2nd INTERNATIONAL CONFERENCE ON
RESEARCH IN SCIENCE AND TECHNOLOGY
Istanbul-Turkey 14 March 2016
RSTCONF
دومین کنفرانس بین المللی
پژوهش در علوم و تکنولوژی
ترکیه - استانبول ۲۴ اسفند ۱۳۹۴

Data Hiding in video H.264 by motion vectors

Masoud Dashtdar
Affiliation: Sama Technical and Vocational Training College, Islamic Azad University, Bushehr Branch, Bushehr, Iran.
Email: dashtdar.m@gmail.com

Ahmad Keshavarz
Affiliation: Persian Gulf University of Bushehr
Email: Ahmad_modarres81@yahoo.com

Abstract

Currently, data transmission over the internet is safe from all directions and are vulnerable to various attacks. So in order to prevent access to valuable information, we need to have special security measures. A method for secure transmission of data, steganography method, which we attribute to hide his message in this way can we create more secure. data steganography is one of the ways that a message can be in the picture , audio , video, text, etc. hidden. In this project we will use the H.264 video stream watermarking algorithm. Unlike previous watermarking methods, the spatial domain, or become used to hide data, we compress the video to hide the secret data we use, so that the motion vectors for encoding and the reconstruction of both the predicted P frames and B frames in video compression used. Where the motion vector using macroblock prediction error is calculated, and then the method based on motion vector features such as measure and angle can be used. Finally, all candidates for the embedded data, and then using the LSB bits of the secret message is replaced. And at the same time each GOP, the control information for the data embedded in the frame are done. At the end of the control information in each frame, we extract the secret message. The algorithm is tested on different types of films based on the above criteria, the proposed method is well done.

Keywords: Data hiding, motion vectors, prediction error, H.264, steganography

1- Introduction

Extension due to the use of digital data on the Internet and the World Wide Web, and easy access to images, documents, music and movies, using data hiding, with an emphasis on copyright protection, content-based authentication, annotation and covert communications developed. Hide information, the ability to embed data in a digital coverage with the least amount of damage is understood. Hide data consists of two sets of data, the media and the coverage embedded message is called. Digital media and the message can be text, audio, picture or video message depends upon the size and capacity dependent watermarking method is proposed to be covered. Early techniques of video data hiding, hiding the message in each frame independently. Such a wide range of ways in which the basic idea, Message in a wide range of frequencies further distribution data host. For general transform domain data hiding in the spatial domain is preferred due to its robustness, the result for the human visual system (HVS) it would be more appropriate. For this purpose, discrete Fourier transform domain (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT) is normally used.

Recent data hiding techniques in the video on the video compression standard features produced by such schemes based on motion vectors for MPEG algorithms focused. Motion vectors by a video encoder in order to remove the barriers of time between frames is calculated. In this method the original motion vectors to embed the information to be replaced by local optimum motion vectors. Also recently, a number of data hiding algorithm is proposed according to the H.264 standard properties .Where a subset of the coefficients of the DCT 4×4 in order to achieve a robust watermarking algorithm for H.264 has emerged. And blind algorithm for copyright protection in the intra prediction of H.264 video standard is also presented.

This project is the first video to divided macroblock and the message in the least significant part of the macroblock sizes such as 16×16, 8×8, 4×4 with respect to the encoding of motion vectors. Sometimes it may also be the result of errors by gradually building up gradually, setting values that are predefined as rounding to the nearest value must be defined. Due to the fact that no pixel will be created and will lead to loss of resolution.

2- steganography scheme Each features

The design of any watermarking method for the three parameters, namely transparency, strength and capacity of the proposed scheme is considered to be evaluated:

- Transparency: Transparency implies that the system changes the video quality before and after the embedded message is not appreciably different, because the target is non-sense messages in the security of a watermarking system, there is the issue of transparency and no matter which video similarity is both free and contains more message security system is at a higher level.
- Strength: Strength, a steganography system that is meant to be hidden message in front of the inadvertent and unintentional changes to the noise along the route of transmission creates and Or deliberate changes that enable attackers to modify or eliminate messages that have done the necessary strength.
- Capacity: steganography systems can be much more of a message can be hidden in a host system would be more appropriate. Volume of data that can be stored in a host depends on the exact nature of the host and to what extent can it be hidden where it would impact without transparency.

It should also be noted that these three characteristics are very closely connected, which means that the constant increase in the first feature and the second, the third feature to be abated.

(Fixed = Strength *Capacity)
The proposal tries to consider these three features Gbrd.

3- The proposed steganography algorithm

Today, digital video watermarking, a lot of research interest in recent years has attracted applications. Standard H.264 The last and most advanced video coding standards, but to date, very little in this field watermarking schemes are designed. Because it is mainly due to the complexity and compression performance, which is currently a major challenge for any video watermarking technique is considered. According to the above process, the aim of the proposal, we present a data hiding method using a high resolution of digital video as a signal of cover. Where locally adaptive watermarking distortion rate optimization and conversion coefficients of the macroblock is placed. Our unique perceptual mask obtained from the motion vectors are used to control the spatial and temporal distortions. We made plans with bit allocation mechanism that ensures optimum distribution of the macroblock of watermarking has been developed. Our watermark provides constant power for video compression H.264 The difference with low bit rate and video quality without generally affect. Experimental results show that our watermarking scheme using compression, encryption, filtering, scaling, rotation, and collusion attacks better.

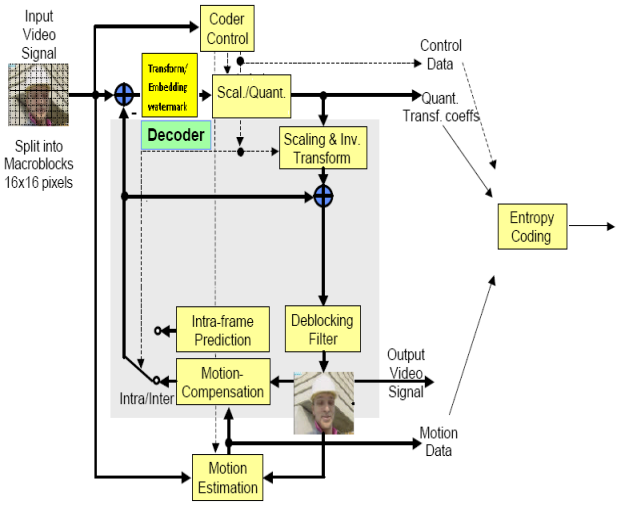

Fig1: The proposed steganography scheme with H.264

3-1- one Step: calculate the motion compensation prediction and motion vector

The main idea of our proposed scheme for embedding watermark using of the inter prediction process, So the first step in the inter prediction process of motion estimation and to obtain motion vectors in current frame based on frame reference.

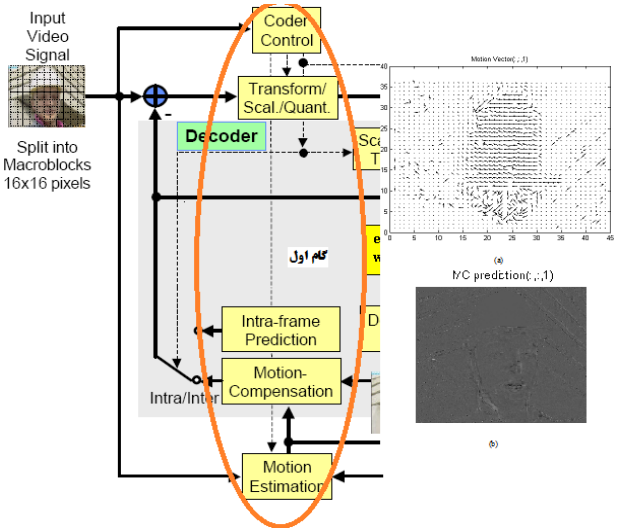

Fig 2: Step One: Get the (a) motion vector, (b) motion compensation prediction

3-2 two Step: Build a perceptual mask based on motion vectors

In the proposed scheme, the candidate locations as well as finding the optimal allocation of bits between the macroblock of watermark by the perceptual mask design (Figure3 b) is carried out. In this method, a perceptual mask is created using motion vectors of features.

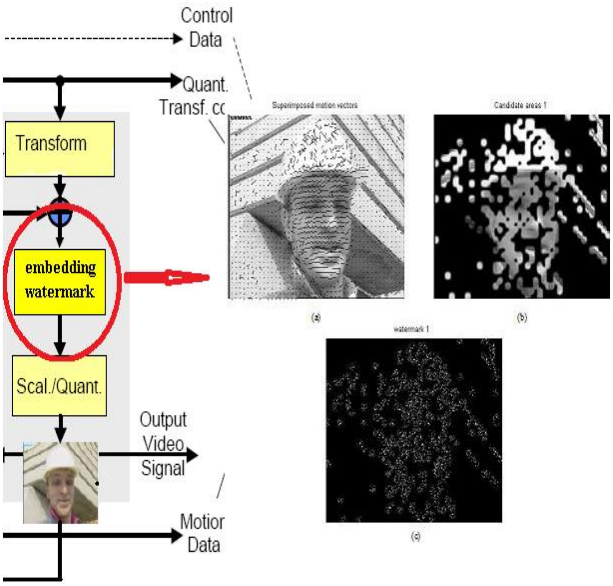

Fig3: Process the data embedded in the frame is predicted

The measure and angle of the motion vectors calculated by comparing the measures seen in areas with large motion vectors drastically reduced the measures of the regions that have changes have little or no is in motion. Then be an appropriate threshold T can be extracted from these regions. Finally, this method can not change the angle where the threshold T can be removed and then the best areas embedding watermark extracted.

3-2-1 Perceptual mask design stages

1. Obtaining motion vectors
   PMV[i] | 0< i< MB
   Here is the MB macroblock and PMV [i] is the motion vectors.

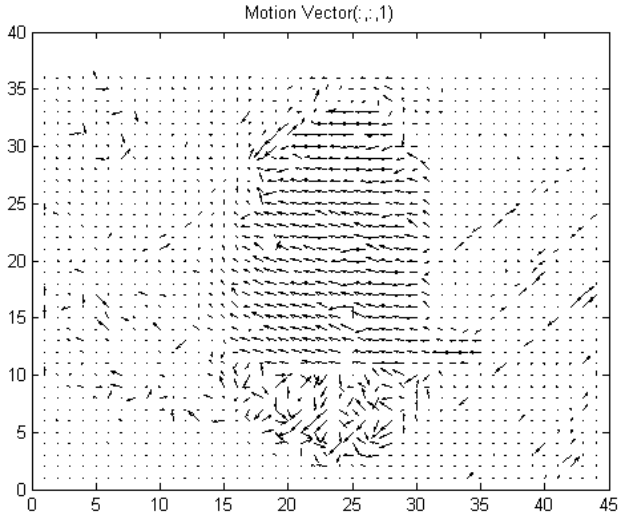

Fig4: motion vectors

2. Calculating the measure and angle of motion vectors
   |PMV[i] | = √(H2[i] + V2[i]) (0< i< MB)
   θ[i] = arctan(v[i] / H[i]) (0< i< MB)
   Where H [i] the horizontal component of the motion vector PMV in macroblock i and V [i] The vertical component of the motion vector PMV in macroblock i and θ [i] is the vector angle.

Fig5: The measure of motion vectors | PMV [i] |

3. Select the appropriate macroblock
   If | PMV[i] | < T → , P[i] = 1
   If | PMV[i] | ≥ T → , P[i] = 0
   If Θ[i] = 0 → , P[i] = 0

E[i] = P[i] . F[i]

Where T is the threshold value, E[i] selected macroblock and F[i] frame. Now, according to the relations given above can easily create a perceptual mask. (Figure 6)

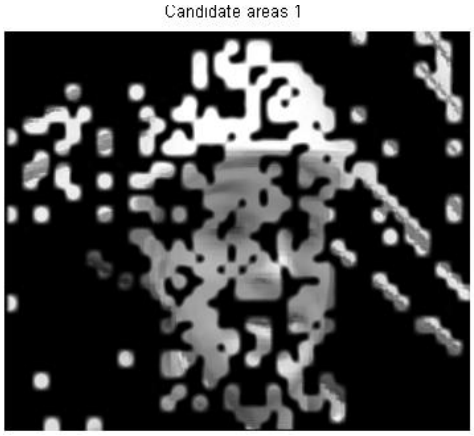

Fig6: candidate regions

3-3 Third step: embedding data

An important factor in any video watermarking schemes, watermark bit allocation between the various macroblock. During video encoding, encryption resource allocation decisions is a bit different areas of the image. Video encoder, bit rate watermark is distributed according to the content. For example, for highly textured areas, and more bits are allocated to areas of lower bit flat. Video watermarked is desirable that it is best to allocate watermark bits between the macroblocks of different done. In video coding, the most important factor for controlling the bit rate of the signal remains that with an appropriate choice of quantization step size to transform coefficients, the controls do. We scheme to obtain the best distribution watermark bit simply perceptual mask and quantization step size change occurs. Watermark to embed this stage (Figure 7) are used. The major advantage is that the bits of the watermark bit allocation mechanisms, the overall rate does not affect the video.

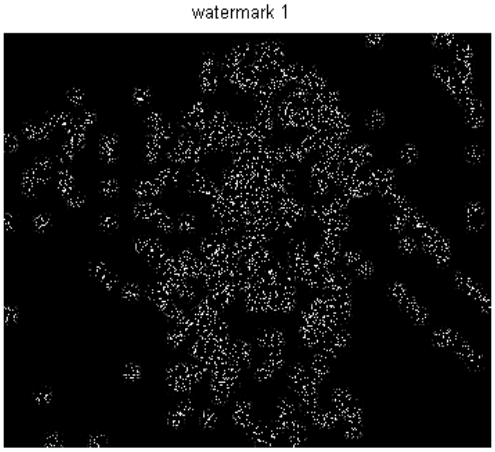

Fig7: Embedded data

3-4 final step: extraction of embedded data

In the data extraction process, at first transform and Inverse quantization coefficients reconstruction conversion, and in next step using the Classification address then carried out with the motion vectors by the perceptual mask can desired data be extracted. (Figure 8)

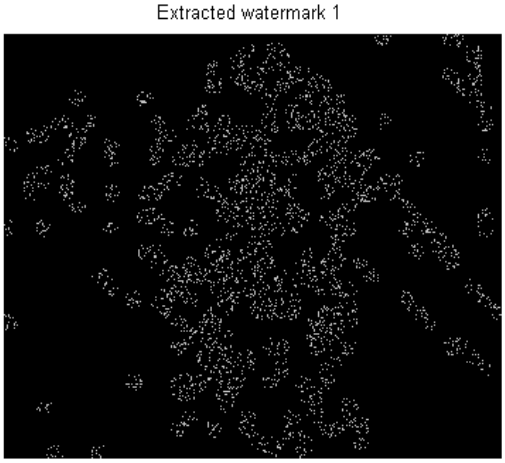

Fig 8: Extracted data

Figure 9 is an example of data steganography in the B, G, R, spaces in a foreman video frame using the proposed scheme shows.

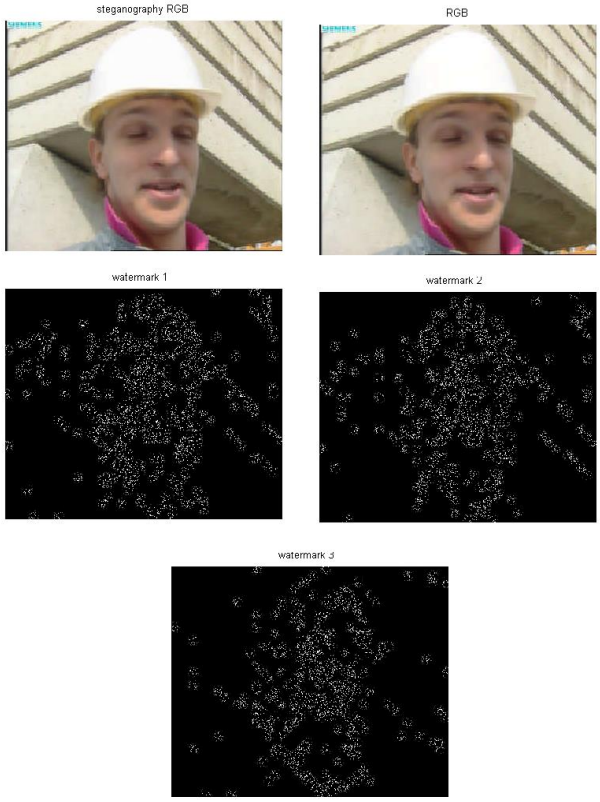

Fig 9 ,steganography: Comparison of the main frame with watermarked frame along with is embedded data.

4- Evaluation of proposed scheme

The first question that may be caused by the proposed scheme by using motion vectors is that why? Regardless of whether the desired motion vectors can not be hid? As the article mentioned at the beginning of the most important things that must be met in a watermarking scheme to maintain transparency, resistance to attacks, watermarking capacity is high. And in this way act 've foregoing is

considered as an example in Figure 10, it is observed that the watermark data , regardless of the motion vectors and transform processes become obscured by the results of data mining is cluttered.

That is virtually the same transformation in the 264H. But can maintain its strength. However, our proposed method due to perceptual mask design, data hiding is carried out in a suitable (Figure 11). Other benefits of transparency in the allocation watermark bit scheme is proposed , as well as resistance to attacks due to the use of motion vectors to put on the edges of the image data , and high capacity watermarking embedding the video. (Figure9)

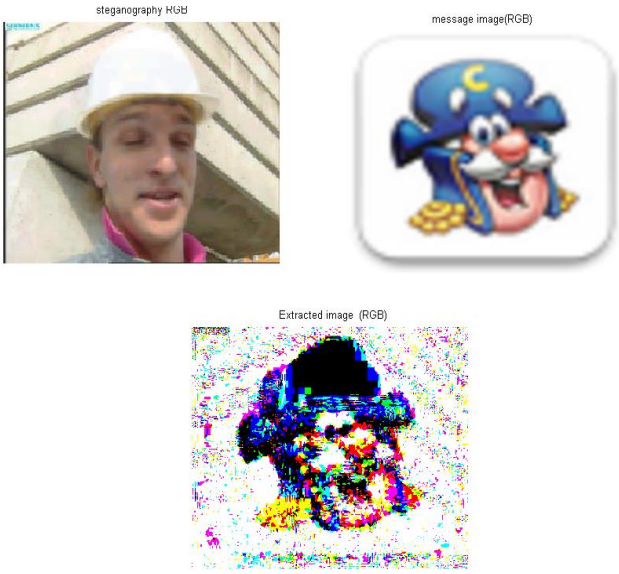

Fig10: Top left: watermarked Frame, upper right: data ,down: extracted data

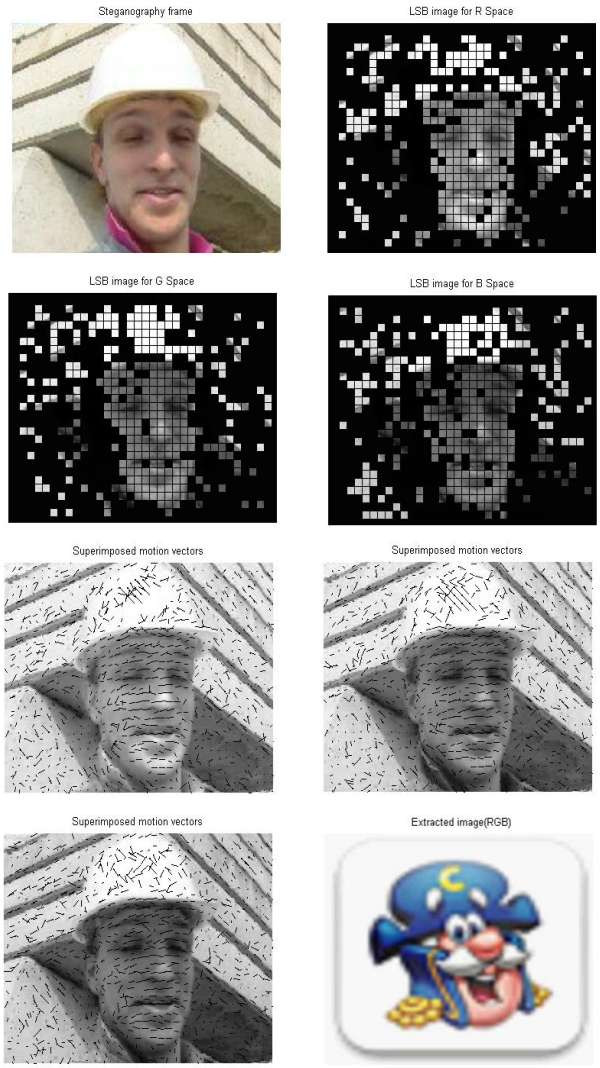

Figure 11: respectively, from top left: Watermarked frame, perceptual mask, motion vectors, extracted data

5- experimental results

In this section, the robustness of the proposed watermarking schemes with some schemes have been tested previously. New video watermarking scheme in which the performance through several experiments ,including experiments with different proportions, experiment with different number of frames, experiment with different qualities and stability test is investigated. In these experiments, the video clip with 1526 frame in size of 352 × 288 was used.

Detect attacks that involve the frame removal, frame averaging, lossy compression, on watermarked video in the resistance test has been done. After extraction and purification watermark, a quantitative measure for judging the extracted data is needed, the results can be measured as Equation 1, the normalized correlation name can be defined.

$$NC = \frac{\sum_i \sum_j W_{ij} \times RW_{ij}}{\sum_i \sum_j W_{ij}^2} \quad (1)$$

In the above equation, normalized correlation using a courier between the reference energy watermarking is performed, where Wij main watermark and RWij extracted watermark. Using these measurements, we evaluate the proposed scheme.
And then also when the NC watermark has been evaluated with various attacks confronted the experimental results it is shown in the following sections.

5-1 Experiment with Frame Dropping in watermarked video

As a video contains a large amount of redundancies between frames, it may suffer attacks by frame dropping. This experiment is aimed at examining the robustness of the scheme under the frame dropping attack. Different percentages of frames are dropped and the obtained results are shown in Figure 12.

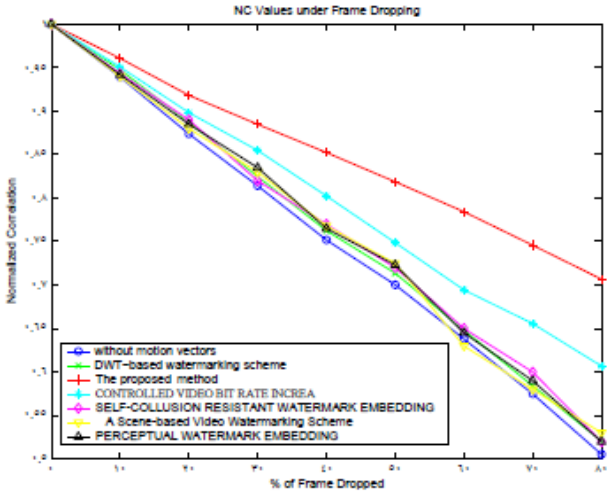

Fig 12: NC values under frame dropping in video

5-2 Experiment with Frame Averaging and Statistical Analysis in watermarked video

Statistical analysis and averaged frames of other common attacks against video watermark . In this way, by taking the average of the number of hidden frames, and finally the original video watermark estimated to be low. Under that scenario, with the results shown.

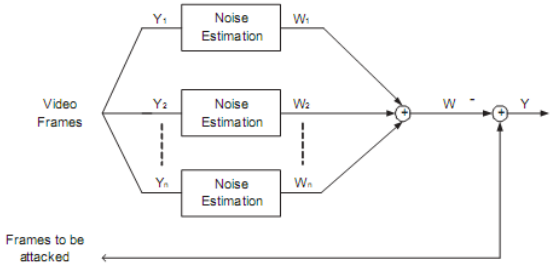

Fig 13: Scenario of statistical averaging attack

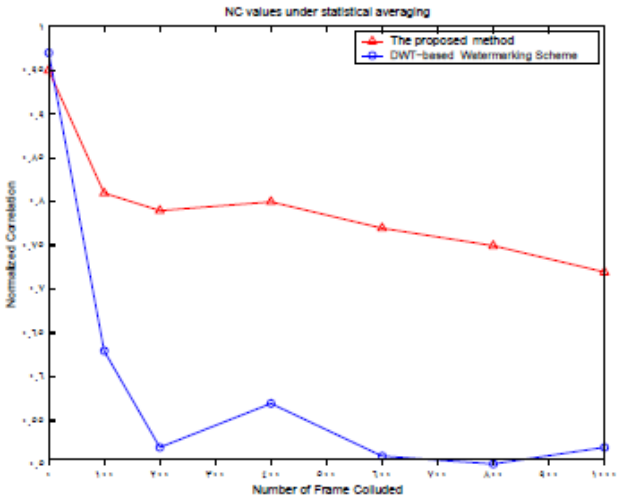

Fig14: NC values under statistical averaging in video

5-3 Experiment with Lossy Compression in watermarked video

This experiment is aimed at testing the robustness of the scheme under attack by lossy compression.

Figure 15 shows the NC values of the extracted watermarks with different quality factors of MPEG.

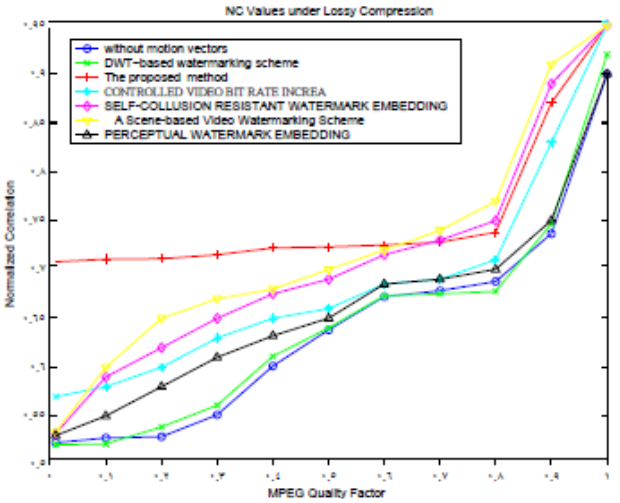

Fig15: NC values under lossy compression in video

5-4 Test of Robustness with StirMark in watermarked frame

In this test video watermark affected by the cropping, PSNR, which has been re-scaling and adding noise values obtained are shown below.

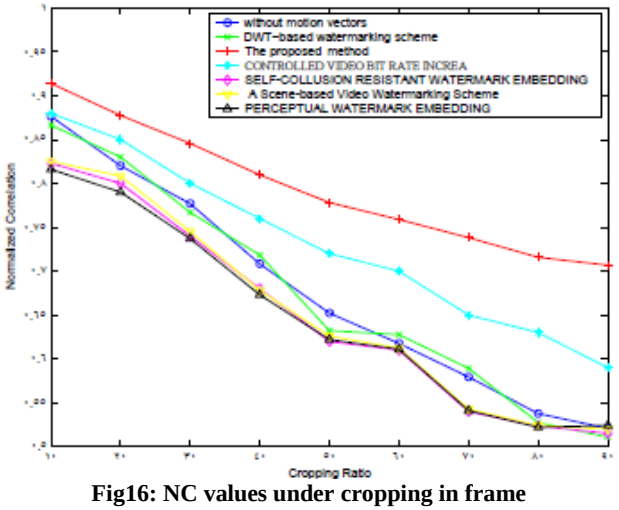

Fig16: NC values under cropping in frame

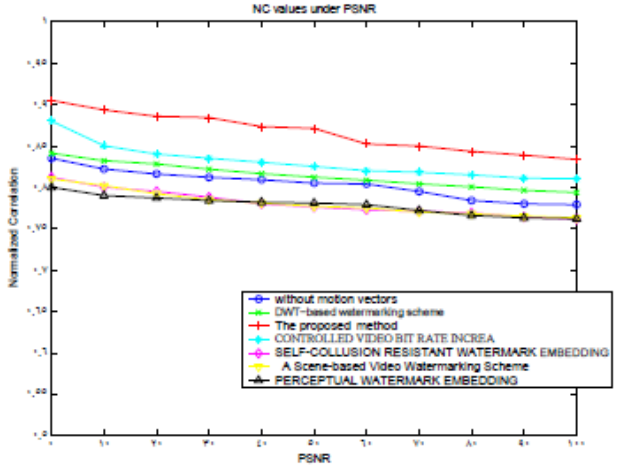

Fig17: NC values under PSNR in frame

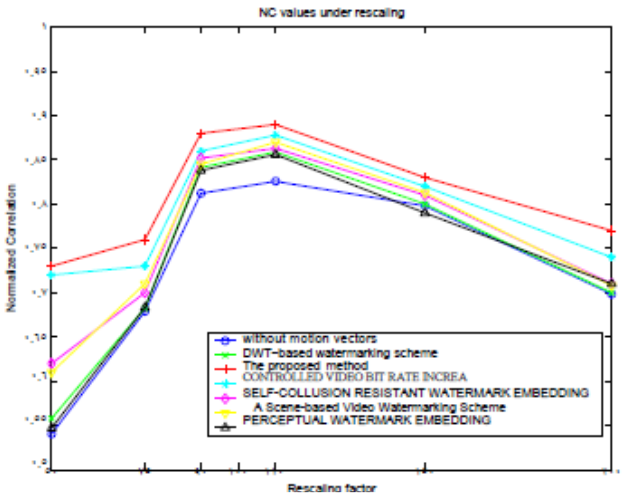

Fig18: NC values under different rescaling factor in frame

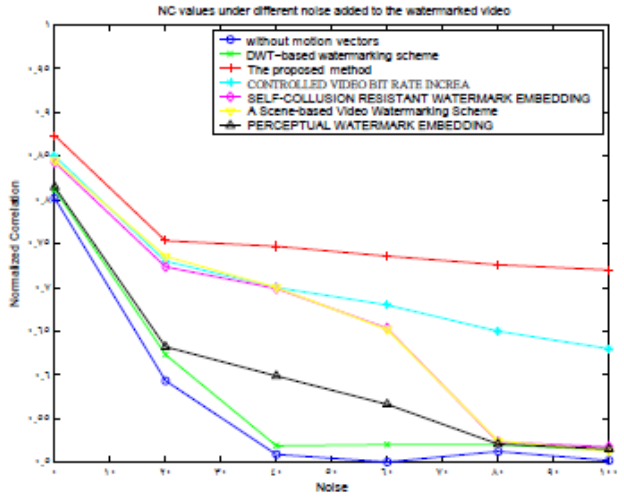

Fig19: NC values under different noise added to the watermarked video

The results obtained above can be seen that our proposed scheme compared to other schemes have been introduced considerably more resistant against attacks your of the show.

6- Conclusions

In this way, we develop new designs video watermarking based on motion vectors for format H.264 We paid. where Watermark the adaptive spatial in transform coefficients of residual macroblock is placed. And a perceptual mask used in a way that ensures optimal distribution between macroblock watermark bit is doing. In this way, a constant power watermark for video compression H.264 Offers a different bit rate and video quality has no impact on the overall rate. The proposed watermarking scheme, we can easily within the framework of the real-time encoder and decoder H.264 be implemented.

7- References

G.C.Langelaar , I. Setyawan and R. L. Lagendijk ,
" Watermarking Digital Image and Video Data " in IEEE Signal Processing Magazine , Sept. 2000 , pp.1053-1058.

S.G. Chang, B. Yu, and M. Vetterli, "Adaptive wavelet thresholding for image denoising and compression," IEEE Transactions on Image Processing, vol. 9, no. 9, pp.1532-1546, September 2000.

S.Jeong , K.Hong Dual , "Detection of A Watermark Embedded in the DCT Domain" ,EE368Aproject Report , Image Systems Eng.Program,Stanford University, 31 May,2001.

F. Argenti and L. Alparone, "Speckle removal from SAR images in the undecimated wavelet domain," IEEE Trans. Geosci. Remote Sensing, vol. 40, pp. 2363–2374, Nov. 2002.

E. Candes, L. Demanet, D. Donoho, and L.Ying, Fast discrete curvelet transforms,Multiscale Model. Simul. 5 (2006), 861{899.

J.W. Goodman, "Some fundamental properties of speckle," Journal Optics Society of America, 66:1145-1150, 1976M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

L. Sendur and I. W. Selesnick, "A bivariate shrinkage function for wavelet-based denoising," in Proc. IEEE Int. Conf. Acoust., Speech, SignalProcessing (ICASSP), Orlando, May 13-17, 2002.

L. Sendur and I. W. Selesnick, "Bivariate shrinkage functions for wavelet-based denoising exploiting interscale dependency," IEEE Trans. Signal Processing, vol. 50, pp. 2744-2756, Nov. 2002.

J.G.Proakis, M.Salehi , " Contemporary Communication Systems using MATLAB" , 2000 by Brooks/Cole Publishing Company, pp. 392-422

D. Field, "Relations between the statistics of natural images and the response properties of cortical cells," J. Opt. Soc. Amer. A, vol. 4, no. 12, pp. 2379-2394, 1987.

E. Simoncelli, "Statistical models for images: Compression, restoration and synthesis," in Proc. 31st Asilomar Conf. Signals, Syst., Comput., Nov. 1997, pp. 673–678.

V. Strela, J. Portilla, and E. Simoncelli, "Image de-noising using a local Gaussian scale mixture model in the wavelet domain," in Proc. SPIE 45th Annu. Meet., 2000.

J. R. Sveinsson and J. A. Benediktsson, "Speckle reduction and enhancement of SAR images in the wavelet domain," in Proc. of Geoscience and Remote Sensing Symposium IGARSS '96, vol.1,pp.63-66, May 1996.

Gérard Blanchet , Maurice Charbit (2008) , " Digital Signal and Image Processing using MATLAB®"

. Iain E. Richardson, (201٠) , "The H.264 Advanced Video Compression Standard" , Second Edition, Vcodex Limited, UK.

- K. S. Thyagarajan, (2011) , "Still Image And Video Compression With MATLAB".

OGE MARQUES, (2011) , "Practical Image And Video Processing using MATLAB®", Florida Atlantic University.

Jayanta Mukhopadhyay, (2011) , " Image and Video Processing in the Compressed Domain" .

C.AGJELIA LYDIA, A.MANJULA, (٢٠١3) , "A Secured Data Hiding Techniques for Motion Vectors using stegnography" , IJCS International Journal of Computer Science .

Hussein A. Aly, (20١1) , "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error". Member, IEEE

P. Johnston, http://pajhome.org.uk/crypt/rsa/intro.html.

Watermarking World, http://www.watermarkingworld.org/.

M. Kutter and F. Hartung, "Introduction to Watermark-ing Techniques," Proceedings Information Techniques for Steganography and Digital Watermarking, S.C. Katzen-beisser et al., Eds. Northwood, MA: Artec House, pp. 11- 111, Dec. 1111.

H. Inoue, A. Miyazaki, and T. Katsura "An Image Wa-termarking Method Based on the Wavelet Transform", Kyushu Multimedia System Research Laboratory.

I. Cox, M. Miller, J. Linnartz, and T. Kalker, "A Review of Watermarking Principles and Practices" Proceedings Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc., pp. 461-482, 1111.

F. Petitcolas, "Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, Vol. 11, pp. 58-64, Sept. 2000.

Maneli Noorkami, " SECURE AND ROBUST COMPRESSED-DOMAIN VIDEO WATERMARKING FOR H.264", thesis, 21 May, 2007

Kutter, M., Jordan, F., and Bossen, F., "Digital signature of color images using amplitude modulation," in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 3022, (San Jose, CA, USA), pp. 518–526,February 1997.

Langelaar, G. C., Lagendijk, R. L., and Biemond, J., "Real-time labeling of MPEG2 compressed video," Journal of Visual Communication and Image Representation, vol. 9, pp. 256–270, December 1998.

Langelaar, G. C., van der Lubbe, J. C. A., and Biemond, J., "Copy protection for multimedia data based on labeling techniques," in Proceedings of 17th Symposium on Information Theory in the Benelux, (Enschede, The Netherlands),May 1996.

Langelaar, G. C., ven der Lubbe, J. C. A., and Lagendijk, R. L., "Robust labeling methods for copy protection of images," in Proceedings of the SPIE - The International Society for Optical Engineering, vol. 3022, (San Jose, CA, USA), pp. 298–309, February 1997.

Liang, Y., Ahmad, I., and Swaminathan, V., "Fast priority search algorithm for block motion estimation," in IEEE International Conference on Multimedia and Expo (ICME), vol. 1, (Taipei, Taiwan), pp. 543–546, June 2004.

Maes, M. J. J. B. and Overveld, C. W. A. M., "Digital watermarking by geometric wrapping," in Proceedings of IEEE International Conference on Image Processing (ICIP), vol. 2, (Chicago, IL, USA), pp. 424–426, October 1998.

Malvar, H. S., Hallapuro, A., Karczewicz, M., and Kerofsky, L.,
"Low-complexity transform and quantization in H.264/AVC," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, pp. 598–603, July2003.

Matsui, K. and Tanaka, K., "Video-steganography," Journal of the Interactive Multimedia Association Intellectual Property Project, vol. 1, no. 1, pp. 187–205, 1994.

Nikolaidis, A. and Pitas, I., "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," IEEE Transactions on Image Processing, vol. 12, pp. 563–571, May 2003.

Nikolaidis, N. and Pitas, I., "Copyright protection of images using robust digital signatures," in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing Conference (ICASSP), no. 4, (Atlanta, GA,USA), pp. 2168–2171, May 1996.