

Robust Video Watermarking Algorithm Using K-Harris Feature Point Detection

Harpreet Singh

Abstract- In this Paper, An effective, robust and imperceptible video watermarking algorithm using K-harris point detection is proposed. The performance of the proposed algorithm was evaluated with respect to imperceptibility, robustness and data payload. This algorithms showed similar but high level of imperceptibility, however their performance varied with respect to robustness and payload. This paper presents a content-based digital image-watermarking scheme, which is robust against a variety of common image-processing attacks and geometric distortions. The image content is represented by important feature points obtained by our image-texture-based adaptive Harris corner detector. These important feature points are geometrically significant and therefore are capable of determining the possible geometric attacks with the aid of the Delaunay-tessellation-based triangle matching method.

Keywords- Robustness, Feature point, video watermarking, Bit error rate(BER)

I. INTRODUCTION

Video watermarking is effectively a new technology that has been provided us a platform to solve the problem of illegal manipulation and distribution of digital video. It is the process of embedding copyright information in video bit streams. In this thesis, I propose one effective, robust and imperceptible video watermarking algorithm using K-harris point detection. In this algorithm, watermark bit information are embedded in the transformed video in a diagonal-wise fashion, and bits are embedded in a blocks-wise fashion. The performance of the proposed algorithm was evaluated with respect to imperceptibility, robustness and data payload. This algorithms showed similar but high level of imperceptibility, however their performance varied with respect to robustness and payload. The diagonal-wise based algorithm achieved better robustness results, while the block-wise algorithm gave higher data payload rate. This paper presents a content-based digital image-watermarking scheme, which is robust against a variety of common image-processing attacks and geometric distortions. The image content is represented by important feature points obtained by our image-texture-based adaptive Harris corner detector. These important feature points are geometrically significant and therefore are capable of determining the possible geometric attacks with the aid of the Delaunay-tessellation-based triangle matching method. The watermark is encoded by both the error correcting codes and the spread spectrum technique to improve the detection accuracy and ensure a large measure of security against unintentional or intentional attacks.

Unobtrusive

The watermark should be perceptually invisible.

Robust

The watermark should not be possible to eliminate even if the principle of the watermarking techniques is public.

Revised Version Manuscript Received on August 14, 2015.

Harpreet Singh, Assistant Professor, Department of Electrical Communication Engineering, Yadawindra College of Engineering, Guru Kashi Campus, Punjabi University Patiala (Punjab). India.

of course, any watermark can be removed with sufficient knowledge of particular embedding process. Therefore, it is enough if any attempts to remove or damage the watermark result in severe quality degradation of the video sequence before the watermark is lost.

Unambiguous

The retrieved watermark should uniquely identify the copyright owner of the content, or in case of fingerprinting applications, the authorized recipient of the content. In order for a watermark to be robust, it must be embedded into perceptually significant regions of video frames despite the risk of eventual fidelity distortion. The reason is quite simple: if the watermark were embedded in perceptually insignificant regions, it would be possible to remove it without severe quality degradation of the cover content. Further, perceptually significant regions should be chosen with respect to sensitivity of human visual system which is tuned to certain spatial frequencies and to particular spatial characteristics such as edge features.

However, geometric manipulations are difficult to tackle because they can introduce the synchronization errors into the watermarking system and render the watermark detection impossible. A lot of research has been conducted to reduce or prevent the asynchronous problem caused by geometric distortions. These methods can be roughly divided into the following three categories:

Template-based watermarking methods [2–4]: These methods intentionally embed additional templates into the image. These templates function as anchor points for the alignment and therefore assist the watermark synchronization in detection process. Invariance-domain-based watermarking methods [5–8]: These methods generally provide rotation, scaling, and translation (RST) invariant domains, namely log-polar domain [7] and Fourier-Mellin transformation domain [5,6,8], for embedding the watermark and maintaining synchronization under affine transforms.

Moment-based watermarking methods [9–13]: These methods utilize the geometric invariants of the image including ordinary moments [9–11] and normalized Zernike moments [12,13] to reduce the synchronization errors in watermark detection process.

II. WATERMARK ATTACKS

This section gives a survey of possible attacks on watermarks. Only attacks that do not severely degrade quality of the cover content are considered. Watermark attacks can be, according to [14], classified into four main groups:

Simple attacks, are conceptually simple attacks that attempt to damage the embedded watermark by modifications of the whole image without any effort to identify and isolate the watermark. Examples include frequency based compression, addition of noise, cropping and correction.

Detection-disabling attacks, attempt to break correlation and to make detection of the watermark impossible. Mostly, they make some geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion. The watermark in fact remains in the cover content and can be recovered with increased intelligence of the watermark detector.

Ambiguity attacks attempt to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which was the first, authoritative watermark.

Removal attacks attempt to analyse or estimate (from more differently watermarked copies) the watermark, separate it out and discard only the watermark. Examples are collusion attack, denoising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements). It should be noted that some attacks do not clearly belong to one group.

III. WATERMARKING EMBEDDING PROCEDURE

The embedding procedure of the first algorithm, with its three possible variations, is described in details in the following steps:

- Step 1: Divide the video clip into video scenes.
- Step 2: Process the frames of each video scene using block division described in steps 3 ~ 9 below.
- Step 3: Convert every video frame F from RGB to YCBCR color matrix format.
- Step 4: Do the block division process for the S matrix in each frame F. This operation generates 3*3 matrices.
- Step 5: Rescale the watermark image so that the size, of the watermark will match the size of the matrix which will be used for embedding S.
- Step 6: Embedding can be done in one of 3*3 matrices frames.
- Step 7: Convert the video frames F' from YCBCR to RGB color matrix.
- Step 8: Reconstruct frames into the final watermarked Video scene.
- Step 9: Reconstruct watermarked scenes to get the final watermarked Video clip.

Block division is a numerical technique for dividing the watermarked image into 3*3 matrices in which the transformed domain consists of basis states that is optimal in some sense. The block division of an $S = N \times N$ matrix, a frame image is treated as a matrix decomposed into the three matrices shown in in Figure 3.1.

Block division Watermark

Block watermarking method belongs to frequency domain techniques. The method consists in coding one watermark element into one block of a macro block residual. Only 3x3 blocks are supported because of the following. The partitioning of macro block residuals into blocks may change when the video sequence undergoes any video signal processing operation. The simplest example is recompression with different parameters.

The problem occurs when the watermark element has been embedded into a macro block partitioned into 8 3x3 blocks and the partitioning has changed to 4 3x3 blocks,

or vice versa. Changes made by watermark embedding in one partitioning are basically undetectable in the other partitioning because the transforms are not equivalent in terms of transform coefficient values. It would be possible to convert the blocks to the former partitioning before detection but it is not obvious which partitioning is the former one. Therefore, the conversion to one type of partitioning has to be applied before embedding. After embedding, the partitioning is converted back to the former type in order to preserve macro block properties. In the detection process, the conversion to the same type as in the embedding process is applied before detection. To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on various standard 8-bit grayscale frames of size 3*3 metrics and different kinds of attempting attacks. Proposed watermarking methods have been exposed to several tests in order to check up and compare their qualities and robustness. The test results are summarized in this chapter. The test scripts have been executed on several video sequences with different characteristics. Most of them have been downloaded from high-definition video gallery [15] on the Apple website. Video-watermarking method with results are conducted with original video and prepared video from original video for water-marking. As it is well known that complete video consist of no. of pictures or frames.

Video = No of picture or frames

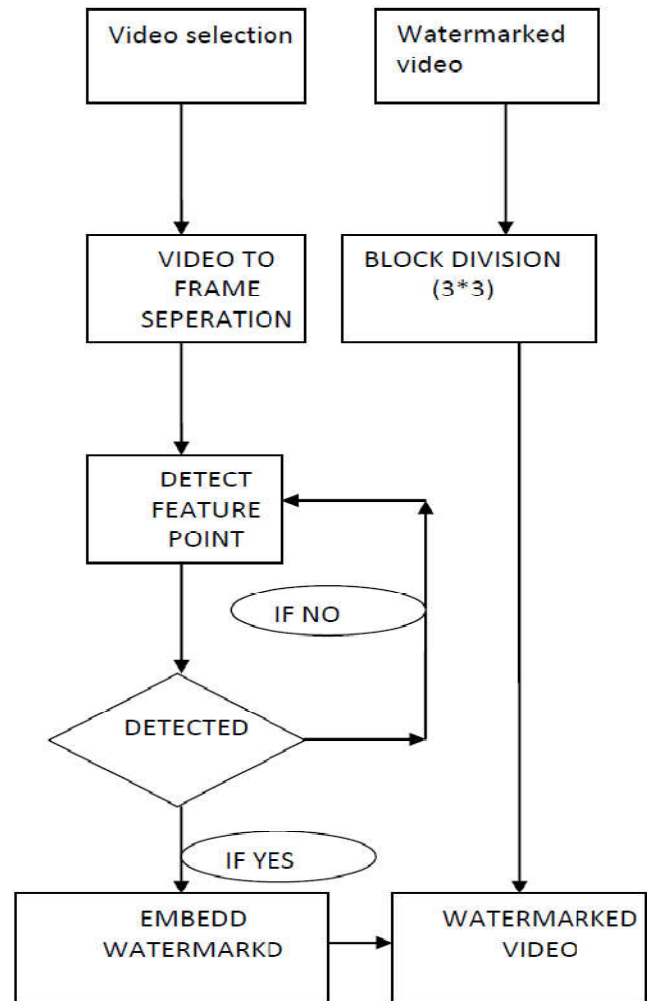


Figure:3.1 flow chart for video watermak Embedding Algorithm

IV. RESULTS

In india as per the frequency range for electricity is 50 HZ and 220 V supply , one complete video can be made with 25 frame/sec for avoiding flickring effect.In following diagrams , we have 20 frames or pictures with one prepared video from original video for water-marking and second watermarked video. In watermarked video ,using detector response earlier discussed , It is detected the the feature corner point on watermarked video. See in Watermarked Video picture no-1 ,where written Director :Sandeep Sharma . At corner of **Director** word feature point is detected ,where watermarked is to be embedded.

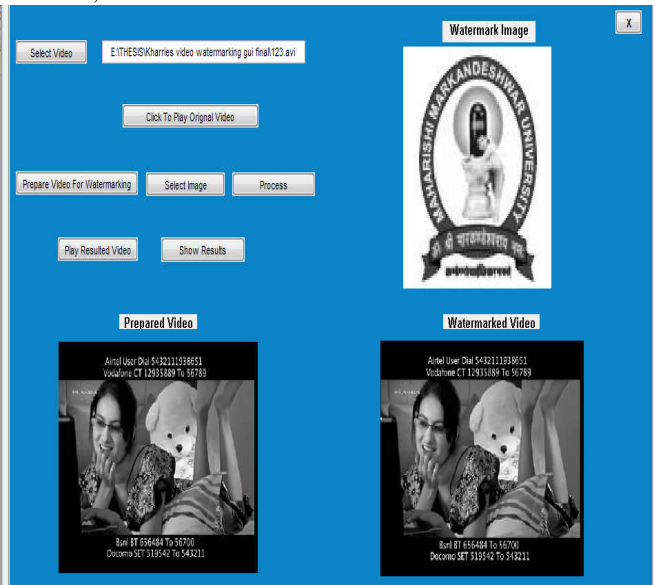
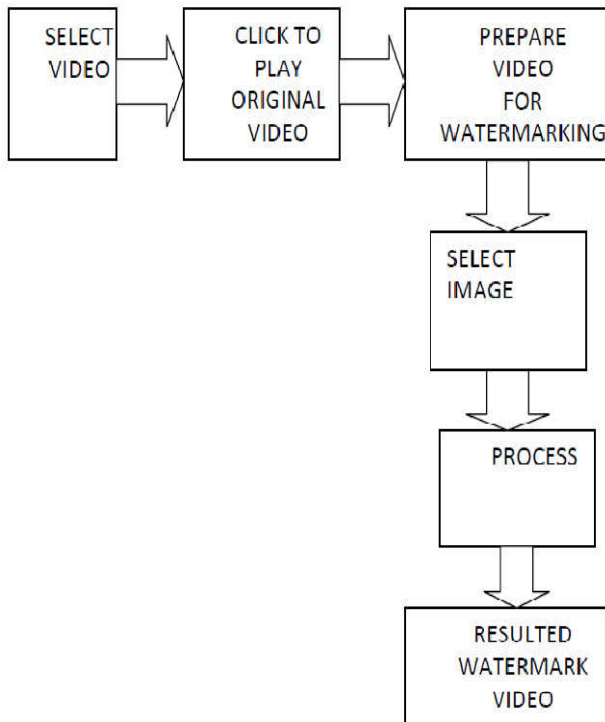
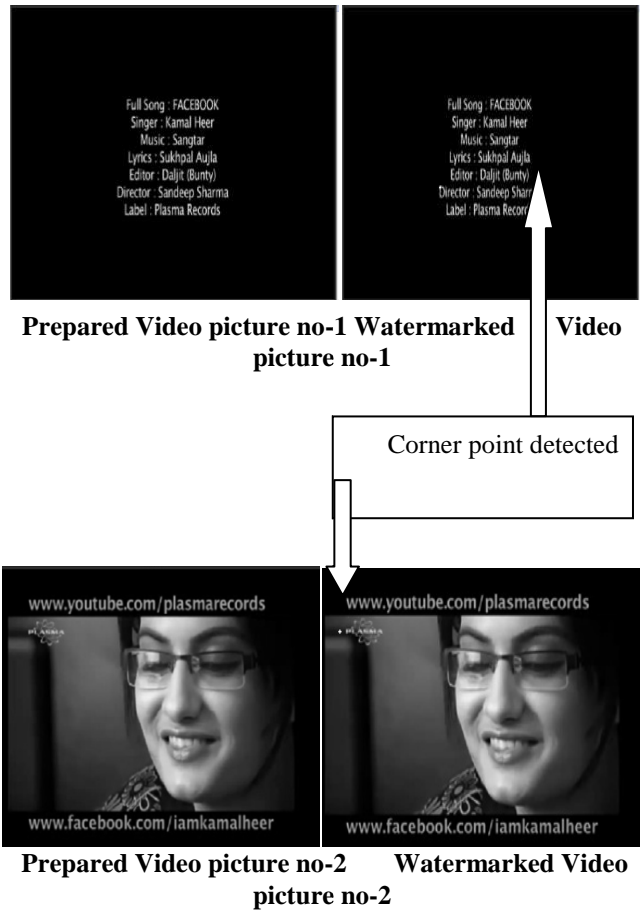


Figure 3.2: Graphical User Interface (GUI) for watermark-embedding Procedure

GUI FLOW CHART



In Graphical user interface(GUI) flow chart, overall video watermarking process is explained to provide proper security to video to avoid unauthorized access.



4.1 Corner point detection

The common Harris corner detector Bas et al. [16] evaluate the performance of three commonly used detectors (i.e., the Harris corner detector [17], That is, for different distorted versions of the same scene, the detector should be able to extract similar, if not identical, points, despite variations due to a change of orientation or sharpness. The results of these studies prove the Harris detector is the most stable. The commonly used Harris corner detector refines the detection function [18] by using the following shape factor-based matrix.

$$M(x,y) = \begin{pmatrix} A_{x,y} & C_{x,y} \\ C_{x,y} & B_{x,y} \end{pmatrix} = \begin{pmatrix} \left[\frac{\partial I(x,y)}{\partial x} \right]^2 & \left[\frac{\partial I(x,y)}{\partial x} \right] \left[\frac{\partial I(x,y)}{\partial y} \right] \\ \left[\frac{\partial I(x,y)}{\partial x} \right] \left[\frac{\partial I(x,y)}{\partial y} \right] & \left[\frac{\partial I(x,y)}{\partial y} \right]^2 \end{pmatrix}$$

where I(x, y) is the gray level intensity in x-axis and y-axis,

The corner points are located at the positions with large corner response values, which are determined by the corner response function R(x, y):

$$R(x, y) = (\det(M(x,y)) - k[\text{trace}M(x,y)]^2) = (A_{x,y}B_{x,y} - C_{x,y}^2) - k[A_{x,y} + B_{x,y}]^2$$

where k is a constant that is set to be 0.04.

The following four steps detail the image content extraction procedure:

1. Apply a Gaussian low-pass filter to original image I(x, y) to avoid corners due to image noise.

2. Apply a rotationally symmetric 33 Gaussian low-pass filter with the standard deviation of 0.5 to three derivative images, namely, $A_{x,y}$, $B_{x,y}$ and $C_{x,y}$ to achieve additional resistance to possible image noise.

3. Calculate $R(x, y)$ within a circular window, which is at the image center and covers the largest area of the original image. The resulting function reduces the effect of image-center-based rotation attacks.

4. Apply a threshold T on $R(x, y)$ and search for important feature points based on the local maxima

$$\{R(x, y) \geq T \cap R(x, y) \geq R(u, v), \forall (u, v) \in V_x\}$$

where T is a predefined threshold value that is empirically set to be 10^6 in our scheme to extract a desired number of corner points, and $V_{x,y}$ represents a circular neighborhood centered at (x, y) .

4.2 Perceptibility

Perceptibility expresses amount of distortion caused by watermark embedding. In other words, it indicates how visible the watermark is. It is measured by peak signal-to-noise ratio (PSNR) Bit error rate (BER) and Mean square error (MSE) which is mentioned in Section III. The less the value of PSNR and more value of MSE and BER is the more perceptible the watermark is. We can see in the first row set of figures (4.2,4.3,4.6,4.7,4.10,4.11 and table (4.1,4.2,4.3,4.4) that the perceptibility grows up with increasing decreasing value of PSNR and increasing value of MSE and BER. It is obvious that block method is the most perceptible method because of the way of embedding. The second row set of the table contains probabilities of watermark detection success in non-attacked sequences as given by the detector.

4.2.1 Mean Square Error (MSE)

Mean Square Error between original video and watermarked video is calculated as follows:

$$MSE = \frac{1}{\text{size of image}} \sum_{i,j} [\text{Original Image} - \text{Watermarked Image}]^2$$

4.2.2 Peak Signal to Noise Ratio (PSNR)

PSNR is calculated between the original and watermarked video. Larger the PSNR value, more similar is watermarked video to the original video. The video quality metric is defined in decibels as:

$$PSNR = 10 \log_{10} \frac{255 \times 255}{MSE}$$

4.2.3 Bit Error Rate (BER)

The performance metric is suitable for random binary sequence watermark. The parameter is defined as ratio between numbers of incorrectly decode bits and length of the binary sequence. BER indicates probability of incorrectly decoded binary patterns. It is defined as follows:

$$BER = \frac{\text{No. of incorrectly decoded bits}}{\text{Total no. of bits}}$$

The performance results of the K-harris algorithm were tested for test video frame 'Clock_480by360' which are shown in figure 4.4. The properties of the test video frame are highlighted in table 4.1 and 4.2 and 4.3,4.4. Three test binary watermarks of different sizes used for implementation of proposed algorithms are shown in table 4.5.



Figure 4.1: watermarked logo of size (9×12)

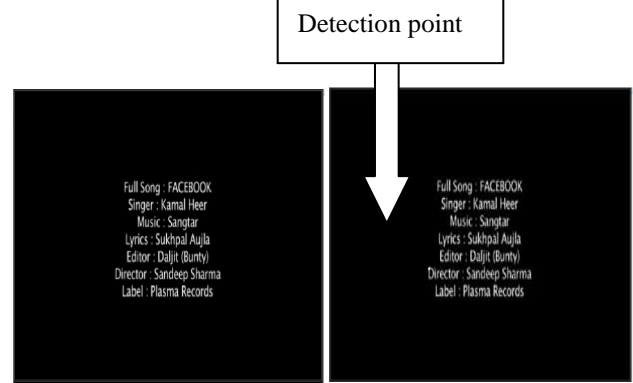


Figure 4.2 : Prepared Video picture no-1 Figure 4.3: Watermarked Video picture no-1

Imperceptibility means that the perceived quality of the video clip should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked video, the Peak Signal to Noise Ratio (PSNR) is typically used. In our study, the watermark was embedded in the video according to the procedure described. The PSNR of the 1st video frame is 71.1852 dB. This high PSNR value and low value of BER and MSE proves imperceptibility of the proposed K-harris based algorithm. As per logo selected of size 9x12 to be embedded in video frames, the PSNR value is 71.1852 dB, BER is 1.42% and MSE is 0.48% shown in figure 4.4 and table 4.1. For an effective watermarking the two fundamental requirements need to be satisfied i.e. transparency and robustness. The transparency represents the invisibility of the watermark embedded in the signal data without degrading the perceptual quality, and the robustness which means the watermark should not be removable by attacks, including signal processing, compression, re-sampling, frame dropping, frame averaging, cropping, etc. It is a very important requirement for digital watermarking in any application.

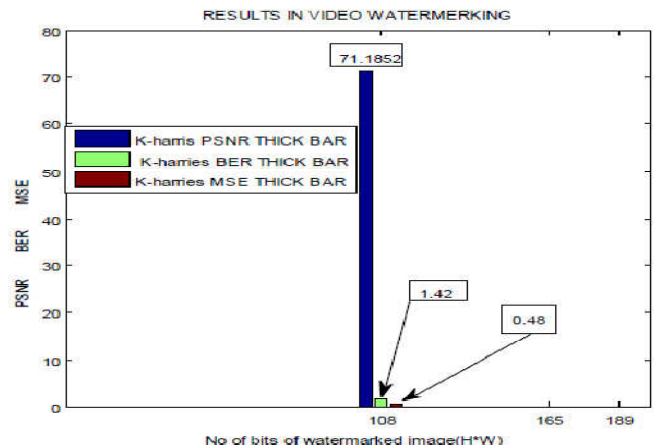


Figure 4.4: Graph for calculation of PSNR, BER, MSE of watermark size (9 x 12) with no imperceptibility

Table 4.1 video watermarking quality parameters (9 x 12)

Parameter for figure (4.2, 4.3, 4.4) with Watermark size (9x12) and video frame Size (322x322)	Values after embedding of water -mark
MSE mean square error	0.48%
PSNR peak signal to Noise ratio	71.1852dB
BER Bit Error Rate	1.42%

Table 4.4 gives test watermarks properties. All watermarks are binary image. From Table 4.5 and 4.6, we plotted a graph of number of bits of watermark image (HxW) versus PSNR(dB) of watermarked video frame /BER(%) of recovered watermark image / MSE of recovered watermark image. Our objective is to find a theoretical watermarking capacity (Number of Bits of watermark image) bound of digital images based on PSNR of watermarked image and MSE and %BER of recovered watermark. As Number of Bits of watermark image is increased, PSNR of watermarked video frame is decreased, MSE is decreased and %BER of recovered watermark is increased as shown in figure 4.4 4.8 ,4.12 and 4.14

The PSNR of the 2nd video frame is 68.1749 dB. This high PSNR value and low value of BER and MSE proves imperceptibility of the proposed K-harris based algorithm. As per logo selected of size 11x15 to be embedded in video frames, The PSNR value is 68.1749 dB, BER is 1.46% and MSE is 0.70%. As Number of Bits of watermark image is increased, PSNR of watermarked video frame is decreased, MSE is increased and %BER of recovered watermark is increased as shown in figure 4.8 and table 4.2.



Figure 4.5: watermarked logo of size (11x15)

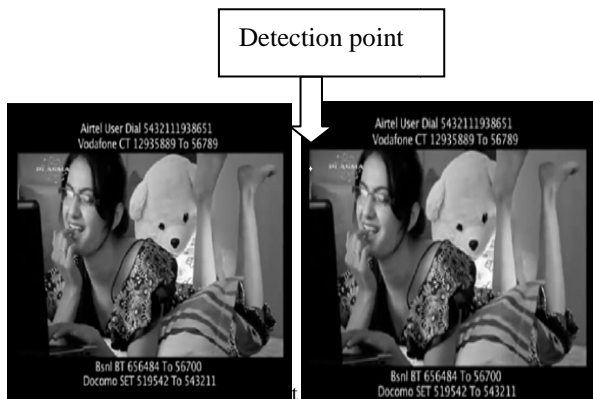


Figure 4.6: Prepared Video picture no-2 Figure 4.7: Watermarked Video picture no-2

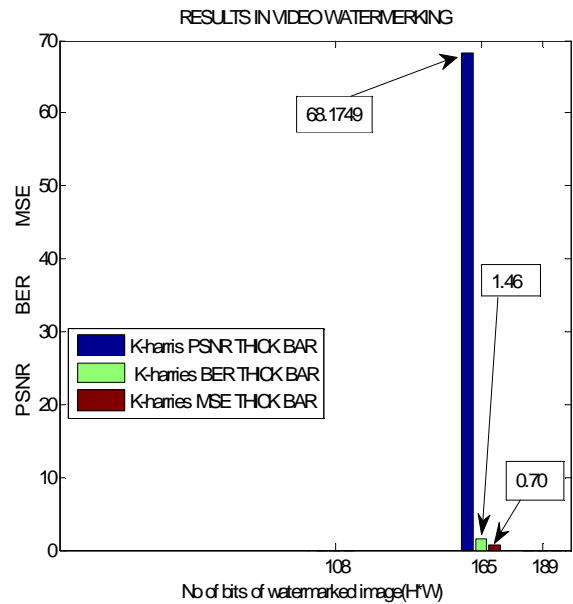


Figure 4.8: Graph for calculation of PSNR, BER, MSE of watermarks size (11 x 15) with no imperceptibility

Table 4.2 video watermarking quality parameters (11 x 15)

Parameter for figure (4.6, 4.7, 4.8) with Watermark size (11x15) figure (4.5) and video frame Size (322x322)	Values after embedding of water -mark
MSE mean square error	0.70%
PSNR peak signal to Noise ratio	68.1749dB
BER Bit Error Rate	1.46%



Figure 4.9: watermarked logo of size (21x9)



Figure 4.10: Prepared Video picture no-3 Figure 4.11: Watermarked Video picture no-3

Robust Video Watermarking Algorithm Using K-Harris Feature Point Detection

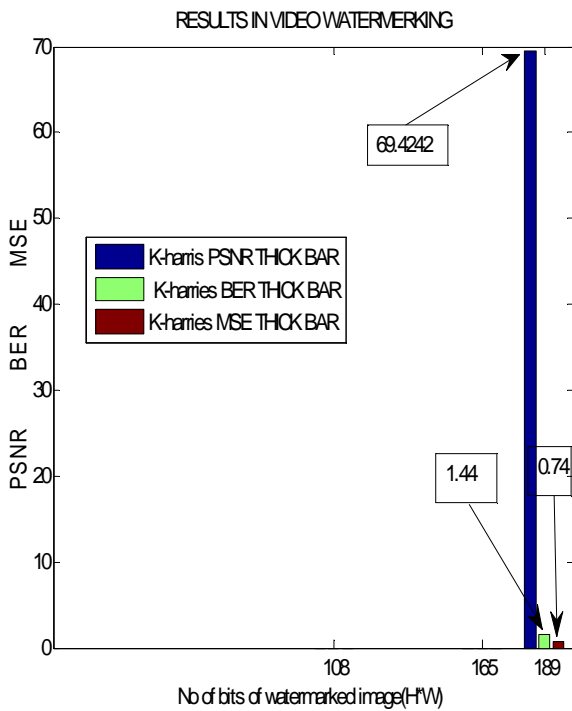


Figure 4.12 Graph for calculation of PSNR, BER, MSE of watermark size (21 x 9) with no imperceptibility.

Table 4.3 video watermarking quality parameters (21 x 9)

Parameter for figure (4.10, 4.11, 4.12) with Watermark size (21x9) figure (4.9) and video frame Size (322x322)	Values after embedding of water -mark
MSE Mean Square Error	0.74%
PSNR peak signal to Noise ratio	69.4242dB
BER Bit Error Rate	1.44%

The PSNR of the 3rd video frame is 69.4242 dB. This high PSNR value and low value of BER and MSE proves imperceptibility of the proposed K-harris based algorithm. As per logo selected of size 21x9 to be embedded in video frames, The PSNR value is 69.4242 dB, BER is 1.44% and MSE is 0.74%. As Number of Bits of watermark image is increased, PSNR of watermarked video frame is decreased, MSE is increased and %BER of recovered watermark is increased as shown in figure 4.12 and table 4.3.

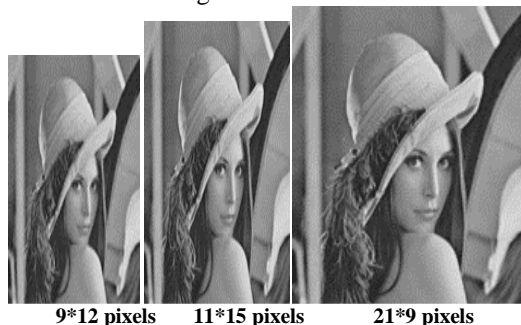


Figure 4.13: watermarked logo of different sizes

Overall results and comparative study of proposed and DWT techniques for parameter PSNR, BER and MSE with different watermarks sizes selected as shown in figures 4.13 to be embedded in video frames AVI extension of size (322x322) with frame rate 10 frames per second have been shown in figure (4.14) and tables (4.4,4.5,4.6).

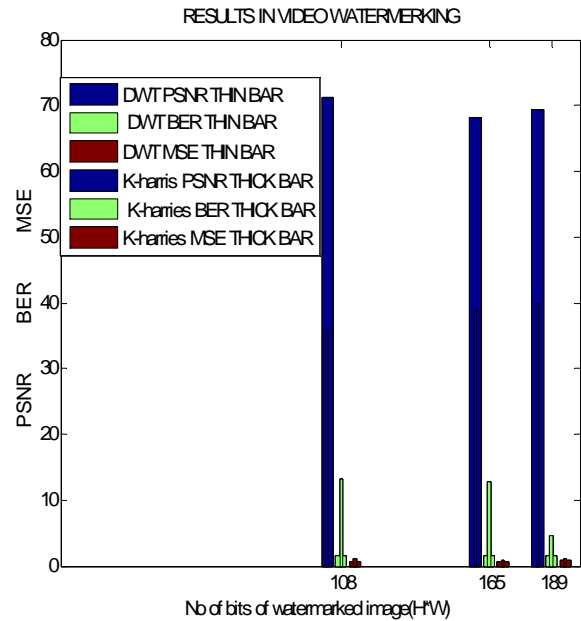


Figure 4.14: Graph for calculation of PSNR, BER, MSE watermarks size (9 x 12, 11 x 15, 21 x 9) with no imperceptibility

Now see Table 4.4 Test Video Properties, Table 4.5: Test Watermarks Properties, Table 4.6: Performance Matrices of Proposed Algorithm for Test Video Frame for 3 Watermarks of Different Sizes

Table 4.4.: Test Video Properties

Test video frame	Type	Frame size (HxW)	No. of frames	Frame rate
Clock _480by360 Using K-harris	AVI	480*360	40	25 frames per sec
Clock _480by360 Using DWT	AVI	322*322	12	10 frames per sec

Video type taken: AVI

Image type to be embedded taken: BMP

Comparison of DWT techniques with K-harris feature point method

Table 4.5: Test Watermarks Properties

Test watermark	TYPE	Using K-harris, Image size(HxW)	Using K-harris No. of bits of watermark image(HxW)
Watermark1	BMP	9x12	108
Watermark2	BMP	11x15	165
Watermark3	BMP	21x9	189

Table 4.6: Performance Matrices of Proposed Algorithm for Test Video Frame for 3 Watermarks of Different Sizes

Test Image frame	Test watermark	Using K-harris PSNR of watermarked videoframe	Using K-harris % BER	Using [49] DWT PSNR of watermarked video frame	Using [49] DWT % BER
9×12	Watermark1	71.1852dB	1.40%	40dB	4.6%
11×15	Watermark2	68.1749dB	1.46%	39dB	12.72%
21×9	Watermark3	69.4242dB	1.44%	36dB	13.22%

V. CONCLUSION

In this paper, interest points in K-harris feature point detection are employed in the video watermarking. Applying K-harris method to video watermarking is beneficial to locate the embedding frame index and coordinates, which improves the robustness resisting against both spatial and temporal attacks efficiently. The quantization scheme realizes the blind extraction meeting the requirement for video watermarking. The experimental results show that the proposed scheme preserves not only the high perceptual quality, but also is robust against various attacks. The key idea of the proposed algorithm is the combination of the k-harris feature point detection algorithm and watermarking algorithm, the performance of K-harris detection scheme influences the performance of the whole scheme greatly. Watermarking is a copy protection system that allows tracking back illegally produced copies of the protected multimedia content. Compared with other copy protection systems like Digital Rights Management, the main advantage of watermarking is that the watermark is embedded permanently in visual data of the content but at the cost of slight loss in fidelity.

REFERENCES

1. F. Peticolas, R. Anderson, M. Kuhn, Attacks on copyright marking systems, in: Proceedings of the Second Workshop Information Hiding, Portland, OR, April 1998, pp. 218–238.
2. S. Pereira, J.J.K. O’Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, Template based recovery of Fourier-based watermarks using log-polar and log-log maps, in: Proceedings of the IEEE International Conference Multimedia Computing Systems, vol. 1, Florence, Italy, June 1999, pp. 870–874.
3. S. Pereira, T. Pun, Robust template matching for affine resistant image watermarks, IEEE Trans. Image Process. 9 (6) (2000) 1123–1129.
4. Digimarc Corporation, US patent 5,822,436, Photographic Products and Methods Employing Embedded Information.
5. J.J.K. O’Ruanaidh, T. Pun, Rotation, scale, and translation invariant digital image watermarking, in: Proceedings IEEE International Conference Image Processing, Santa Barbara, CA, 1997, pp. 536–539.
6. J.J.K. O’Ruanaidh, T. Pun, Rotation, scale, and translation invariant spread spectrum digital image watermarking, Signal Process. 66 (3) (1998) 303–317.
7. D. Zheng, J. Zhao, A. El Saddik, RST-invariant digital image watermarking based on log-polar mapping and phase correlation, IEEE Trans. Circuits Syst. Video Technol. 13 (8) (2003) 753–765.
8. C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller, Y.M. Lui, Rotation, scale, and translation resilient watermarking for images, IEEE Trans. Image Process. 10 (5) (2001) 767–782.

9. M. Alghoniemy, A.H. Tewfik, Geometric distortion correction through image normalization, in: Proceedings of IEEE International Conference Multimedia Expo, vol. 3, 2000, pp. 1291–1294.
10. M. Alghoniemy, A.H. Tewfik, Image watermarking by moment invariants, in: Proceedings of IEEE International Conference Image Processing, vol. 2, January 2000, pp. 73–76.
11. M. Alghoniemy, A.H. Tewfik, Geometric invariance in image watermarking, IEEE Trans. Image Process. 13 (2) (2004) 145–153.
12. H.S. Kim, H.K. Lee, Invariant image watermark using Zernike moments, IEEE Trans. Circuits Syst. Video Technol. 13 (8) (2003) 766–775.
13. Y. Xin, S. Liao, M. Pawlak, Geometrically robust image watermarking via pseudo-Zernike moments, in: Proceedings of the Canadian Conference Electrical and Computer Engineering, vol. 2, May 2004, pp. 939–942.
14. Frank Hartung, Jonathan K. Su and Bernd Girod: Spread Spectrum Watermarking: Malicious Attacks and Counterattacks. Security and Watermarking of Multimedia Contents, 1999.
15. Apple - QuickTime - HD Gallery, <http://www.apple.com/quicktime/guide/hd/>
16. P. Bas, J.M. Chassery, B. Macq, Geometrically invariant watermarking using feature points, IEEE Trans. Image Process. 11 (9) (2002) 1014–1028.
17. C. Harris, M. Stephen, A combined corner and edge detector, in: Proceedings of Fourth Alvey Vision Conference, Manchester, 1988, pp. 147–151.
18. H. Moravec, Obstacle avoidance and navigation in the real world by a seen robot rover, Robotics Institute, Carnegie- Mellon Univ., Pittsburgh, PA, Tech. Rep. CMU-RI-TR-3, September 1980.
19. Deepa Satish Khadtare(2011), International Journal of Advanced Engineering Research and Studies, A robust video watermarking approach for raw video and its DSP implementation, pp 1-6