Robust Watermarking for Video Using Mean Modulation Technique

Zainab J. Ahmed\textsuperscript{1*}, Loay E. George\textsuperscript{2}

\textsuperscript{1}Department of Biology Science, College of Science, University of Baghdad, Baghdad, Iraq.
\textsuperscript{2}Department of Remote Science and GIS, College of Science, University of Baghdad, Baghdad, Iraq

Abstract
This paper is directed toward the task of embedding a robust invisible watermark in the found sprite object (survive object) in each Group of Video (GOV). The proposed system is designed to provide authentication and protection to video by embedding invisible watermark. Three different watermark data embedding methods have been developed and used; they are: (i) Blocks average modulation applied on RGB domain, (ii) Blocks average modulation applied on Y-band only, and (iii) Haar wavelet approximation modulation. Uniform quantization is used as part of hiding step for modulating the block mean value of one or more of the color bands. The conducted tests indicated that the proposed block mean modulation method in the Y-subband of sprite blocks offer excellent robust watermark embedding; it was capable to withstand against lossy JPEG and JPEG2000 compression attacks.

Keywords: Watermark, MPEG-4, Sprite, I-frame, Motion Compensation, Haar, JPEG, JPEG-2000.

Introduction
Due to the recent explosive growth in the digital technique and internet usage recently, a new set of challenging problems had been created (like, authentication, content integrity and verification of the
digitized properties, copyright protection). Over the last few years, watermarking has proved to be the solution to these problems [1]. Video watermarking refers to embedding watermarks in a video sequence in order to protect the video from illegal copying and identify manipulations.

A variety of robust and fragile video watermarking methods have been proposed to solve the illegal copying and proof of ownership problems as well as to identify manipulations[2]. Watermarking can be considered as a part of information hiding [3]. Watermark can be kept visible on file or it can be hidden in the file as required. Visible watermarks can be a logo or text on frames of videos either in all frames or in just a few selected frames. Invisible watermarks or Hidden watermarks on other hand are present in the file in such a way that they cannot be sighted but have to be extracted [4]. Several algorithms have been developed to handle the problem of MPEG-4 video watermark. Zhang et al. proposed a video watermarking technique to hide copyright information in MPEG motion vector. In this method, watermark is embedded in larger value motion vectors, and especially in the less phase angle changed component. Then, the motion vector is modified into a new bitstream from which the watermark information can be easily retrieved. From the experimental results, it indicates that to embed watermark in motion vector has the advantage of little degrading the video quality, little influence on the MPEG decoding speed, capability to embed watermark in a short video sequence, and can be used to watermark on both the uncompresssed and compressed video sequence [5]. Meftin introduced a method for copyright protection for digital media (video) by embedding a digital image for video sequences compressed according to the MPEG-1 video coding standard. She implemented the third degree B-spline curve equation on intra-frame (I-frames) MBs data to interpolate data, then using a comparing condition to select location (effective points) where the watermark image could be embedded. The used B-spline curve fitting equation shows the distribution of watermark location through the intra-frame (I-frames) of MPEG-1 standard by drawing curves depending on watermarked points as control points [6]. Sinha et al. brought a novel approach to embed a robust visible and invisible watermark into video frames, such that the authenticity of the original signal is maintained. They used Discrete Wavelet Transform (DWT) and standard deviation to determine the region of less information, then, they embedded the watermark. The embedding is based on scene change analysis. This method provided more protection to the owner's information [7]. Rekka and Jayalakshmi presented a secure algorithm called DCT domain watermarking in MPEG-4, which could survive against video compression procedures and the attacks attempting to remove the watermark, with a visibly degraded video quality result after the watermark attacks [8].

The objective of this paper is to embed a robust watermark (secret message) in the allocated sprite object (i.e., survived region) in each Group of Video (GOV) using modulation technique; this will lead to robust watermarked video against video attacks. The introduced digital video watermarking system provides authentication and copyright protection for video contents by embedding invisible (imperceptible) watermark. The evaluation was done using a similarity measure applied on the watermark before and after attack. The watermark must be resistant against attacks. The embedding process will be based on three types of modulations; they are: (i) Blocks average modulation applied on RGB domain, (ii) Blocks average modulation applied on Y-band only, and (iii) Haar wavelet approximation modulation.

**The Proposed Video Watermark System**

In the proposed system, the watermark is embedded in the sprite region in I-frame of each GOV, and then later the embedded watermark can be extracted. The watermark embedding stage should be done by the original copyright owner of video. The watermark can be, later, extracted to prove authenticity. Thus, the watermarking process involves two stages: **Embedding stage and Extraction stage**. The layout of the proposed system is illustrated in Figure-1; it is similar to that mentioned in Ahmed & George article [9].

1. **Embedding Unit**

In this unit, for embedding the invisible watermark in the I-frame the block mean modulation technique is utilized. In this technique the watermarked I-frame can be viewed very similar to the original. The existence of an invisible watermark can only be determined using an appropriate watermark extraction or detection algorithm. This unit has four primary modules; these modules contain essential steps whose tasks are focused toward producing the suggested video watermark.
A. Load Video Data

The video frames belong to each GOV are loaded as BMP raster still images. Each GOV consists of N frames (in this paper work it was taken 10). Then, the values of the gray component of the pixels belong to each frame is calculated [9][10][11].

B. Motion Compensation

Motion compensation is applied to assess the motion vectors of the blocks that belong to predictive frames; motion compensation scheme to that in the previous work [10] was executed.

C. Sprite Region Allocation

A simple and fast method to allocate sprite objects (or areas) in the reference frame of each Group of Video (GOV) was adopted [11]; the system allocates the sprite blocks using motion compensation information. The outcomes of motion compensation have been used as key data for tracking the motion history of all scene blocks in order to detect the survived regions (sprite regions) in I-frame.

D. Watermark Data Embedding

The sprite region is identified and flagged as host block; each of these blocks will be used as individual place for hosting one bit of the watermark message. The applied modulation technique is based on making uniform quantization to the block mean value of one or more of the color bands [9]. The introduced hiding method was designed to apply embedding in one of the following image domains:

1. In RGB color bands (one, or all bands),
2. The Y-band only (in YUV band); taking into consideration the values of Y component is same in the color spaces (YUV, YIQ, YCbCr),
3. The approximation (Low-Low) subband of Haar wavelet.

D1. Blocks Average Modulation Applied on RGB Domain (BAMRGB)

In this work, BAMRGB scheme, similar to that mentioned in Ahmed & George article [9], was executed. The flagged sprite blocks are considered as the host areas for embedding the secret watermark. Each sprite block will be used as a separate entity for hosting one bit of the watermark. The proposed scheme performs watermark embedding by applying modulation on the average value of each color (i.e.; red, green and blue) separately.

The main steps of the developed BAMRGB are:

1. Read the secret message and save it as a binary sequence (bits: 0's and 1's) in WaterMarkBits() array. Then fetch one bit (S) from this array for embedding in each hosting block.
2. Read the I-frame and load its color data into three colors bands array; Red(), Green() and Blue.
3. For each flagged host sprite block:
   (A) Find the corresponding location in I-frame.
(B) Compute the mean of each color band (i.e.; red, green and blue) for the pixels belong to hosting block.

(C) Checks the mean values, such that:

(a) If the mean value is zero, then check (S) value,
   i. If S is zero then set all pixels fall in the host block equal to zero.
   ii. Otherwise (i.e., S is one) then set all pixels values equal to the quantization step \( Q_{stp} \).
(b) Otherwise, compute the corresponding quantization index value \( m_q = \text{round}(\text{Mean}/Q_{stp}) \) to modulate pixel components values in host block. The modulation depends on S value:

   i. When \( m_q \) is even:
   \[
   m'_q = \begin{cases} 
   m_q & \text{for } S = 0 \\
   m_q + 1 & \text{for } S = 1 
   \end{cases} 
   \]  

   ii. When \( m_q \) is odd:
   \[
   m'_q = \begin{cases} 
   m_q + 1 & \text{for } S = 0 \\
   m_q & \text{for } S = 1 
   \end{cases} 
   \]  

   (1a)  

   (1b)

The above equations are applied on each color subband (Red, Green, Blue) separately, such that three modulated quantized mean indexes \( (m'_q^{\text{Red}}, m'_q^{\text{Green}}, m'_q^{\text{Blue}}) \).

(D) Determine the new mean value after embedding using the following:

\[
\text{Mean}' = m'_q Q_{stp} 
\]  

(2)

Where three Mean' values are calculated one for each color band.

(E) Apply modulation on the color bands of pixels belong to the hosting block:

\[
P_w(x,y) = \text{round} \left( P(x,y) \times \frac{\text{Mean}'}{\text{Mean}} \right) 
\]  

(3)

Where \( P(x,y) \) represents the value of color bands (Red, Green, Blue) at the image location \( (x,y) \), and \( Pw(x,y) \) is the corresponding watermark value.

**D2. Blocks Average Modulation Applied on Y Band (BAMY)**

This method implies the same steps of BAMRGB except that:

**1** The (RGB) data of the reference hosting frame is loaded, and then converted to YUV components, the following conversion equations have been used [12]:

\[
Y(x,y) = ((66 R(x,y) + 129 G(x,y) + 25 B(x,y) + 128) \gg 8) + 16 
\]  

(4)

\[
U(x,y) = ((-38 R(x,y) - 74 G(x,y) + 112 B(x,y) + 128) \gg 8) + 128 
\]  

(5)

\[
V(x,y) = ((112 R(x,y) - 94 G(x,y) - 18 B(x,y) + 128) \gg 8) + 128 
\]  

(6)

**2** The watermark is embedded in Y component because it contains the most part of information. The applied embedding steps are similar to those applied in (BAMRGB).

**3** After the embedding stage, the (YUV) data are converted back to (RGB) using the following equations [12]:

\[
R(x,y) = (298(Y(x,y) - 16) + 409(V(x,y) - 128) + 128) \gg 8 
\]  

(7)

\[
G(x,y) = (298(Y(x,y) - 16) - 100(U(x,y) - 128) - 208(Y(x,y) - 128)) \gg 8 
\]  

(8)

\[
B(x,y) = (298(V(x,y) - 16) + 516(U(x,y) - 128) + 128) \gg 8 
\]  

(9)

Besides being the most informatics band, the other reason behind using Y-component is it usually imposed to lower distortion than the U and V components when it is passed through lossy compression (e.g., JPEG, JPEG2000). Figure -2 illustrates the BAMY watermark embedding scheme.
This process depends on transforming the hosting block in I-frame from spatial to wavelet domain. The embedding hides a secret message (watermark) in the approximation sub-band (i.e., LL). The reason behind embedding the watermark into LL band is to get fast, easy and robust process for embedding in the video data. The embedding process on LL coefficients was applied in two different ways:

1st Method (Making embedding in RGB domain): The embedding is applied on one of the (RGB) bands only; because it was found that embedding in the three bands at a time causes noticeable (high) image distortion. The embedding steps are similar to those in BAMRGB. Figure-3 illustrates watermark embedding in RGB domain with wavelet transform.

2nd Method (The embedding is applied on Y domain): Taking into consideration Y-band holds the highest part of the image information. This method uses the same mechanism of BAMY. Figure-4 illustrates watermark embedding in Y domain with wavelet transform.
The modulation is obtained by applying uniform quantization (as in previous embedding methods). In this paper, the applied wavelet transform is Haar transform with wavelet decomposition level is set one. The forward and inverse wavelet (in RGB or in YUV) transforms are obtained by following equations [13]:

$$ s = \begin{bmatrix} I(2x, 2y) & I(2x + 1, 2y) \\ I(2x, 2y + 1) & I(2x + 1, 2y + 1) \end{bmatrix} $$

$$ T = \frac{1}{2} \begin{bmatrix} LL & HL \\ LH & HH \end{bmatrix} $$

Where, $I()$ a two dimensions image, each sub-image $s(2x2)$, Haar wavelet output $T(2x2)$ consist of:

- **Top Left**: $LL=[I(2x,2y)+I(2x+1,2y)+I(2x,2y+1)+I(2x+1,2y+1)]/2$ is the 2-D low pass (Lo-Lo) filter.
- **Top Right**: $HL=[I(2x,2y)-I(2x+1,2y)+I(2x,2y+1)-I(2x+1,2y+1)]/2$ is the average of horizontal gradient or horizontal high pass and vertical low pass (Hi-Lo) filter.
- **Lower Left**: $LH=[I(2x,2y)+I(2x+1,2y)-I(2x,2y+1)-I(2x+1,2y+1)]/2$ is the average vertical gradient or horizontal low pass and vertical high pass (Lo-Hi) filter.
- **Lower Right**: $HH=[I(2x,2y)-I(2x+1,2y)-I(2x,2y+1)+I(2x+1,2y+1)]/2$ is the diagonal curvature or 2-D high pass (Hi-Hi) filter.

Note a division by 4 was applied in the forward transform stage to reduce the overall computation complexity (i.e., no division is done in the inverse transform).

2. **Extraction Stage**

The extraction unit is responsible for extracting the watermark information from video to restore the original video. The extraction is the inverse process of watermark embedding. The blind watermark extraction is based on the same procedure given in Ahmed & George article [9]; it has the following two essential steps:

A. **Allocation of Sprite Host Blocks**

This step aims to define the watermarked frame; this frame is the I-frame. Usually in MPEG-4, it is associated with a binary map defining the locations of sprite blocks.

B. **Watermark Data Extraction**

The extraction operation is similar to that mentioned in embedding stage but it is arranged in reverse manner. The watermark data values are extracted directly from the mean value of the hosting block, using $\{m_q = \text{round}(\text{mean}/Q_{map})\}$, as presented in Ahmed & George article [9]. The quantization index value ($m_q$) of the mean are checked whether it is odd or even to recover watermark data, such that:

$$ S = \begin{cases} 0 & \text{if } m_q \text{ is even} \\ 1 & \text{if } m_q \text{ is odd} \end{cases} $$
For each of the introduced watermark embedding methods (i.e.; BAMRGB, BAMY and HWAM), the watermark data must be extracted. In case of embedding in Haar wavelet coefficients, the watermark is extracted from the approximation sub band.

Test Results Evaluation

The performance of the proposed watermark system was tested to discuss the performance of the proposed method for hiding a secret watermark message within a test video, and to investigate the effect of lossy compression on the extracted message. The used video test samples are Family and Conference (with frame size specifications=320x240 pixels, and the pixel color depth=24 bit/pixel). The system was established using C# programming language.

A. Test Results with JPEG Compression Attack

The adopted test strategy was based on determining the effects of the lossy compression schemes on the watermarked I-frame. In this situation the contents of this watermarked I-frame will change and, consequently, this may cause degradation in the integrity of extracted hidden message. In this set of tests the robustness of watermarked I-frame was evaluated against JPEG compression before its watermark is extracted. It should also be considered that the so called created redundancy should not increase much the file size of the compressed watermarked data which is the primary goal of compression operation.

To study the embedding perceptual effect the Mean Square Error (MSE) is used [14]:

\[ MSE = \frac{1}{WH} \sum_{y=1}^{H} \sum_{x=1}^{W} (f_{org}(x,y) - f_{w}(x,y))^2 \]  \hspace{1cm} (12)

Where, W & H are the width and height (in pixels) of each image (video frame), \( f_{org}() \) is the original image and \( f_{w}() \) is the corresponding watermark image. Also the rate of correct retrieved bits (RCRB) was used to determine the accuracy of the extraction process:

\[ RCRB = \frac{N_{r}}{N} \times 100\% \] \hspace{1cm} (13)

Where, \( N_{r} \) is the number of correct retrieved bits (CRB), and \( N \) is the total number of hidden bits. As long as RCRB goes to %100, better extraction results were obtained. The size of used watermark was fixed at size (376 bit) [9].

Figure-5 shows the effect of modulation quantization step \( Q_{sp} \) on compression ratio and the parameters MSE and RCRB, the modulation block size is taken 4x4 and threshold (Thr) value is set (12), the used hiding method is BAMY method. Compression ratio (CR) is determined using [14]:

\[ CR = \frac{\text{Original watermark file size}}{\text{compressed watermark file size}} \] \hspace{1cm} (14)

Figure-6 shows the effect of \( Q_{sp} \) under same circumstances but for modulation block size is set 8x8 & Thr=60. Figures (7, 8) show the effect of \( Q_{sp} \) on CR and the parameters MSE and RCRB when HWAM applied on Y band (in YUV color domain) is applied using block size: (i) 4x4 (Thr=12) and (ii) 8x8 (Thr=60), respectively. It is obvious that the increase of \( Q_{sp} \) causes a decrease in the attained compression gain and considerable degradation in the quality of watermarked frame. The results indicate that the increase of CR causes an increase in the fidelity level. When applying low compression (i.e., high QF) with block size 4x4 the hiding method works well; that is the rate of correct extracted bits (RCRB) reaches to [97%-100%] when \( Q_{sp} \in [2-20] \). On the other hand, when applying high compression, the hiding method leads to RCRB values that lie within [98%-100%] when \( Q_{sp} \in [5-20] \). When applying high or low compression on the I-frames that are watermarked using modulation on sprite blocks with size 8x8, the RCRB decreases because the applied lossy method (i.e., JPEG) partitions, also, the I-frame into blocks of size 8x8 pixels; and this makes higher distortion in the modulated means values.'

Figures (9,10) show the effect of \( Q_{sp} \) on MSE and RCRB when HWAM method is applied on one of three bands (RGB), here in this set of test, high lossy compression (i.e., QF=10) is applied and the block size is taken (i) 4x4 (Thr =12) and (ii) 8x8 (Thr =60), respectively. The hiding method HWAM in Green band leads to robust watermark. At high compression the proper values of \( Q_{sp} \) should lay within the range [7-20]. The Red and Blue bands are less robust at high compression lossy attack; the suitable \( Q_{sp} \) should be high and, in general, it depends on the used block size. So, hiding in Y band (in
BAMY or in HWAM with Y band) can lead to robust watermark even at high compression circumstances.

The suitable watermark setup must satisfy a trade-off between low distortion, capacity and robustness. For completeness of tests, other set of tests was applied to investigate the effectiveness of watermark capacity (watermark size). In this test set the results indicated that HWAM (in YUV domain) and BAMY (in Y band) show better robustness than other embedding cases even under high compression. Figure-11 illustrates the effect of changing the watermark size (i.e., decreasing to 200 bits and increasing to 528 bits) at high compression circumstance (at QF=10) in Family video. The results indicate that in case of decreasing the watermark size then it can

![Graph showing the effect of watermark size on robustness](image1)

a. The video sample is Family (When \( Q_{Stp} \in \{8,12,16,20\} \) the RCRB= 100%)

![Graph showing the effect of watermark size on robustness](image2)

b. The video sample is Conference (When \( Q_{Stp} \in \{8,12,16,20\} \) the RCRB= 100%)

**Figure 5-** The effect of quantization step on CR and the parameters MSE and RCRB using BAMY method (Block =4x4, Thr=12) (JPEG compression attack)
a. The video sample is Family (When $Q_{stp} \in \{8, 16, 20\}$ the RCRB= 100%)

b. The video sample is Conference

**Figure 6**- The effect of quantization step on CR and the parameters MSE and RCRB using BAMY method (Block =8×8, Thr=60) (JPEG compression attack)

a. The video sample is Family (When $Q_{stp} \in \{8, 12, 16, 20\}$ the RCRB= 100%)

b. The video sample is Conference (When $Q_{stp} \in \{8, 12, 16, 20\}$ the RCRB= 100%)

**Figure 7**- The effect of quantization step on CR and the parameters MSE and RCRB using HWAM method in Y band (Block =4×4, Thr=12)(JPEG compression attack)
a. The video sample is Family (When $Q_{Stp} \in \{16, 20\}$ the RCRB = 100%)

b. The video sample is Conference (when $Q_{Stp} = 16$ the RCRB = 94.946%)

Figure 8- The effect of quantization step on CR and the parameters MSE and RCRB using HWAM method in Y band (Block = 8x8, Thr=60) (JPEG compression attack)

a. The video sample is Family

b. The video sample is Conference

Figure 9- The effect of quantization step on MSE and RCRB using HWAM method in one of three band (RGB) (Block = 4x4, Thr=12) (QF=10)
a. The video sample is Family

b. The video sample is Conference

Figure 10 - The effect of quantization step on MSE and RCRB using HWAM method in one of three band (RGB) (Block = 8x8, Thr=60) (QF=10)

Figure 11 - The effect of watermark capacity on quantization step and RCRB

exactly extracted (reach to 100%) even at low Qstp, while in case of increasing watermark size it can extracted correctly by increasing Qstp.

B. Test Results with JPEG2000 Compression Attack

JPEG2000 is a still image lossy compression scheme. Some watermark robustness tests were conducted using JPEG2000 compression attack. The size of used watermark was fixed at size (376 bit). In this set of tests the adopted hiding methods BAMY (in Y band) and HWAM (in YUV domain); because they show better robustness than other embedding cases even under high JPEG compression ratio.

Figures- (12, 13) show the effect of Qstp on CR and the parameters MSE and RCRB when the used hiding method is BAMY method using block size (i) 4x4 (Thr =12) and (ii) 8x8 (Thr =60), respectively. Figures (14,15) show the effect of Qstp on CR and the parameters MSE and RCRB when HWAM applied on Y band (in YUV color domain) it is applied using block size (i) 4x4 (Thr =12) and
Ahmed and George  

(ii) 8×8 (Thr =60), respectively. It is obvious that the increase of $Q_{Stp}$ and CR causes the fidelity of watermarked frame is considerably decreased. When applying low compression (i.e.; CR= 6:1) the hiding method works well; that is the rate of correct extracted bits (RCRB) reaches to [97%-100%] when $Q_{Stp} \in [2-20]$ (in Family and Conference video) using block size 4×4. Furthermore, in high compression (i.e.; CR= 20:1), the hiding method leads to RCRB values that lie within [81%-100%] when $Q_{Stp} \in [2-20]$ in Family video and $Q_{Stp} \in [4-20]$ in Conference video. Similar to JPEG compression case, when applying high or low compression on I-frames watermarked using mean modulation of blocks with size 8×8, the RCRB decreases especially in Conference video.

![Graphs](image.png)

a. The video sample is Family (When $Q_{Stp} \in \{8,12,16,20\}$ the RCRB= 100%)

b. The video sample is Conference (When $Q_{Stp} \in \{16,20\}$ the RCRB= 100%)

**Figure 12**- The effect of quantization step on CR and the parameters MSE and RCRB using BAMY method (Block =4×4, Thr=12) (JPEG2000 compression attack).
a. The video sample is Family (When $Q_{stp} \in \{8,16,20\}$ the RCRB= 100%)

b. The video sample is Conference

**Figure 13** - The effect of quantization step on CR and the parameters MSE and RCRB using BAMY method (Block =8×8, Thr=60) (JPEG2000 compression attack)

c. The video sample is Conference (When $Q_{stp} \in \{12,16,20\}$ the RCRB= 100%)

**Figure 14** - The effect of quantization step on CR and the parameters MSE and RCRB using HWAM method in Y band (Block =4×4, Thr=12) (JPEG2000 compression attack)
Conclusions
The test results indicated that:
1. The proposed watermark system method can preserve the frames quality and it provides excellent watermark hiding action.
2. When JPEG and JPEG2000 lossy attack are imposed on the watermarked frames, the tests results indicated the watermark embedded in Y in BAMY or in HWAM sub-band is robust against:
   a. JPEG lossy compression attack up to (27:1) compression ratio
   b. JPEG2000 lossy compression attack up to (20:1) compression ratio.

For future:
1. Developing the modulation process by applying mean modulation for left and right halves (or upper/ bottom halves) of each host block.
2. Using other domains, to make watermark embedding by applying modulation in low frequency components of sprite regions.

References


