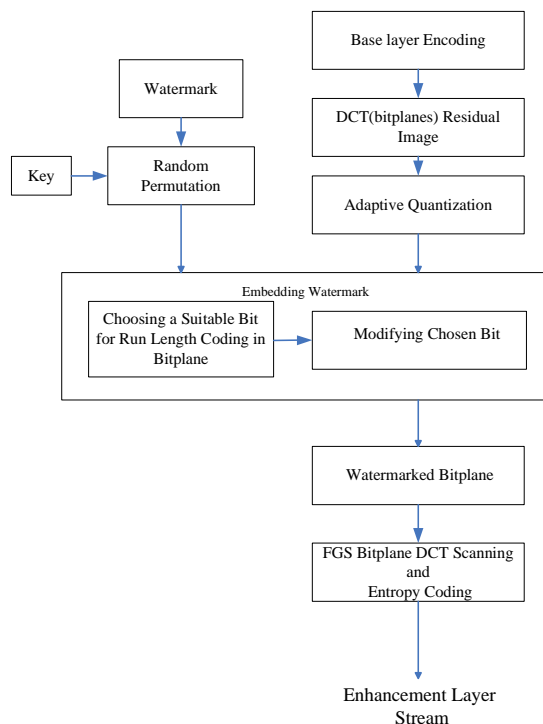


Fig. 1. Block diagram of proposed watermark embedding.

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0
0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(a) Block data before embedding.

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(b) Block data after embedding.

Fig.2. An example of BCW algorithm for hiding watermark.

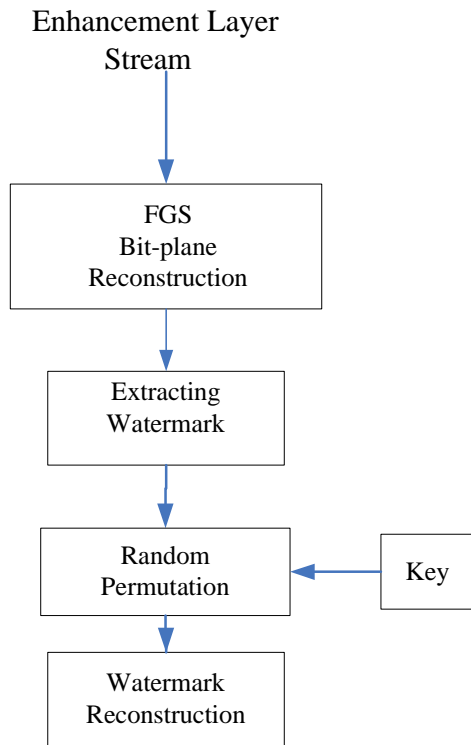


Fig. 3. Block diagram of proposed watermark extracting.

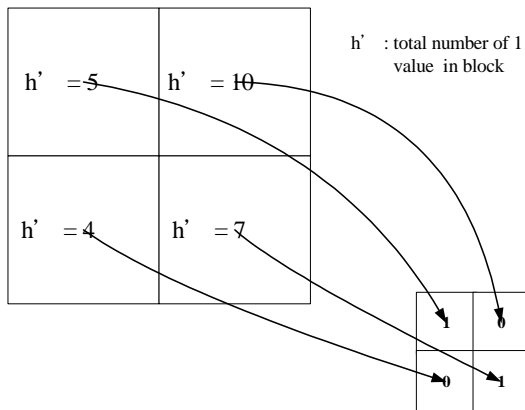


Fig. 4. An example of extracting watermark from the blocks of residual bit-plane.



Fig. 5. Original watermark of size 40x40 binary image.



(a)



(b)

Fig. 6. The comparisons of video quality with and without proposed watermarking (a) 44.63dB (b) 43.35dB.

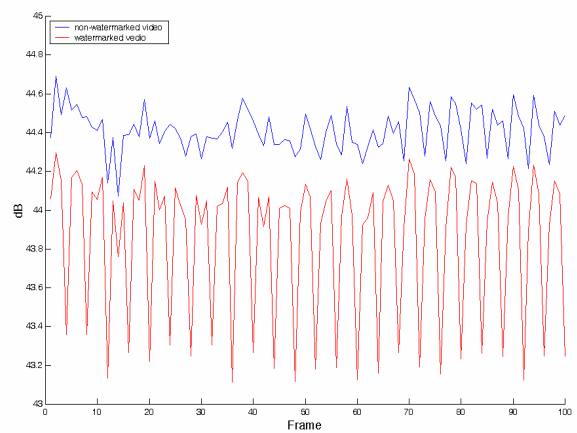


Fig. 7. PSNR from first ten frames in "Bus" video sequence with and without watermark.

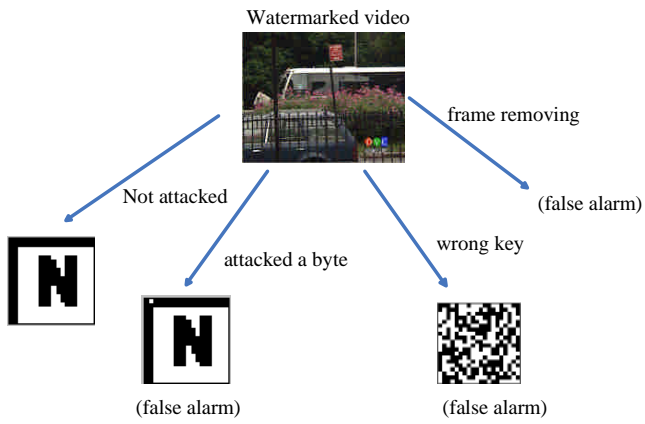


Fig 8. Experimental results of attacking test

Table 1. Improvement of compression rate with BCW algorithm.

File name	File size of without watermark	File size of watermarked video	Improve of compression rate
Akyio	4074KB	3921KB	3.8 %
Bus	4897KB	4810KB	1.8%
oreman	7709KB	7536KB	2.2%
Mobile	14200KB	14027 KB	1.2%