

Original Research Articles

Robust Watermarking for Video Using Modulation Technique on RGB Domain

ABSTRACT

In this paper, a robust invisible watermarking system for digital video encoded by MPEG-4 is presented. The proposed scheme provides watermark hidden by embedding a secret message (watermark) in the sprite area allocated in reference frame (I-frame). The proposed system consists of two main units: (i) Embedding unit and (ii) Extraction unit. In the embedding unit, the system allocates the sprite blocks using motion compensation information. The allocated sprite area in each I-frame is used as hosting area for embedding watermark data. In the extraction unit, the system extracts the watermark data in order to check authentication and ownership of the video. The watermark data embedding method is Blocks average modulation applied on RGB domain. The applied modulation technique is based on making uniform quantization to the block mean value of the color bands. The tests indicated that the proposed block mean modulation method of the sprite blocks showed robust watermark embedding; it was capable to withstand against lossy JPEG.

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

1. INTRODUCTION

The main problem encounters content providers and owners are the protection of their content material. They are aware about copyright protection and other forms of exploitation of their digital owned content. The ease of duplicating and distributing the copied digital information had stimulated the need for effective copyright protection tools [1]. Even though encryption can be a good key for safe distribution, the encrypted data can decrypt and copied during the data presentation phase [2]. Various types of techniques have been introduced, including watermarking, to handle these increasing concerns. Digital watermarking approach had been emerged as an effective key for protecting the digital content from unauthorized copying [3].

Digital watermarking is a methodology to protect the ownership identity of multimedia data and discourage the unauthorized copying; it embeds a perceptually transparent pattern in digital data using certain specially designed algorithm. Watermarking is a category of information hiding. In the published literature different watermarking schemes have been suggested for multimedia content (such as images, video and audio data). One data is copied, and then the carried information is, also, copied [4]. The embedded watermark information can be a serial number or random number sequence, copyright messages, ownership identifiers, transaction dates, gray level images, information about the work creators, text or other digital data formats. There is a large number of text, image, audio and video watermarking algorithms are introduced and developed, and they can be found in the literature. Any digital watermarking system includes two basic modules: (i) watermark embedding and (ii) watermark extraction (or detection). Any watermark embedding algorithm uses an embedding key to drive the embedding way of watermark information into the

original carrier. The extraction algorithm of embedded watermark uses the extraction key to extract watermark. Any attacker has to find the proper extraction and modification tasks which are very difficult to be found or developed [5]. Video watermarking denotes to embedding watermarks in a video sequence in order to prevent the video from unauthenticated methods that work on compressed or uncompressed data to hide the ownership of digital video. Now-a-days almost all digital videos are watermarked by their creators due to fast sharing and viewing of videos over the internet [6].

Several algorithms have been developed to handle the problem of video watermark. Jammetige et al proposed a technique for robust and invisible watermarking of sprite in MPEG-4. The technique implies three steps for generating sprites: (i) Initialization, (ii) Updating and (iii) Blending. The sprite is initialized for the very first Video Object Plane (VOP) of the video object sequence by just placing the VOP at a pre-specified location within the sprite. Then, the sprite is updated for each of the subsequent VOPs of the video object sequence by estimating the motion of the VOP with respect to the sprite. Then, the VOP is warped by the estimated motion parameters. The warped VOP and the sprite are then blended together. The blending factor may be different for different pixels on the sprite and it is a function of the number of times this pixel. The principal advantage of this watermarking technique is that the watermark bits are modulated onto the sprite depending on the merit of each pixel [7].

Barni et al embedded a watermark in each video object by imposing a particular relationship between some predefined pairs of quantized Discrete Cosine Transform (DCT) coefficients. The embedding is applied on the luminance blocks of selected macroblocks (MBs). Watermarks are equally embedded into intra and inter MBs. They proposed that while a video object is transferred from a sequence to another, it is still possible to correctly access the data embedded within the object itself [8].

Mirza et al proposed a new digital video watermarking scheme based on Principal Component Analysis. Video file is a continuous collection of static images, and each image is composed of three color channels, the proposed algorithms allow embedding a watermark in the three color channels RGB of an input video file. The results showed a high robustness against most common video attacks, especially frame dropping, cropping and rescaling for a good perceptual quality [9].

Essaouabi et al presented a novel object based watermarking solution for MPEG4 video authentication using the shape adaptive-discrete wavelet transform (SA-DWT). In order to make the watermark robust and transparent, the watermark embedded in the average of wavelet blocks using the visual model based on the human visual system [10].

Kumar et al presented a method of concealing an image, individually, on multiple frames of a video, using DWT Algorithm. The aim was obtaining a color output image, as a watermark, on each frame of the video, and to do so, color component decomposition had been performed. Using DWT technique, successfully applied image watermarking on video frames, and had successfully obtained the improved PSNR and MSE values for the same. [11].

The objective of this paper is to embed a watermark (secret message) in the found sprite object (survive object) in each Group of Video (GOV); to produce robust watermarked video encoded with MPEG-4. The proposed system is designed to provide the authentication and protection to video by inserting invisible watermark. The watermark always remains in the sprite and the video can be used as though it was not watermarked. The developed embedding process is based on low level modulation for the averages of blocks (applied in RGB domain).

2. PROPOSED METHODOLOGY

The implemented video watermark system consists of two units:

1. Embedding unit,
2. Extraction unit.

The embedding unit has of four modules; they are: (i) load video data, (ii) Motion compensation, (iii) Sprite region allocation and (iv) watermark data embedding. The extraction unit consists of two modules; they are: The allocation of sprite blocks (hosting blocks) and the watermark data extraction. The layout of the proposed system is illustrated in figure 1.

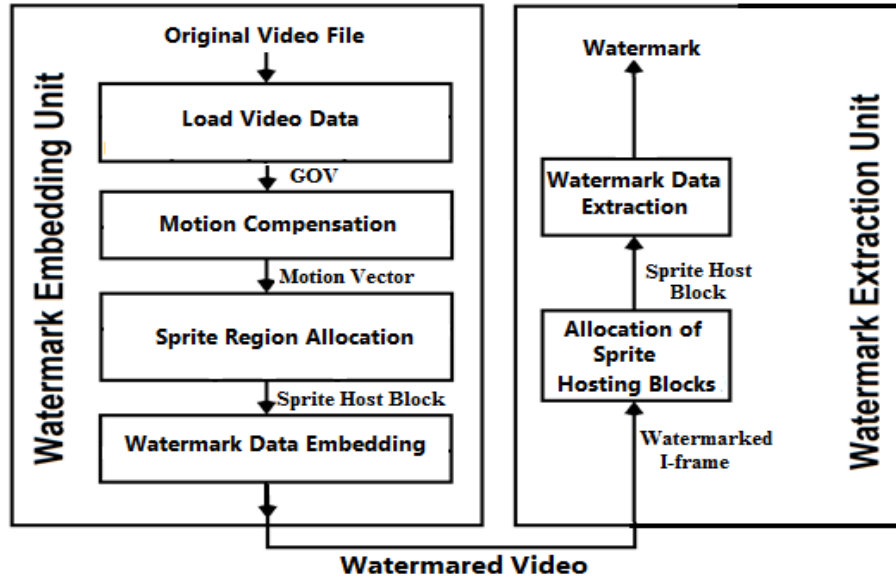


Fig. 1. The Layout of Proposed System

2.1 Embedding Unit

It aims to embed (hide) information in the sprite regions in such a way that the hidden information is imperceptible to human eye. The hidden data is treated as watermark. The embedding technique must keep the perceptual information of video without changing and the watermark information should be founded by extraction algorithm. It has four primary modules; these modules contain essential stages whose tasks are focused toward producing the suggested video watermark. Firstly, a set of video processing operations are applied in order to prepare the video data for application of motion compensation. In order to avoid coding time delay, it is important to simplify the task of motion compensation. Secondly, motion compensation is applied to assess the motion vectors of the blocks that belong to predictive frames. Thirdly, the determined motion vectors are used for registering the motion history of all blocks in order to find out the survived region (i.e., sprite regions) in I-frame. The applied motion compensation method was called controlled prediction method. Three variants for the controlled prediction method have been introduced; they are the 8-Neighbor (8-N), 4-Neighbor (4-N) and Hybrid Search (HS)). Fourthly, 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 the color bands (RGB).

2.1.1 Load Video Data Module

The video frames belong to GOV are represented using BMP raster format. Each GOV consists of N frames (in this paper it was taken as 10). Then, the values of the gray component of the pixels belong to each frame is calculated using the following equation [12]:

$$Y(x,y) = ((66 R(x,y) + 129 G(x,y) + 25 B(x,y) + 128) \gg 8) + 16 \quad (1)$$

2.1.2 Motion Compensation Module

In this work, same motion compensation scheme to that described in [13] was applied. Two simple, efficient and fast block matching search algorithms are given. The first algorithm is called 8-Neighbor Search (8-N) and the second called 4-Neighbor Search (4-N). In 8-Neighbor method, the eight surrounding neighbor blocks (but in the previous frame) are used to assess the initial search position of the target block (belong to current frame) to find the best matched block (that lay in previous frame); the suggested 4-Neighbor search method differs from the proposed 8-neighbor search in:

1. Beside the initial position, determine the MAE of the 4-nearest neighbor blocks adjacent to the initial block.
2. Beside the 4-neighbors blocks, one of the 4-diagonal neighbors (i.e., the corner that close to the two pre-tested points have lowest MAE) will be included in the tests.

Also a hybridization that mixes the proposed two predictive mechanisms (i.e., 8-N and 4-N searches) with the exhaustive search (ES) mechanism is adopted.

2.1.3 Sprite Region Allocation Module

A simple and fast method to allocate sprite objects (or areas) in the reference frame of each Group of Video (GOV); the system allocates the sprite blocks using motion compensation information [14]. 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). The strategy of sprite region allocation is based on categorizing the video frames' contents into foreground and background areas. The main objective is to generate the background sprite with better quality. Although, the sprite region is located and isolated from the rest of the frames by making detection process, but it is very difficult to completely eliminate the effects of foreground objects; which significantly deteriorates the quality of sprite images. So, a post processing process is necessary to eliminate the produced gaps/pores and, consequently, enhances the sprite allocation process result. The sprite blocks are constructed according to simple uniform partitioning scheme.

The proposed sprite detection system consists of three main stages: (i) Sprite Blocks Nomination (SBN), (ii) Gaps Filling and Islands Remove (GFIR) and (iii) Partitioning the Sprite Area into Blocks (PSAB). These stages are necessary in order to decide which of these blocks represent the sprite [14].

2.1.4 Watermark Data Embedding

The main idea of the applied watermarking process is to create a safe embedding area in the I-frame using block mean modulation technique. The modulation is applied after making uniform quantization to the mean value of the marked host blocks. The P and B frames are not affected when embedding the watermark. Although, the main characteristic of this introduced method is its low hiding capacity, but it can offer enough hiding space for watermark. The reasons for applying the method of block mean modulation is due to many reasons: (1) the method is easily implemented, (2) needs low computational complexity, (3)

the embedded watermark is robust against compression attacks, (4) the embedded information is perceptually invisible, and (5) to ensure high visual quality.

A survey was done to check whether the embedding mechanism proposed in this paper was pre-introduced in the literature, and no similar mechanism was found. Some articles in the literature discussed the idea of transform coefficients modulation for image (see [15]) which can offer similar vision for hiding method.

The introduced hiding method was designed to apply embedding on RGB color bands. The method is based on making **blocks average modulation on the RGB domain (BAMRGB)**. 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. Figure 2 illustrates the watermark embedding (BAMRGB) process.

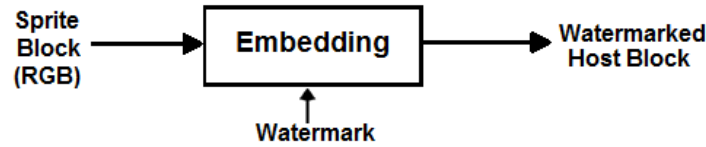


Fig.2. Watermark embedding applied directly on RGB domain

195

196

197

To clarify the proposed method 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 belongs 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:

$$m'_q = \begin{cases} m_q & \text{for } S = 0 \\ m_q + 1 & \text{for } S = 1 \end{cases} \quad (2a)$$

218

219

220

ii. When m_q is odd:

$$m'_q = \begin{cases} m_q + 1 & \text{for } S = 0 \\ m_q & \text{for } S = 1 \end{cases} \quad (2b)$$

221

222

223 The above equations are applied on each color subband (Red, Green, Blue)
 224 separately, such that three modulated quantized mean indexes (m_q^{Red} ,
 225 m_q^{Green} , m_q^{Blue})
 226

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

$$228 \quad Mean' = m_q' Q_{stp} \quad (3)$$

229 Where three Mean' values are calculated one for each color band.
 230

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

$$232 \quad P_w(x,y) = round \left(P(x,y) \times \frac{Mean'}{Mean} \right) \quad (4)$$

233 Where P(x,y) represents the value of color bands (Red, Green, Blue) at the image
 234 location (x,y), and Pw(x,y) is the corresponding watermark value.
 235

236

237 2.2 Extraction Unit

238

239 The extraction of hidden watermark from video is to prove its authentication and/or
 240 ownership. The blind watermark extraction implies that the embedded watermark is retrieved
 241 without requiring any information from the original video. In the proposed system, the most
 242 difficult task associated with blind watermark extraction is how to identify the sprite host
 243 block. The applied watermark extraction for BAMRGB hiding method implies the essential
 244 steps whose tasks are:

245

246 2.2.1 Allocation of Sprite Host Blocks

247

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

250

251 2.2.2 Watermark Data Extraction

252

253 The watermark data values are extracted directly from the mean value of the hosting block
 254 (using $\{m_q = round (mean/Q_{stp})\}$); here, the quantization index value (m_q) of the mean are
 255 checked whether it is odd or even to recover watermark data, such that:

$$256 \quad S = \begin{cases} 0 & \text{if } m_q \text{ is even} \\ 1 & \text{if } m_q \text{ is odd} \end{cases} \quad (5)$$

257

258 For the introduced watermark embedding method (i.e.; BAMRGB), the watermark data must
 259 be extracted.
 260

261

262 3. EXPERIMENTS RESULTS

263

264 In this paper, a set of tests were conducted to examine the performance of the proposed
 265 method for hiding a binary payload within a test video, and to investigate the effect of lossy
 266 compression on the extracted message. The used video test samples are Family and
 267 Conference (with frame size specifications= 320 x240 pixels and pixel color depth=24 bit).
 268 These videos were taken from YouTube. The system was established using C#
 269 programming language. Figure 3 presents the I-frame with and without watermark
 embedding.

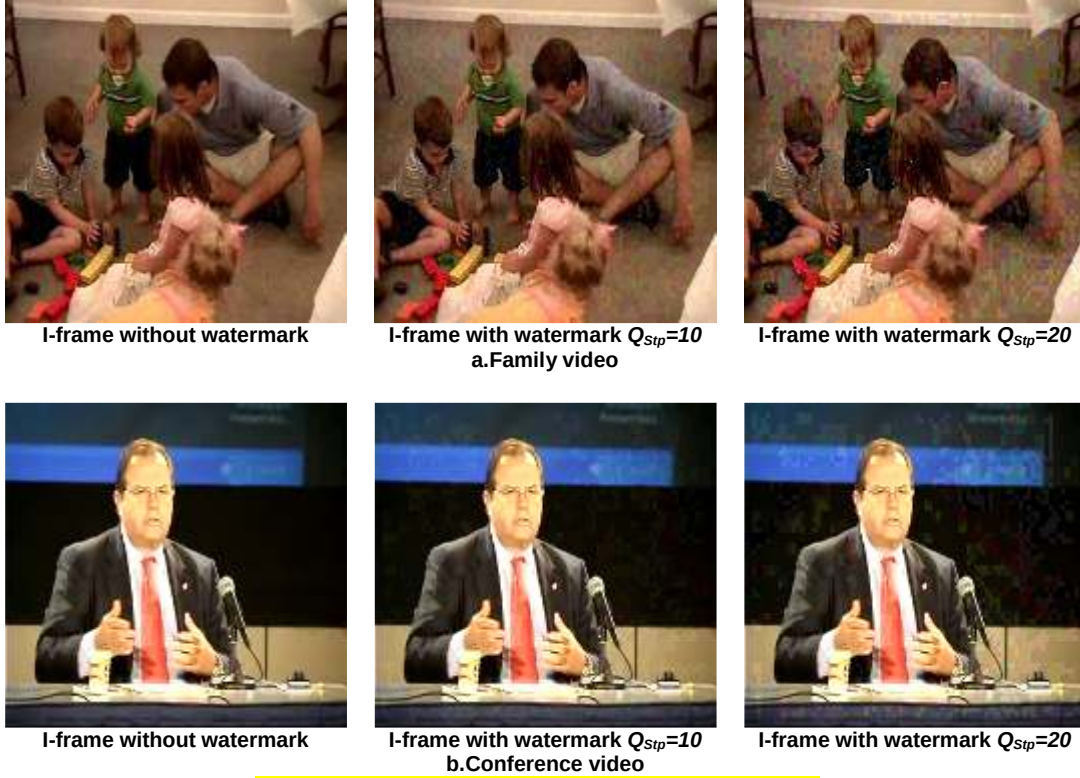


Fig.3. I-frame with and without watermarking

3.1. Results of Conducted Tests without Compression Attack

The proposed video watermark system embeds the content of a hidden watermark message in I-frames of the video; such that the visual quality of this frame does not change perceptually. To study the embedding perceptual effect the Mean Square Error (MSE) is used [16]:

$$MSE = \frac{1}{WH} \sum_{y=1}^H \sum_{x=1}^W (f_{org}(x,y) - f_w(x,y))^2 \quad (6)$$

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:

$$RCRB = \frac{N_r}{N} \times 100\% \quad (7)$$

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 kept at fixed size (376 bit), taken into consideration the size of watermark taken in previous published works was taken around (30-100 bit). The secret message is the string "Robust Watermarking for Video Using Modulation"... Figures 4 and 5 show the effect of modulation quantization step Q_{Stp} on BAMRGB method when block size is set: (i) 4×4 (Thr=12) and (ii) 8×8 (Thr=60). The MSE results indicate that the increase of Q_{Stp} causes considerable quality degradation in watermarked frame. Mostly, the watermark message is

completely extracted using fairly low Q_{Stp} and the visual quality of the watermarked frame is not perceptibly changed.

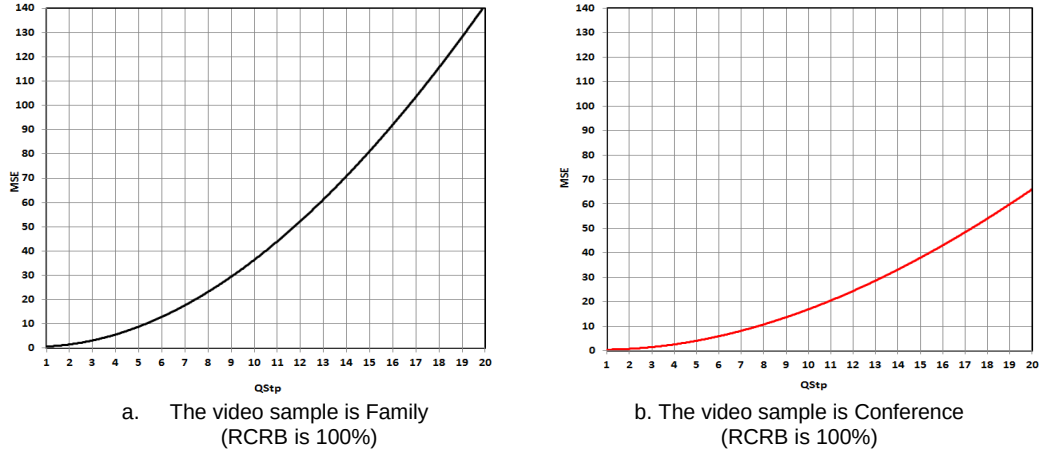


Fig.4. The effect of quantization step on MSE and RCRB using BAMRGB method without attack (Block 4×4, Thr=12)

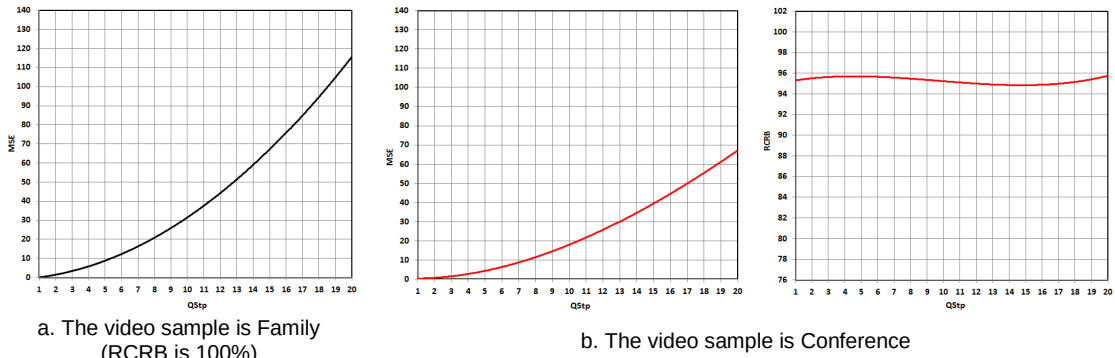


Fig.5. The effect of quantization step on MSE and RCRB using BAMRGB method without attack (Block 8×8, Thr=60)

3.2. Results of Conducted Tests with Compression Attack

The watermarked I-frame may be compressed using one of the lossy compression schemes. In such case the contents of the watermarked image is changed and, consequently, it may cause degradation in the integrity of extracted secret message. To assess the level of lossy compression effectiveness, another set of tests were conducted. In this set the watermarked I-frame is passed through JPEG compression before its watermark is extracted. During the conducted tests various degrees of compression rates were applied. The size of used watermark was fixed at size (376 bit). Figure 6 shows the effect of modulation quantization step Q_{Stp} on compression ratio and the parameters MSE and RCRB under high lossy compression (i.e., QF=10), the modulation block size is taken 4x4 and threshold (Thr) value is set (12). Figure 7 shows the effect of Q_{Stp} under same circumstances but for modulation block size is 8×8 and Thr=60. Compression ratio is determined using [16]:

$$CR = \frac{\text{Original watermark file size}}{\text{compressed watermark file size}} \quad (8)$$

320 The results refer that the increase of Q_{Stp} causes an increase in the quality degradation of
 321 watermarked frame in MPEG-4. The acceptable result of RCRB (which is nearly more than
 322 80%) is occurred when $Q_{Stp} \in [6-20]$ with CR 28:1 to 23:1 in Family video and $Q_{Stp} [8-20]$ with
 323 CR 27:1 to 25:1 in Conference video. The visual quality of the watermarked frame is not
 324 perceptibly changed. For comparison purpose with other research work, the results in [15]
 325 illustrated that it can preserve image quality and provide good hiding capacity of hidden
 326 message, which it reaches up to 9.18% in JPEG compression, while in [7] good performance
 327 of the detector up to a JPEG compression of 35%.
 328

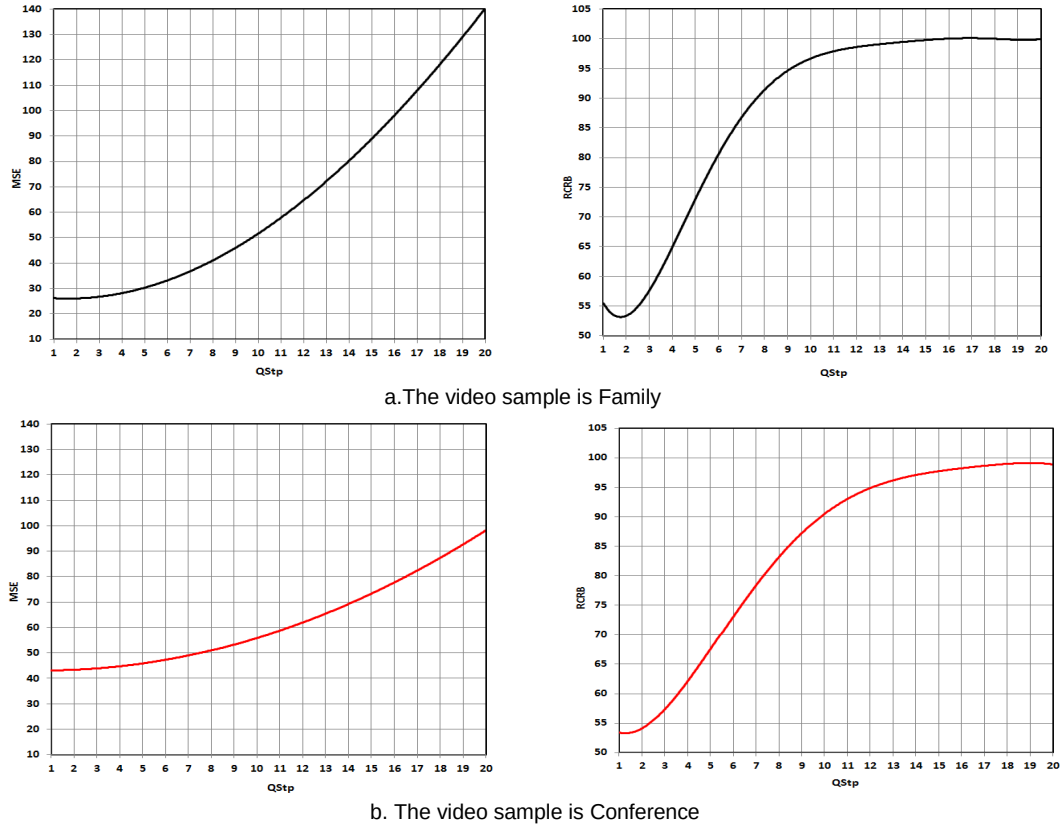
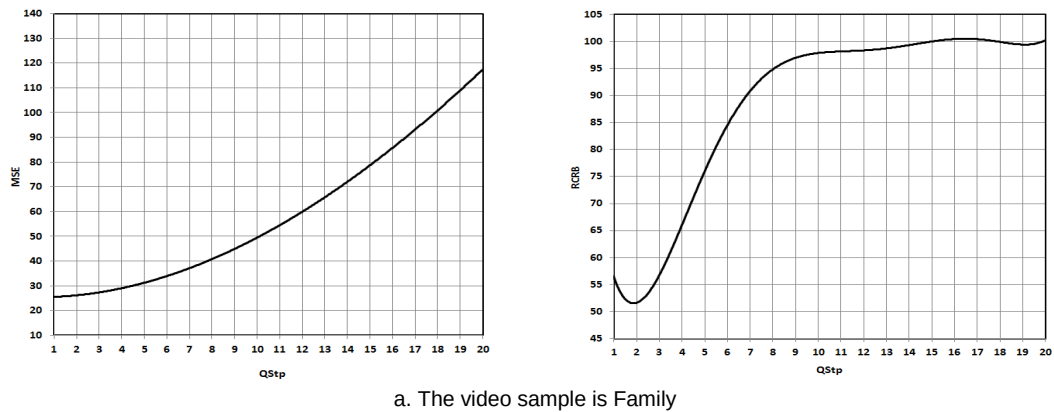
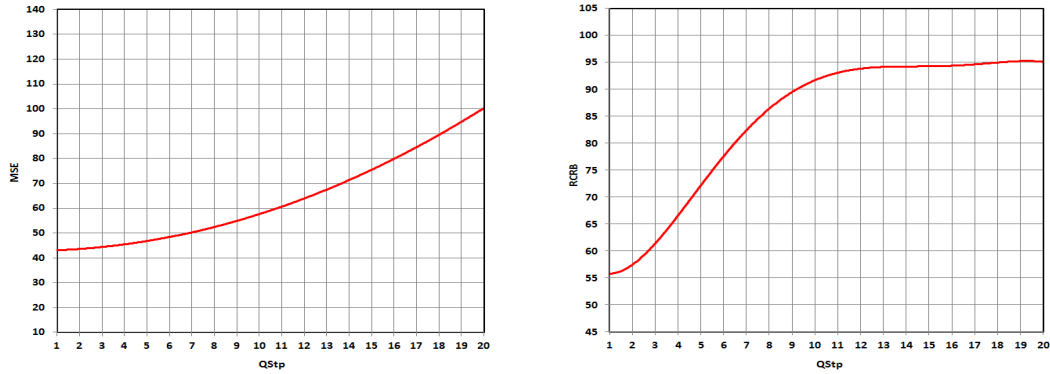


Fig.6. The effect of quantization step on MSE and RCRB using BAMRGB method (Block =4x4, Thr=12) (QF=10)





b. The video sample is Conference

Fig.7. The effect of quantization step on MSE and RCRB using BAMRGB method (Block =8×8 Thr=60) (QF=10)

Generally, there are three parameters in watermarking that have the most important role: capacity, quality, and robustness. Video watermarking capacity is an evaluation of how much information can be hidden in a digital video without perceptible distortion, while maintaining watermark robustness against usual signal processing manipulation and attacks. So, other set of tests is applied to evaluate the performance of watermark capacity (watermark size). Figure 8 illustrates the impact of changing the watermark size (i.e., decreasing to 200 bits and increasing to 528 bits) under high compression. The secret message is "Robust Watermarking video" in decreasing capacity while the secret message is "Robust Watermarking for Video Using Modulation Technique on RGB //" in increasing capacity. The results show that with low hiding capacity the secret can be an exactly extracted (reach to 100%) even at low Q_{Stp} ; while when secret message volume is high it can be extracted correctly in case of increasing Q_{Stp} .

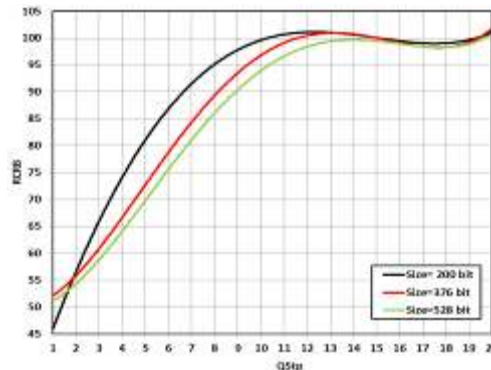


Fig.8. The effect of watermark capacity on quantization step on and RCRB (The video sample is Family)

4. CONCLUSION

From the test results of proposed watermark system, the following remarks are stimulated:

1. No harm distortion in frames quality is occurred, and it provides good watermark hiding action.
2. When no attack is applied, the extraction process is fully successful whatever the block mean quantization value is taken.
3. When JPEG lossy attack is imposed on the watermarked frames, the tests results indicated the embedded watermark is robust against JPEG lossy compression attack.

361

362 For future research work the following issues can be investigated:

- 363 1. Embedding the watermark by modulating Y-band.
364 2. Embedding by applying modulation on the transform domain of host video.
365 3. Investigate the effectiveness of JPEG2000 compression attack.

366

367

368

REFERENCES

- 369 [1] Prasad M. Koliwad Sh. A Comprehensive Survey of Contemporary Researches in
370 Watermarking for Copyright Protection of Digital Images. International Journal of
371 Computer Science and Network Security (IJCSNS). 2009, 9(4): 91-107.
- 372 [2] Palaiyappan C. Sekhar RJ. A Block Based Novel Digital Video Watermarking Scheme
373 Using Dct. Journal Of Electronics And Communication Engineering. 2013, 5(2): 34-44.
- 374 [3] Kumar N. Gupta V. Kumar P. Analysis and Implementation of Different Digital Image
375 Watermarking Techniques for Secure Data Transmission. International Journal of
376 Computer Trends and Technology. 2013, 4(5):1140-1148.
- 377 [4] Khanzode P. Ladhake S. Tank S. Digital Watermarking For Protection of Intellectual
378 Property. International Journal of Computational Engineering & Management. 2011, 12:
379 8-12.
- 380 [5] Singh A. Jain S. Jain A. A Survey: Digital Video Watermarking. International Journal of
381 Scientific & Engineering Research. 2013, 4(7): 1261-1265.
- 382 [6] Cheng M. Xi M. Yuan K. Wu Ch. Lei M. Recoverable Video Watermark in DCT Domain.
383 Journal of Computers. 2013, 8(2): 533-538.
- 384 [7] Jammetige M. Nagaraj R. Panchanathan R. Watermarking of Sprites in MPEG-4. SPIE.
385 2001, 4209:273-283.
- 386 [8] Barni M. Bartolini M. Checcacci N. Watermarking of MPEG-4 Video Objects. IEEE. 2005,
387 7(1): 23-32.
- 388 [9] Mirza HH. Thai HD. Nagata Y. Nakao Z. Digital Video Watermarking Based on Principal
389 Component Analysis. 2007, IEEE.
- 390 [10] Essaouabi A. Ibnelhaj E. Regragui F. A Wavelet - Based Object Watermarking System
391 For MPEG4 Video. International Journal of Computer Science and Security.2010, 3(6):
392 448-461.
- 393 [11] Kumar S. Gupta A. Chandwani A. Yadav G. Swarnkar R. RGB Image Watermarking On
394 Video Frames Using DWT. IEEE. 2014, Pp. 675-680.
- 395 [12] [HTTP://MSDN.MICROSOFT.COM/EN-US/LIBRARY/MS893078.ASPX](http://msdn.microsoft.com/en-us/library/ms893078.aspx). 2004.
- 396 [13] Ahmed ZJ. George LE. Sultan BA. New Predictive Block Matching Searching Algorithms
397 and Hybrid Predictive Search System. International Journal of Engineering and
398 Innovative Technology. 2014, 3(8):230-235.
- 399 [14] Ahmed ZJ. George LE. Sprite Region Allocation Using Motion Compensation Technique.
400 International Journal of Computer Science and Mobile Computing. 2015, 4(2): 188-197.
- 401 [15] Al-Momen SMA. George L E. Image Hiding Using Magnitude Modulation on The DCT
402 Coefficients. Journal of Applied Computer Science & Mathematics. 2010, 4(8):9-14.
- 403 [16] Salomon D. Motta G. Handbook of Data Compression. Fifth Edition, Springer, 2010.