Mathematical Model for Digital Video Watermarking based on 3D Wavelet Transform

Sonam A. Bhandari
B.E. COMP,
S.N.J.B.'s K.B.J. COE
CHANDWAD.

Amar D. Rana
B.E. COMP,
S.N.J.B.'s K.B.J. COE
CHANDWAD.

Swati Z. Bhandari
B.E. COMP,
S.N.J.B.'s K.B.J. COE
CHANDWAD.

Vaibhav A. Kalange
B.E. COMP,
S.N.J.B.'s K.B.J. COE
CHANDWAD.

Mahesh R. Sanghvi
Research Scholar
Jodhpur National University, Jodhpur

ABSTRACT:

The protection of intellectual property rights became recently a pressing need especially with the rapid growth of transmission techniques. In this paper, we present a mathematical model of a copyright protection method a blind video scene segmentation and 3D wavelet transform according to scene change. Mathematical model will be easier way to explain any sort of problem for research point of view first gray scale image as copyright sign is decomposed with different resolution of the decomposed video. As the multiresolution of the video is for spatial axis of the video. The experimental results show that this technique has more visually recognizable information of copyright ownership. In addition, these results proved its robustness against several video degradations and watermarking attacks including frame dropping, frame averaging and glossy compression.

Keywords

Video watermarking, security, copyright protection, access control, wavelet transform

1. INTRODUCTION

Recently there has been great emphasis on the networking area which is related to the multimedia components and the information explained through it. The 21st century is the more advancing age of internet and related contents, highly exposing data which innovated before a minute or say as to some seconds. All the data exposes by internet related to multimedia blocks like either it was in text format or Image format or via video format. In this session accessing, transmission of the data leads to problems relating to security, ownership, copyright protection. Whatever the algorithms created for providing some security to multimedia data like encryption-decryption key, steganography, cryptography etc. that's gives protection only up to the end-user but what after next? The end-user may be broadcast it on to the non-authorized broadcasters or by some technique he/she will make some profit without permission of its real owner, It is the point where the watermarking technique comes in the path of multimedia technology and protection scheme by adding an invisible or visible and non-erasable content on the multimedia data which is readable by only that individual who have the key to extract it.

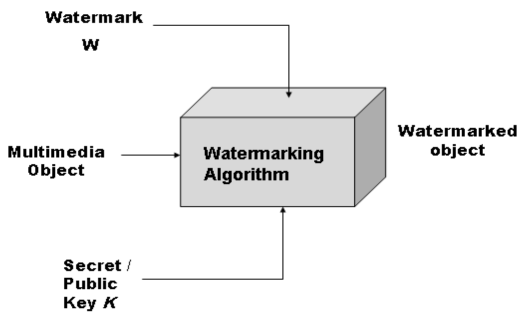

Fig 1: Basic Watermarking scheme

Digital watermarking technology mainly applied for content authentication, copyright protection, ownership, traffic monitoring, privacy tracking etc. There are two types of watermark, a robust watermark, which is designed to resist attack (malicious or not) in order to detect the mark. Secondly, a fragile watermark, which gets vanished when the source document is corrupted.

Many algorithms established for watermarking multimedia data but still no one was so much identical. There are so many attacks on which previous algorithms doesn't get proper result what the programmer expects as well as no one algorithms doesn't propose any mathematical module for their algorithms. Mathematical module is nothing but models describe our beliefs about how the world functions. In mathematical modeling we translate those beliefs into the language of mathematics. Mathematics is a very precise language. This helps us to formulate ideas and identify underlying assumptions. There is a large element of compromise in mathematical modeling. The majority of interacting systems in the real world are far too complicated to model in their entirety. Hence the first level of compromise is to identify the most important parts of the system. These will be included in the model, the rest will be excluded. The

second level of compromise concerns the amount of mathematical manipulation which is worthwhile. Mathematics has the potential to prove general results; these results depend critically on the form of equations used. Mathematical modeling can be used for a number of different reasons. How well any particular objective is achieved depends on both the state of knowledge about a system and how well the modeling is done.
This paper is organized into four sections. The previous section covers the Introduction. Next section describes literature review & findings. Section III describes the details of the proposed scheme. The Mathematical module is shown in Section IV. Section V presents a conclusion and the future work.

2. LITERATURE SURVEY

Various comprehensive investigations on the existing watermarking technologies have been accomplished. And it has been discerned that none of the recent watermarking schemes can resist all sorts of attacks. With this outcome, this paper proposes a mathematical model for a robust scheme for digital video watermarking based on 3D wavelet according to scene change.
Literature review reveals that watermarking schemes can be crudely divided into two classes: spatial domain, and transformed domain. Some of the spatial domain techniques discussed are:

2.1 Spatial Domain Techniques

The watermark is applied in the pixel domain. Combination with the host signal is based on simple operations, in the pixel domain. The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. However, they also exhibit a major drawback: The need for absolute spatial synchronization leads to high susceptibility to desynchronization attacks. Some spatial domain techniques are explained here.

Least Significant Bit (LSB) Technique is most straightforward method of watermark embedding would be to embed the watermark into the least significant bits of the cover object [1].

Predictive coding schemes exploit the correlation between adjacent pixels by coding the prediction error instead of coding the individual values.

In Binary Image Watermarking a binary image is a digital image that has only two possible intensity values for each pixel. The two values are often 0 for black, and either 1 or 255 for white. In binary image watermarking embed a binary watermark in binary image. Usually it is much difficult to embed a watermark in binary image than in gray scale or colored image. The reason is that for binary image there are only two bits per pixel. So, change in any bit will change the pixel entirely [2].

2.2 Frequency Domain Techniques

Here we embed watermark in DCT, DFT, FFT domains etc. The main strength offered by transform domain techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. A possible disadvantage of spatial techniques is that they are not very robust against attacks.

2.2.1 DCT based Watermarking Techniques:

The classic and still most popular domain for image processing is that of the Discrete Cosine Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). One such technique utilizes the middle-band DCT coefficients to encode a single bit into a DCT block [3].

2.3 Wavelet Domain Techniques

Most of the researchers focus on embedding watermark in wavelet domain because watermarks in this domain are very robust. The existing wavelet based watermarking techniques are explained below:

Xia, Boncelet, and Arce proposed [4]a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark is detected. Otherwise, the image is decomposed into finer and finer bands until the entire, extracted watermark is correlated with the entire, original watermark. This technique proved to be more robust than the DCT method.

Lu et al. proposed a novel watermarking technique called as "Cocktail Watermarking" in (1999) [5]. It is a blind watermarking technique. This technique embeds dual watermarks which complement each other. This scheme is resistant to several attacks, and no matter what type of attack is applied, one of the watermarks can be detected.

In (1999) Zhu et al. has presented a multi-resolution watermarking technique for watermarking video and images [6]. The watermark is embedded in all the high pass bands in a nested manner at multiple resolutions. This technique doesn't consider the HVS (Human Visual System) aspect; however, Kaewkamnerd and Rao improve this technique by adding the HVS factor in account.

Voyatzis and Pitas (1999), provide a technique to embed binary logo as a watermark, which can be detected using visual models as well as by statistical means[7]. So in case the image is degraded too much and the logo is not visible, it can be detected statistically using correlation. Watermark embedding is based on a chaotic (mixing) system. Original image is not required for watermark detection. A similar approach is presented for the wavelet domain, where the authors propose a watermarking algorithm based on chaotic encryption.

X. Niu and S. Sun had proposed new wavelet-based digital watermarking for video in 2000[8]. In this all video frames have been transformed in to wavelet domain and watermark is embedded in to all video frames. Scheme is robust against the frame dropping.

Lu et al. (2001) present another robust watermarking technique based on image fusion [9]. They embed a grayscale and binary watermark which is modulated using the "toral automorphism" described in. Watermark is embedded additively. The novelty of this technique lies in the use of secret image instead of host image for watermark extraction and use of image dependent and image independent permutations to de-correlate the watermark logos.

Raval and Rege have proposed a multiple watermarking technique in (2003)[10]. The authors argue that if the watermark is embedded in the low frequency components it is robust against low pass filtering, lossy compression and geometric distortions. On the other hand, if the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus to achieve overall robustness against a large number of attacks the authors propose to embed multiple watermarks in low frequency and high frequency bands of DWT.

Tao and Eskicioglu (2004) present an optimal wavelet based watermarking technique [11]. They embed binary logo watermark in all the four bands. But they embed the watermarks with variable scaling factor in different bands. The scaling factor is high for the LL sub band but for the other three bands its lower.

Zhao et al. (2004) present a dual domain watermarking technique for image authentication and image compression [12]. They use the DCT domain for watermark generation and DWT domain for watermark insertion.

Dragos N. Vizireanul, Radu O. Preda proposes a digital image watermarking scheme for image copyright protection using wavelet packets [13]. The basic idea is to decompose the original image into a series of details at different scales by using Wavelet Packets; a binary image used as a watermark is then embedded into the different levels of details. This algorithm does minimal degradation to the original image and can improve the robustness of watermarking against different attacks.

2.4 Findings

From above literature survey it can be concluded that the main strength offered by wavelet domain techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. A possible limitations of spatial techniques is that they are not very robust against attacks. In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain.
Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions. Taking these aspects into consideration, working in a frequency domain and wavelet domain are more robust techniques as well as no any mathematical model is proposed until now on wavelet based watermarking. Hence this paper proposed a mathematical model on watermarking in wavelet domain.

3. PROPOSED WATERMARKING SCHEME - MATHEMATICAL MODEL

1) Decomposition of gray level watermark image

Considering a watermark, in origin, should be a visually recognizable pattern, we adopt 2-D gray level digital image (64x64) as a watermark. In order to embed the watermark invisibly, the watermark information should adapt itself to the detail of original video. Hence, we decompose the watermark into a multiresolution hierarchical structure of images L0, L1 and G2 by the resolution-reduction method described in literature [14][15]
Here 'S' is the system. $\boldsymbol{S} = \{\boldsymbol{G}, \boldsymbol{Gp}, \boldsymbol{Gpi}, \boldsymbol{Lp}, \boldsymbol{V}, \boldsymbol{F}, \boldsymbol{Sc} | \emptyset \boldsymbol{s}\}$

G_0 = 2D gray level image as watermark (64x64)

Gp = Gaussian pyramids [3 x 3]

Gpi = Gaussian pyramid interpolation

Lp = Lapacian pyramids

a) $G_0 \times G_p = G_1 (32 \text{ x } 32)$
$G_1 \times G_p = G_2 (16 \text{ x } 16)$
b) $G_1 \times G_{pi} = G_1{}' (32 \text{ x } 32)$
$G_2 \times G_{pi} = G_2{}' (16 \text{ x } 16)$
c) $G_0 \times L_p = L_0 (64 \text{ x } 64)$
$G_1 \times L_p = L_1 (32 \text{ x } 32)$
d) $(L_0 \wedge L_1 \wedge G_2) \times Dcom = Bitplane\ Pixel(W)$

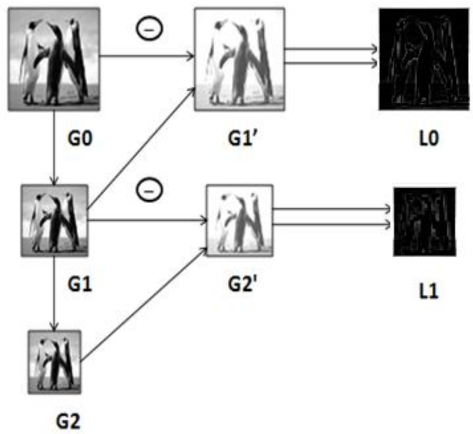

Fig 2: The first three levels of the pyramid Structure of an image

So, this can be the result after the preprocessing of watermark image where G0, G1' and L0 are 64x64. G1, G2' and L1 are 32x32 and G2 is 16x16. Also G1' and G2' are the interpolated images.

2) Decomposition of video

For watermarking the motion content of video, we decompose the video sequence into multiresolution temporal representation with a 2-band or 3-band perfect reconstruction filter bank by 1-D Discrete Wavelet Transform (DWT) along the temporal axis of the video. To enhance the robustness against the attack on the identical watermark for each frame, the video sequence is broken into scenes and the length of the 1-D DWT depends on the length of each scene. Let N be the length of a video scene, Fk be the k-th frame in a video scene and WFk be the kth wavelet coefficient frame. The Wavelet frames are ordered from lowest frequency to highest frequency i.e., WF0 is a DC frame. The wavelet coefficient frame WFk is decomposed into multiresolution representation by the 2D discrete Wavelet transform 2DDWT.

$$V = \{Sc_0, Sc_1, Sc_2, \dots Sc_m\}$$

$Sc_i = Scenes\ in\ a\ video, 0 \leq i < m$

$m = Total\ no.of\ Scenes$

$Sc_0 = \{f_0, f_1, f_2 \dots f_{a-1}, f_a\}$

$Sc_1 = \{f_{a+1}, f_{a+2} \dots f_{b-1}, f_b\}$

…

$Sc_m = \{f_{b+1}, f_{b+2} \dots f_{c-1}, f_c\}$

$f_i = Video\ frames, 0 \leq i < n$

$n = Total\ no.of\ frames$

$TDWT = Temporal\ DWT$

a) $f^k \times TDWT = Wf^k$
$Wf = \{wf^o, wf^1, wf^2 \dots wf^{n-1}\}$
$Where\ frequency\ of\ wf^0 < wf^1 < wf^2\ \dots < wf^{n-1}$

b) $Wf^k \times 2DDWT = V'$

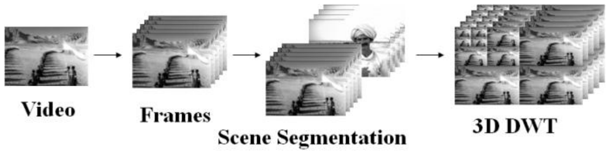

Fig 3: Video Decomposition Process

As shown in above fig., a video can be converted in the number of scenes and then scenes into the frames. Then the watermark can be added in the LH1, HL1, LH2, HL2, LH3 and HL3 coefficients of frames.

3) Watermark Embedding procedure

a) Generating the pyramid structure of the watermark image and decomposing them into bitplanes. Pseudo-random permutation of the bitplane.
b) For robustness to the common picture-cropping processing, a fast two-dimensional pseudo-random number traversing method is used to permute each bitplane of the watermark image to disperse its spatial location for the sake of spreading the watermarking information.
c) Modification of 2-D DWT Coefficients

$C[i] = i^{th}\ DWT\ coefficient\ of\ video\ frame$

$W[j] = j^{th}\ pixel\ of\ certain\ bitplanes$

a) $if\ W[j] = 1$

$C[i] = \max(C[i], C[i+1], C[i+2], C[i+3])$

$C[i+1] = \min(C[i], C[i+1], C[i+2], C[i+3])$

$Elseif\ W[j] = 0$

$C[i] = \min(C[i], C[i+1], C[i+2], C[i+3])$

$C[i+1] = \max(C[i], C[i+1], C[i+2], C[i+3])$

Hence only DWT coefficient of HL1, LH1, HL2, LH2, HL3, and LH3 are watermarked.

d) Inverse of 2-D DWT and 1-D DWT

4) Watermark Extracting Procedure

The watermark extraction does not requires the original video. The extraction steps are as follows:
a) The watermarked video is broken into scenes and each scene is decomposed into multiresolution temporal representation (a series of wavelet coefficient frames) by 1-DDWT along the temporal axis of the video. Each video frame is transformed to wavelet domain by 2-D DWT with 3 levels.
b) Watermark is extracted from the frames by checking the magnitude of some DWT coefficients to extract the 8 bitplanes of images L0, L1 and G2. The condition is shown as follow:
V= watermarked video

Pr = Pseudo-random permutation

Cmp = Composition

Bp = Bit plane

$f^k \times TDWT = Wf^k$

$Wf = \{wf^0, wf^1, wf^2 \dots wf^{n-1}\}$
$Where\ frequency\ of\ wf^0 < wf^1 \dots < wf^{n-1}$

c) The pseudo-random permutation is reversed according to the predefined pseudo-random order for these bitplanes.
$wf^k \times 2D\ DWT = V'$
$W[j] = 1 \quad if\ WC[i] > WC[i+1]$
$W[j] = 0 \quad Otherwise$
$V_w \times P_r = V'$

d) By composing these bitplanes into the graylevel images G2, L1, and L0, the extracted watermark is reconstructed.
$B_p \times Cmp = (G^2 \wedge L^1 \wedge L^0)$

4. CONCLUSION

This paper proposes a mathematical model of blind video watermarking scheme in the 3D wavelet transform using a gray scale image as a watermark. Mathematical model is easier way to understand the system. The process of this video watermarking scheme, including watermark preprocessing, video preprocessing watermark embedding, and watermark detection, is described in detail. Experiments are performed to demonstrate that our scheme is robust against attacks by frame dropping, frame averaging, and lossy compression.

REFERENCES

[1] N. Memon, ―Analysis of LSB based image steganography techniques Chandramouli,‖ in *Proc. 2001 Int. Conf. Image Processing*, vol. 3, Oct. 2001, pp. 1019–1022.

[2] M. Wu, E. Tang, and B. Liu, "Data hiding in digital binary image," *in Proc. IEEE Int. Conf. on Multimedia and Expo*, New York City, pp. 393-396, July 31 to August 2, 2000.

[3] F. Duan, I. King, L. Xu, and L. Chan, ―Intra-block algorithm for digital watermarking,‖ in *Proc. IEEE 14th Int. Conf. Pattern Recognition*, vol. 2, Aug. 1998, pp. 1589–1591.

[4] Xiang-Gen Xia, Boncelet, C.G., Arce, G.R., "A multiresolution watermark for digital images", *in the proc. of IEEE International Conference on Image Processing*, Vol. 1, pp 549 – 551, Oct 1997.

[5] "Announcing the Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, November 2001.

[6] Kaewkamnerd, N., Rao, K.R., "Wavelet based image adaptive watermarking scheme" *in IEE Electronics Letters*, vol.36, pp.3 12-313, 17 Feb.2000.

[7] Voyatzis, G., Pitas, I., "Digital Image Watermarking using Mixing Systems", *in Computer Graphics, Elsevier*, vol. 22, no. 4,pp. 405-416, August 1998.

[8] Xiao, W., Ji, Z., Zhang, J., Wu, W., "A watermarking algorithm based on chaotic encryption", *in Proc. of IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering TENCON*, vol. 1, pp. 545-548, 28-31 Oct. 2002.

[9] Lu, C. S., Huang, S.-K., Sze, C.-J., Liao, H.-Y., "A new watermarking technique for multimedia protection," *in Multimedia Image and Video Processing*, pp. 507 –530, 2001.

[10] Raval, M.S., Rege, P.P., "Discrete wavelet transform based multiple watermarking scheme", *conference on Convergent Technologies for Asia-Pacific Region*, TENCON 2003, vol. 3, pp. 935 - 938, 15-17 Oct. 2003.

[11] Tao, P & Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", *in Symposium on Internet Multimedia Management Systems V, Philadelphia, PA*, 2004.

[12] Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", *in IEEE Transactions on linage Processing*, vol. 13, no. 3, pp. 430-448, March 2004.

[13] Vizireanu, D.N., Preda, R.O., "A New Digital Watermarking Scheme for Image Copyright Protection using Wavelet Packets", *in 7th International Conference of IEEE on telecommunications in Modern Satellite, Cable and Broadcasting Services*, Vol. 2, pp. 518 – 520, Sept. 2005.

[14] Xiamu Niu, Shenghe Sun " A New Wavelet-Based Digital Watermarking for Video", 9th IEEE Digital Signal ProcessingWorkshop[C].Texas,USA:IEEE,2000.

[15] P.J.Burt and E.H. Adelson, "The Laplacian Pyramid as a Compact Image Code", IEEE Trans. On Communications, Vol.31, No.4, April 1983, pp.532-54

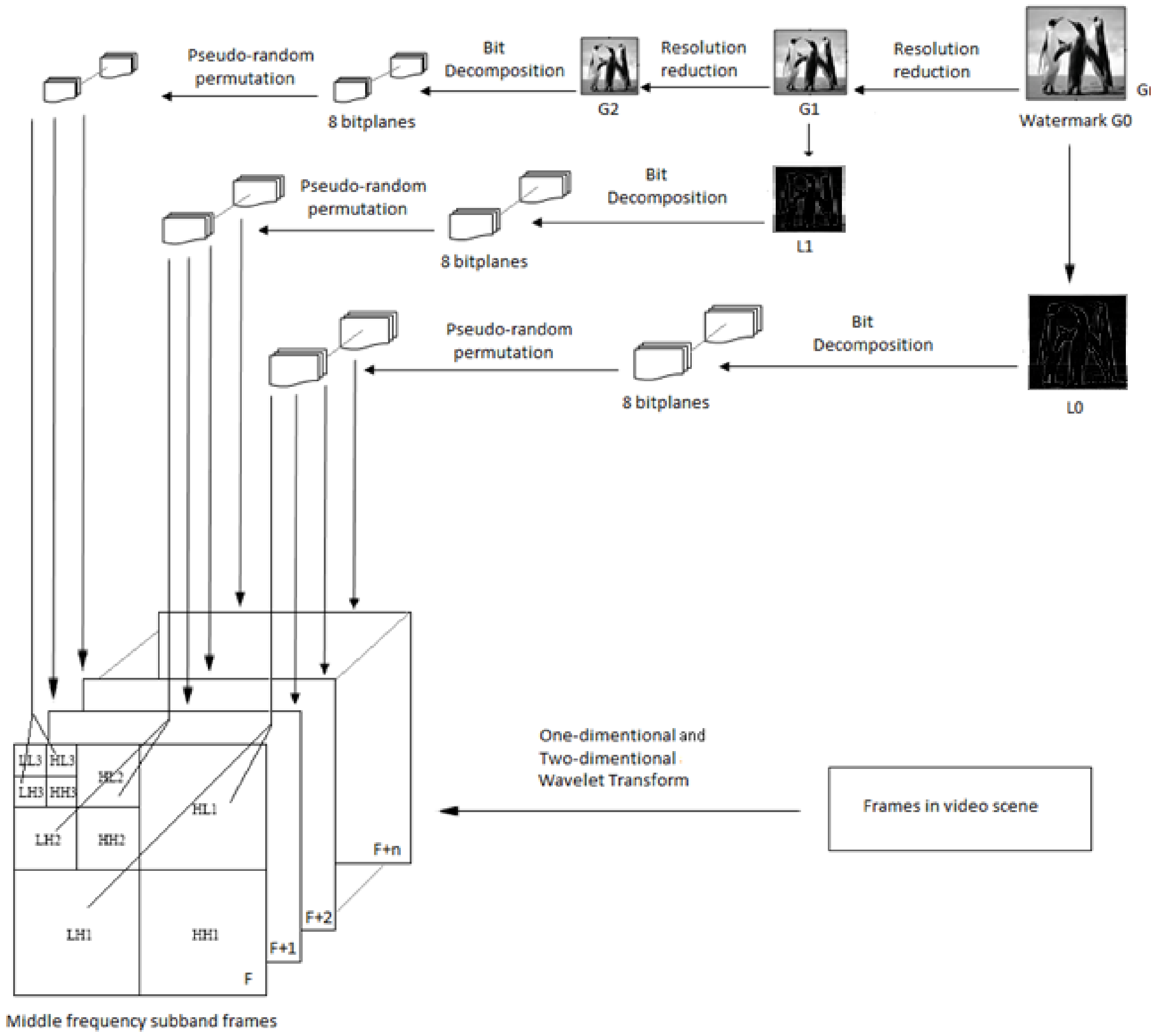

Fig 4: Video Watermarking embedding scheme diagram