

ISSN 2063-5346



IMPROVED TOOL FOR EVALUATING ROBUSTNESS OF VIDEO WATERMARKING SCHEME USING DWT SUB-BAND

Kainjan Sanghavi¹, Mahesh Sanghavi², Neeta Deshpande³

Article History: Received: 10.05.2023

Revised: 29.05.2023

Accepted: 09.06.2023

Abstract

Video watermarking is the best technique for copyright protections & proof of ownership, and many researchers in the past devised robust algorithms to protect the same. Visimark 1_0 proposed in 2013 as an evaluation tool for video watermarking, working with raw video, i.e. avi format. Visimark 1_0 covers many more attacks and saves much more time for the video watermarking community. By observing the need for the recent file format, this article proposes the next version of Visimark, i.e. Visiamark 2_0, with some new kinds of attacks. Visimark 2_0 also offers the provision for watermark extraction from all the attacked videos.. Visimark 2 covers all the attacks of Visimark 1. Additional attacks proposed in Visimark 2 are, in the transform domain, ambiguity attack and improved frame dropping attacks. For the demonstration purpose, HL & LH sub-band of DWT is used for all the attacks

Keyword: Copyright, Digital Watermarking, DWT, MSE, PSNR.

¹Associate Professor, SNJB's Late Sau KBJ CoE, Chandwad-423101, Maharashtra, India, kainjan@gmail.com

²Professor, SNJB's Late Sau KBJ CoE, Chandwad-423101, Maharashtra, India, sanghavi.mahesh@gmail.com

³Professor, RH Sapat CoE, Nashik, Maharashtra, India, neeta.deshpande@ges-coengg.org

DOI:10.48047/ecb/2023.12.9.74

1. Introduction

The utilization of the web is expanding step by step; contributing to the greater part of information in text, image, audio and video dispersed straightforwardly from the web. This leads to broad curiosity in multimedia security and multimedia copyright protection. Digital watermarking is proven to be one of the pioneering technique to protect the copyrights and hence ownership issues. Many kinds of literature are proposed to solve the problem of copyright protection [1], [2], copy protection [3], authentication [4], ownership problems [5], [6]. There are so many algorithms are proposed for the robustness of the image, audio and videos. Table 1 summarises different benchmarking tools for assessing the robustness of the video watermarking introduced previously.

2. Motivation

This work is motivated due to the trouble that the author faced while designing the attacked videos during dissertation work. Many benchmarking tools are available for the evaluation of image and audio watermarking. Unfortunately, there is no tool to authenticate the sturdiness of the video watermarking algorithm. To assess the robustness, one has to go through the cumbersome processes depicted in figure 1.

Figure 1 shows steps to create an attacked video from the original supplied video.

1. Decompose the video into various frames
2. Apply different attacks using any of the benchmark tools like Stirmark [8], [9], Checkmark [10] or Optimark [11], Open Watermark [12] to every frame.
3. Resemble all the frames to form an attacked video.

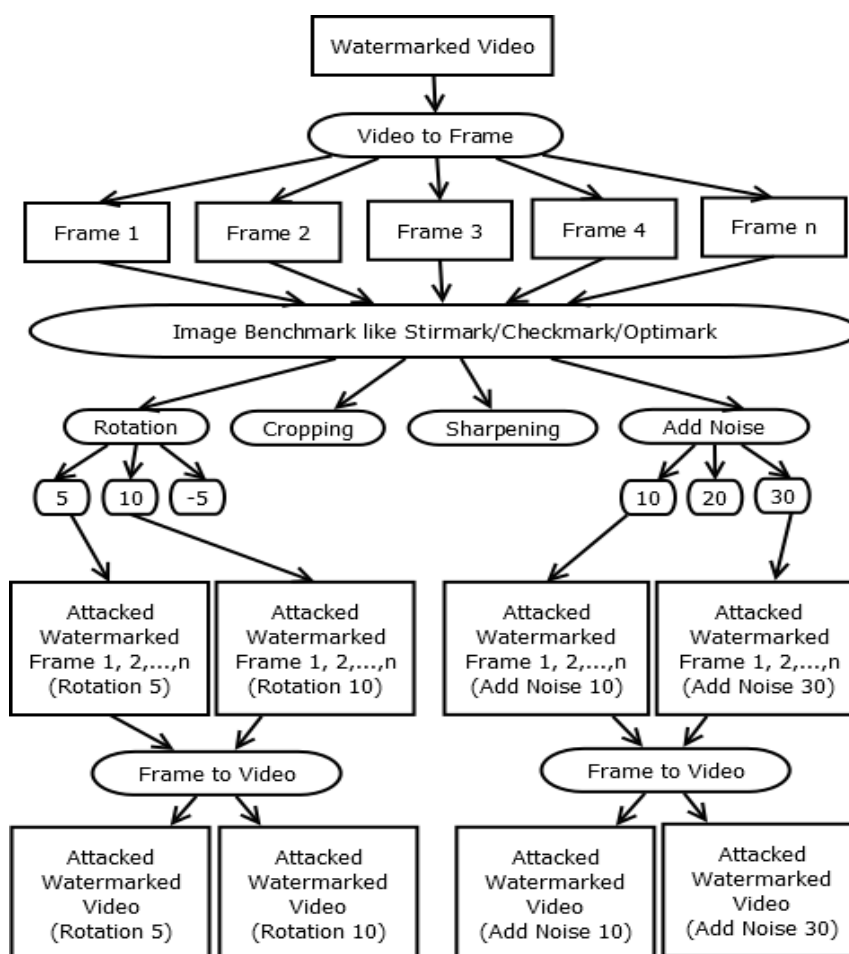


Fig. 1 Flowchart to get attacked watermarked video before Visimark Tool

Table 1 Comparison of various Benchmarking Tools [7]

Parameters/ Tools	Stirmark (Audio & Image)	Check mark	Optimark	Matmark	Open Watermark	Mesh Bench mark	Visimark 1_0
Developed in Language	C++	Matlab	C++	C++	Java	C++	Matlab
Media	Image & Audio	Image	Image	Audio	Image	Image	Image / Video
Signal Processing Attacks & Watermark Disabling Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Watermark Removal Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ambiguity Attack	No	No	Yes	No	No	No	No
Video Attacks	No	No	No	No	No	No	Yes

This system turns out great for different attacks such as image processing attacks, filtering, noise inclusion etc.

But with a limitation, one cannot use direct video attacks like frame dropping, frame averaging and many more. In the reference [7], the author also introduced many tools for the evaluation of video watermarking algorithm. A crystal clear comparison of various available benchmarking tools for images and audio are shown in table 1. Given the future scope, there is no direct tool available for the evaluation of video watermarking algorithm. The author of the paper [7] discusses the four types of attacks possible for watermarking schemes. They are as follows:

1. Simple Attack: The attack applied to the whole image to damage the watermark. Here the intention is only to damage the watermark but not to detect it. Compression, noise addition, cropping etc., are examples of such a category of attack.

2. Detection-disabling attack: This attack category usually tries to disable the cover media's watermark. Here, an attacker attempts to recognize the location of the

watermark in the given input image/video. Examples of this type of attacks are geometric transformations like rotation, cropping, translation, flipping, pixel removal, scaling etc.

3. Ambiguity attacks: This attack category is mainly confusing the detector by embedding several fake watermarks into watermarked image/video. For the watermark research community, handling this category of attacks is a challenging task.

4. Removal attacks: As the name indicates, this attack attempts to eradicate the watermark from the input image/video. Collusion attack, denoising etc., comes under this category of removal attacks.

Apart from the above category of the attacks, there is some more special category of the video attacks such as dropping, averaging, swapping of frames, and swapping or dropping of scenes.

I. About Visimark 1_0:

Visimark 1_0 proposed in [13] gives a details discussion about the Visimark 1_0, a mechanism for sturdiness assessment of the digital watermarking algorithm especially for Video and images. Visimark 1_0 dealt with a raw video (avi format) and stated the few video watermarking attacks. It supports almost 30 attacks. There are mainly three categories of attacks implemented in VisiMark1_0.

1. Video attacks (Frame-based, Scene-based attacks).
2. Geometrical attacks (Rotation, Scaling, Cropping, Sharpening, Shearing, Flipping etc.)
3. Signal and/ image processing attacks (Noise, Filtering attacks etc.).

Visimark 1_0 supports all kinds of attacks like Simple, Detection disabling, removal attack and special video category attack but does not help the ambiguity attack and file attack.

Features of the Visimark 1_0:

1. Supports raw video as input.
2. Covers 30+ attacks with the novelty of the nine video category attacks.
3. GUI Based tool.
4. Supports text and graphical report based on MSE, PSNR, DELTA, and MSAD.

IV. Contribution of Visimark 2_0

Visimark 2_0 is the next version Visimark 1_0 which includes many new things in addition to Visimark 1_0. Some new features like supporting compressed video formats like MPEG-4. The provision of having an extraction algorithm for the research community is the most novel feature. Once the extraction algorithm is selected, and upon submitting the original watermarked, the tool extract watermark from all the attacked watermarked video. It stores the entire recovered watermark into a separate folder and designs a graph of NC values & SSIM values of each recovered watermark and input watermark. NC values and SSIM values graph is further used by the research community for their experimental results and discussion. In Visimark 2.0, naive additions like applying all attacks mentioned above in the transform domain along with the spatial domain. As a contribution, an ambiguity attack added to Visimark 2_0 where one more different watermark embedded into a watermarked video. Frame dropping attack also implemented with a new concept.

Visimark2_0 is a generic GUI based tool developed for the evaluation of compressed and uncompressed domain video watermarking schemes. The goal of this deliverable is to provide an architecture that will be used by two main kinds of users. User A: who want to use this platform as a tool to obtain attacked videos and test the perceptual visibility of watermarking algorithms, and User B: who want to check the perceptual visibility as well as the robustness of their watermarking scheme. The architecture is composed of 3 main parts, as shown in Figure 2.

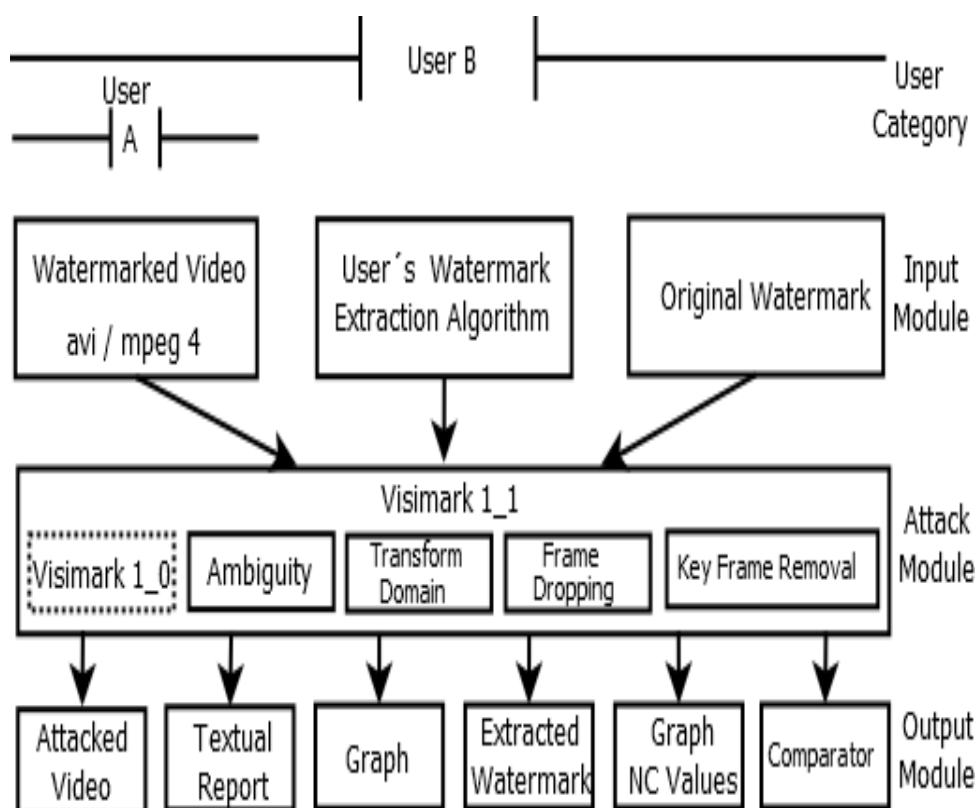


Fig. 2 Visimark 2_0 Architecture

Input Module includes the first part of the Visimark2_0. Here User A, provides a watermarked video in either a raw or compressed video format. User B submits extraction algorithm and the original watermark embedded in the video along with watermarked video.

Attack Module is used to process the input by applying a variety of attacks discussed in Visimark 1_0 [13] as well as seven new attacks introduced in the proposed tool presented in further sub-section.

Output Module contains output in the form of attacked watermark videos, reports, metric evaluation, extracted watermark and a comparator. This module is further classified into following five sub-modules.

3-1: Attacked Watermark Video Module, where the output is the set of attacked videos after applying various attacks by the attack module.

3-2: Report writer is the module where all results are written in text file. This report file contains the table holding the names of

attack applied based on the parameter values as tabulated in the table 3. A decision report is also containing the name of attack and its average NC value. This is the novel contribution is useful to test the robustness of the supplied algorithm by User B.

3-3: Metric Evaluation Module is the process-dependent module, where metrics concerning visual quality and robustness are generated and put forth in the graphical form.

3-4: Extractor Module will apply the watermark extraction algorithm provided by user B on all the attacked videos and store extracted watermarks.

3-5: Comparator Module facilitates the frame by frame comparison between two supplied videos.

Features of the Visimark 2_0:

1. Supports compressed video like mp4 format.

2. Covers 30+ attacks from Visimark and four new categories of attacks like the attack in the transform domain, ambiguity attack, key-frame removal attack, improved frame dropping attack etc.
3. GUI Based Tool, which adds simplicity for the use.
4. Provision of inclusion of the User's Extraction Algorithm for extracting the watermark from all the watermarked video with some restriction.
5. Supports text and graphical report based on MSE, PSNR, DELTA, MSAD, SSIM and NC.

Attacks Supported

The proposed version of Visimark supports more than 40 attacks categorized as below.

1. Spatial domain attacks

Noise addition, rotation, translation, scaling, blurring, sharpening, denoising, motion blurring, chroma sampling, fade and dissolve, contrast stretching, up/down sampling, dithering, pixel removal, compression, affine, filtering, ambiguity, and transformed domain attack.

2. Temporal Domain Attack

Frame dropping, frame swapping, frame copy, frame replacement, frame averaging, collusion, scene swapping, key-

frame dropping, scene dropping, and temporal synchronization.

3. Spatio-Temporal Domain Attack

All spatial domain attacks that are applied to the key-frames of the video sequence fall into this category.

Explanation of the newly added attacks:

1. Ambiguity attack: In this category, the attacker may embed a different fake watermark into the watermarked video. DWT-based watermarking used to embed the fake watermark, leading to confusion on the detection side—an algorithm for watermark embedding used from [14].

2. Attacks in Transformed domain:

Video is decomposed in frames and then transformed into 2D DWT (Discrete Wavelet Transform) domain. All the attacks except video category attacks applied on HL & LH sub-bands. After attacking, modified HL and LH sub-bands composed with LL and HH sub-band for inverse DWT.

3. Key-frame removal attack:

Here, the key-frame is detected first using key-frame detection algorithm explored in Algorithm 1. All these key-frames simply dropped—the same algorithm from [13] used for key-frame detection.

Algorithm 1 To extract key-frames from video

Input: Video V i. e. . avi file from user. V is represented as below.

$$V = \{F_1, F_2, F_3, \dots, F_l\}$$

Where, $F_1, F_2, F_3, \dots, F_l$ are the frames of video V and is represented as follows.

$$F_i = \begin{bmatrix} f_{1,1} & \cdots & f_{1,n} \\ \vdots & \ddots & \vdots \\ f_{m,1} & \cdots & f_{m,n} \end{bmatrix} \text{ where, } f_{1,1} \text{ to } f_{m,n} \text{ represents intensity of Pixel}$$

Where, $[m, n]$ represents the size of frame F_i and $1 \leq i \leq l$, here l is no. of frames

```

    T : Threshold           // Value is decided after empirical analysis
Output: SceneCount       // Number of scene changes found
           Key_Frames(.) // First frame number of all the scenes
Procedure:
    Step 1. Initialize,
           Set, i ← 1
           SceneCount ← 1
           Key_Frames(1) ← 1
           RefFrame ← F1           // Assign First Frame as Reference Frame

    Step 2. for i ← 2 to l           // for all frames
           1. Fi ← READ_FRAME(i)
           2. Convert Fi and RefFrame from RGB to Gray
              Fi ← RGB2GRAY(Fi)
              RefFrame ← RGB2GRAY(RefFrame)
           3. Find edges of RefFrame and Fi using Canny Filter
              eRefFrame ← EDGE(RefFrame, 'Canny')
              eFi ← EDGE(Fi, 'Canny')
           4. Perform block processing: Computing average intensity
              AvgIntensity_eFi ← AVERAGE_INTENSITY(eFi)
              AvgIntensity_eRefFrame ←
              AVERAGE_INTENSITY(eRefFrame)
           5. Compute Edge Difference by
              EdgeDiff ← AvgIntensity_eRefFrame –
              AvgIntensity_eFi
           6. Compute absolute sum of EdgeDiff
              Result ← |∑ EdgeDiff|
           7. if Result > Threshold (T) then           // Scene cut detected
              SceneCount ← SceneCount + 1
              Key_Frames(SceneCount) ← i
              RefFrame ← Fi
              i ← i + 1
              Go to Step 2.

    Step 3. Stop

```

4. Improved Frame Dropping Attack: In Visimark 1_0, frame dropping attack implemented using frame drop ration (FR). For FR = 3, will drop every frame of multiple of 3 from the watermarked video

leads to the limitation of optimizing the value of FR. So, in Visimark 2_0, some improvement to this attack is implemented in Algorithm 2 as follows.

Algorithm 2 Improved Frame Dropping Attack

Input: V_i, N // V_i is Input video sequence, N is number of frames
 FR // Frame dropping Ratio

Output: V_o // V_o is the output video sequence without key frames
 nN // nN is the new value of number frames

Procedure:

Step 1. Read FR from the user.

Step 2. If $FR \geq 1$ and $FR \leq 100$

Step 3. Compute the number of frames to be dropped using as:

$$T \leftarrow \text{round} \left(\frac{FR * 100}{N} \right)$$

Step 4. $nN \leftarrow N - T$ // New value of Number of frames

Step 5. Randomly generate frame number to be dropped using formula:
 $In \leftarrow \text{random}(1, N)$

Step 6. For $i:=1$ to In
 $V_o(i) \leftarrow \text{Drop_Frame}(i)$

Step 7. End for.

Step 8. End if

Step 9. Stop

5. Provision of inclusion of the user's extraction algorithm: Visimark 2_0 adds the novel feature to include the user's extraction algorithm. Here, a user has to submit the original video, extraction algorithm along the original watermark. Currently, this version supports the code of the extraction algorithm in MatLab only.

After inclusion of the Watermark Extraction algorithm, Visimark 2_0 will automatically do the following things:

1. Extract the watermark from all the attacked watermark videos.
2. Compute NC values for each extracted watermark.
3. Plotted and saved the graph of NC Values in NC folder of the graph.

Due to this feature, the watermark research community will save a lot of time needed for robustness testing.

V. Experimental Results:

In this paper, different proposed attack algorithms tested for Visimark 2_0 have been implemented in Matlab. For User A, the input to Visimark2_0 is a watermarked video in MP4/AVI format. We have tested our attack algorithms with several watermarked AVI available in matlab & MP4 videos as given in Table 3.

Table 4 provides an overview of attack results along with its permissible range. The permissible range values are devised after experimentation and some of them, from different standard benchmarking tools.

Table 3 List of watermarked video sequences used for test of fidelity and robustness by Visimark2_0

SN	Name of Video	Total No. of frames	Frame Rate (fps)	Frame size	Duration (secs)
1	wScenevideoclip.avi	92	15	160 x 120	6
2	wTraffic.avi	120	15	160 x 120	8
3	wVipcolorsegmentation.avi	75	15	160 x 120	5
4	wVipsnowydays.avi	40	8	320 x 240	5
5	wVipwarnsigns.avi	270	30	360 x 180	9
6	wRhinos.avi	144	15	320 x 240	7
7	wAnimatedcat.mp4	150	30	640 x 360	5
8	wMyfamily.mp4	8	15	256 x 256	1
9	wJeet.mp4	100	30	320 x 240	4

Table 4 Attacks with Permissible Min- Max Values

Attacks And Evaluated Parameters	Min	Max
Frame Attacks:		
Frame Averaging	3	10
Frame dropping (%)	0	99
Frame swapping	2	10
Frame copy or addition	1	5
Frame replacement	1	5
Changing the sequence of video	2	10
Scene dropping	1	1
Changing frame rate of the video [17]	16	60
Chroma sampling attack [18]	4:4:4	4:2:0
Fade and dissolve attack	20	100
Inter-frame filtering	3	3
Ambiguity Attack	1	4
Geometric Attacks:		
Scale [9], [10]	0.5	2
Crop [8]-[11]	1/0	100/100
Rotation	-90	90
Contrast Stretching [9], [10]	0	25
Rotation scale [9], [10]	-2	2
Rotation Crop [9], [10]	-2	2

Rotation/scaling/cropping	-2	2
Shear [11]	0	100
Blurring	4	20
Row/column Removal [9], [10]	10	100
Up/down sampling	0.1	2
Signal Processing Attacks:		
Noise [9], [10]	0	15
Filtering [9], [10]	3	9
Compression Attack [9]-[11]	20	100
Key frame Dropping Attack	None	All
Ambiguity Attack	1	4

The results of the all the three video categories of attacks i.e. spatial, temporal, and spatio-temporal discussed in previous section, considering the above permissible ranges, are presented here for the watermarked video 'wMyfamily.mp4' shown in figure 3 (a) with original watermark in figure 3 (b).



Fig. 3 a) Original Watermarked Video Frame (I-frame) (wMyfamily.mp4) and b) original watermark

The researcher can use their algorithm to embed a watermark in a video—watermarked video supplies as an input to VisiMark2_0 in mp4 format. VisiMark2_0 also prepares five folders to store the results for researchers' future use as the previous version.

a) Attacked Video Folder: All the videos generated by VisiMark 2 after applying some attacks are stored in this folder. The researchers has the facility to access these attacked videos as and when needed. Figure 11 depicts the sample snapshot.

b) Graph Folder: Various graphs based on MSE, PSNR, MSAD, DELTA and SSIM stored in this folder. Some of the charts illustrated in figure 5 and figure 6.

c) Attacks Report Folder: This folder consists of the report of the attack in a text file generated by VisiMark 2_0. The researchers can any time use these report files as it will be saved permanently for the future references.

d) Comparison Folder: Here, the evaluation of the input and the output videos along with listed values is stored. All these

comparisons are saved permanently for the future references.

5.1 Spatial Domain Attacks: The figure 4 shows the results on the I-frame of input video after the application of spatial domain attacks already listed in previous section.

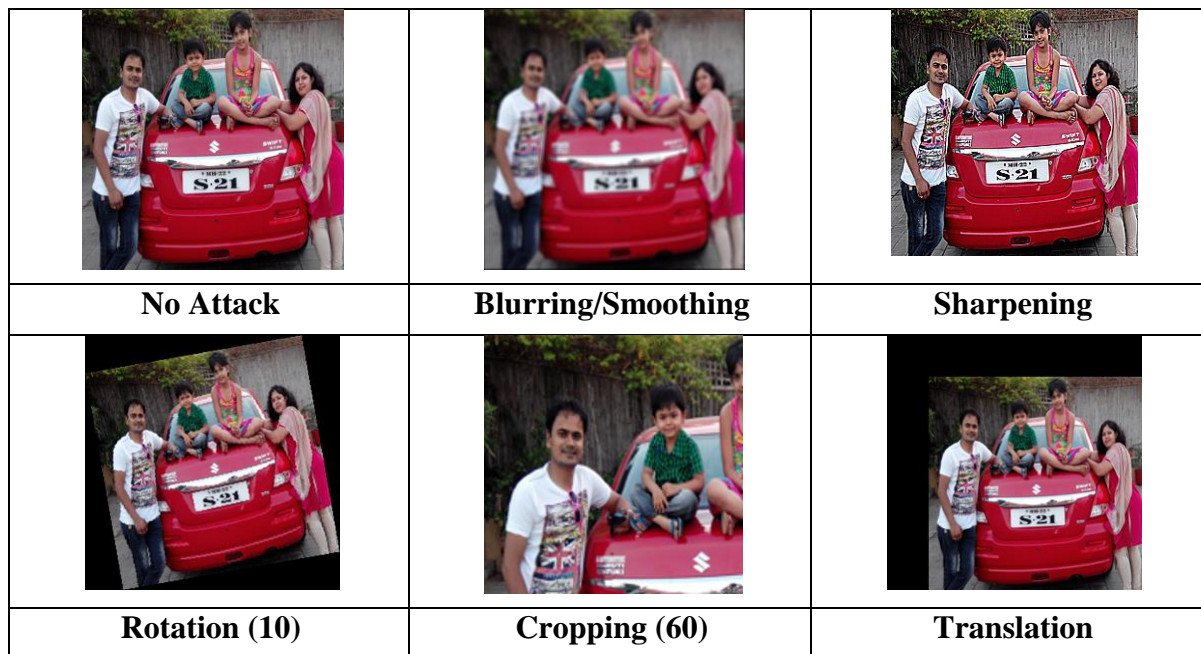
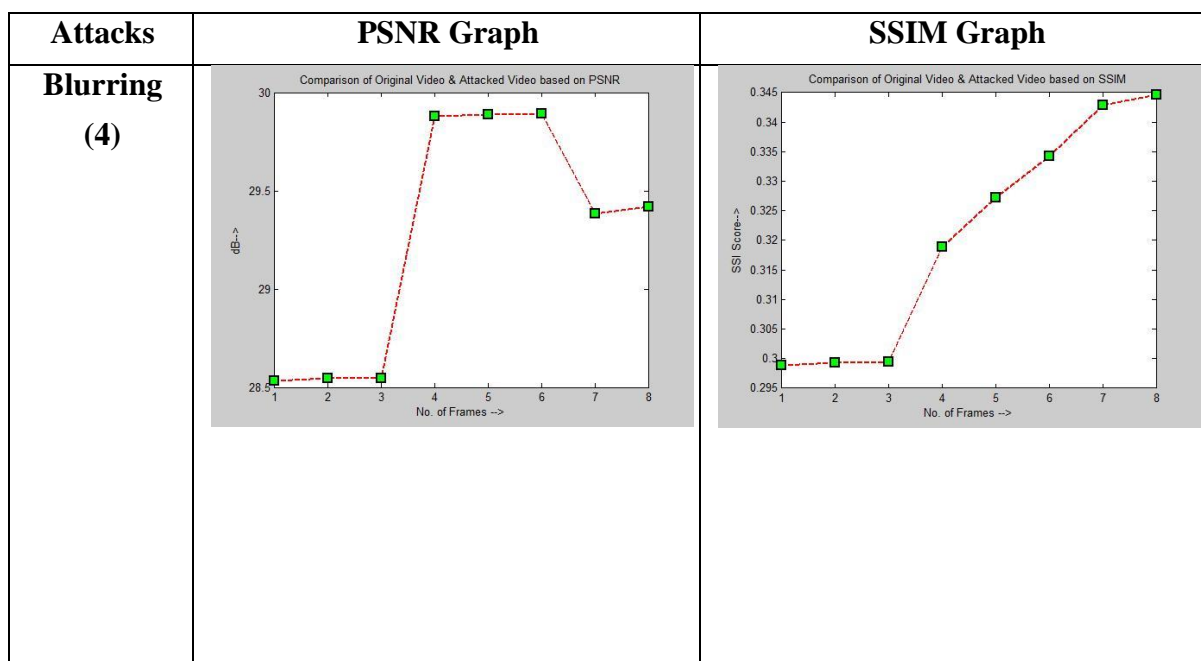


Fig. 4 The attacked watermark video frames for spatial domain attacks

The graphs of PSNR and SSIM attacked video frames are depicted in figure 5.

This comparison states, how far the perceptual visibility and video quality of the original watermarked frame is maintained.



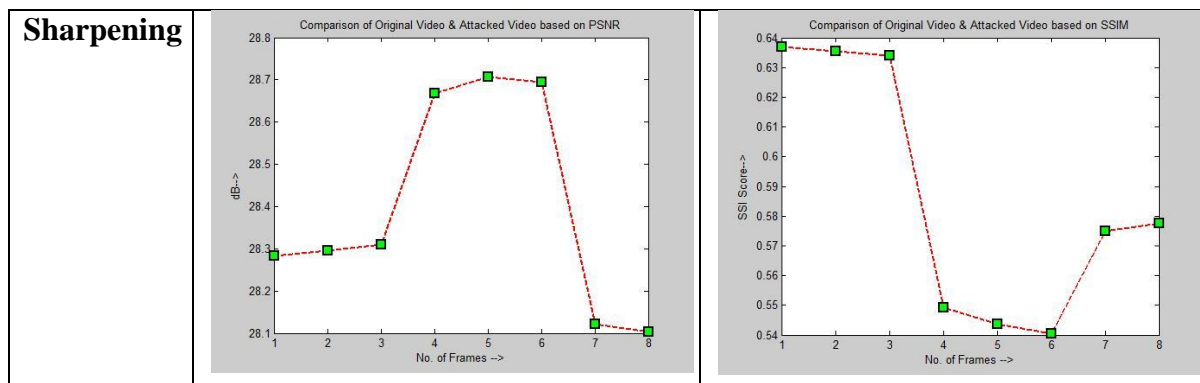
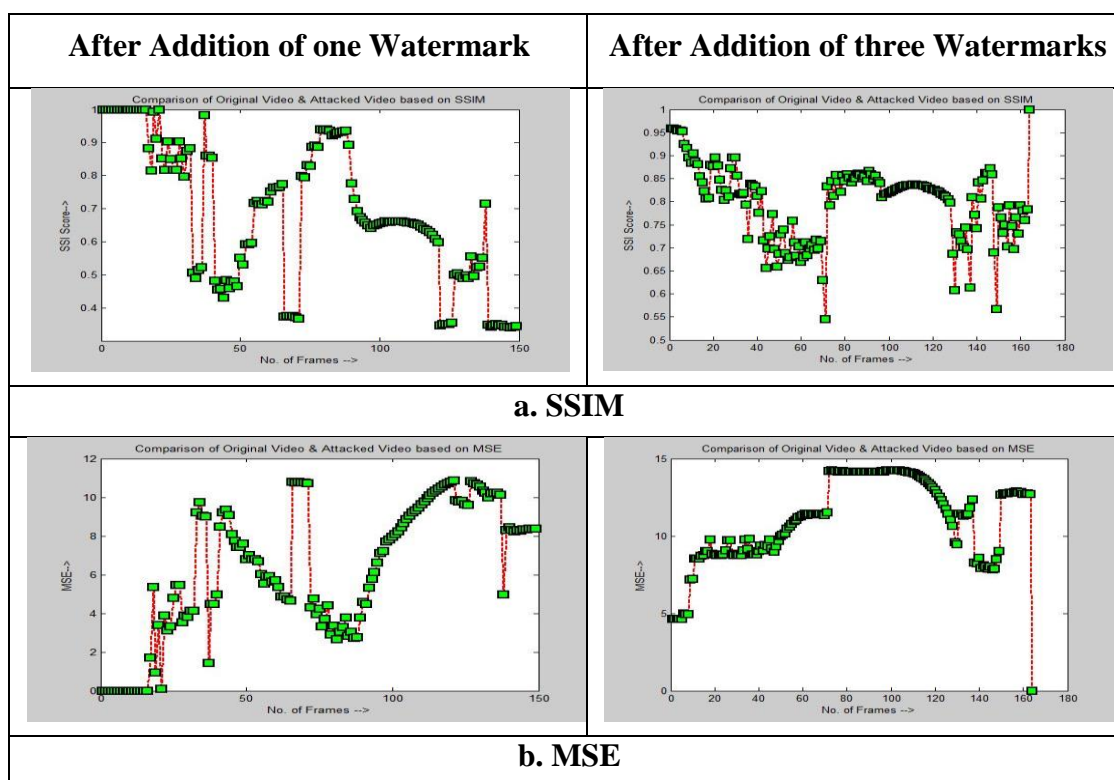


Fig. 5 Fidelity based comparison of input watermarked video with attacked watermark video after applying the attacks

5.2 Ambiguity attack: We compute the different performance metrics such as SSIM, MSAD, MSE and PSNR observe that the perceptual visibility after addition of one watermark is better than the one after the addition of the three watermarks as presented using

four metrics shown in figure 6 (a–d). For this demonstration we have used wAnimatedcat.mp4 file as an input watermarked video file. The perceptual visibility for different attacks like rotation by 45° and Blurring by 14% is computed and presented in figure 10.



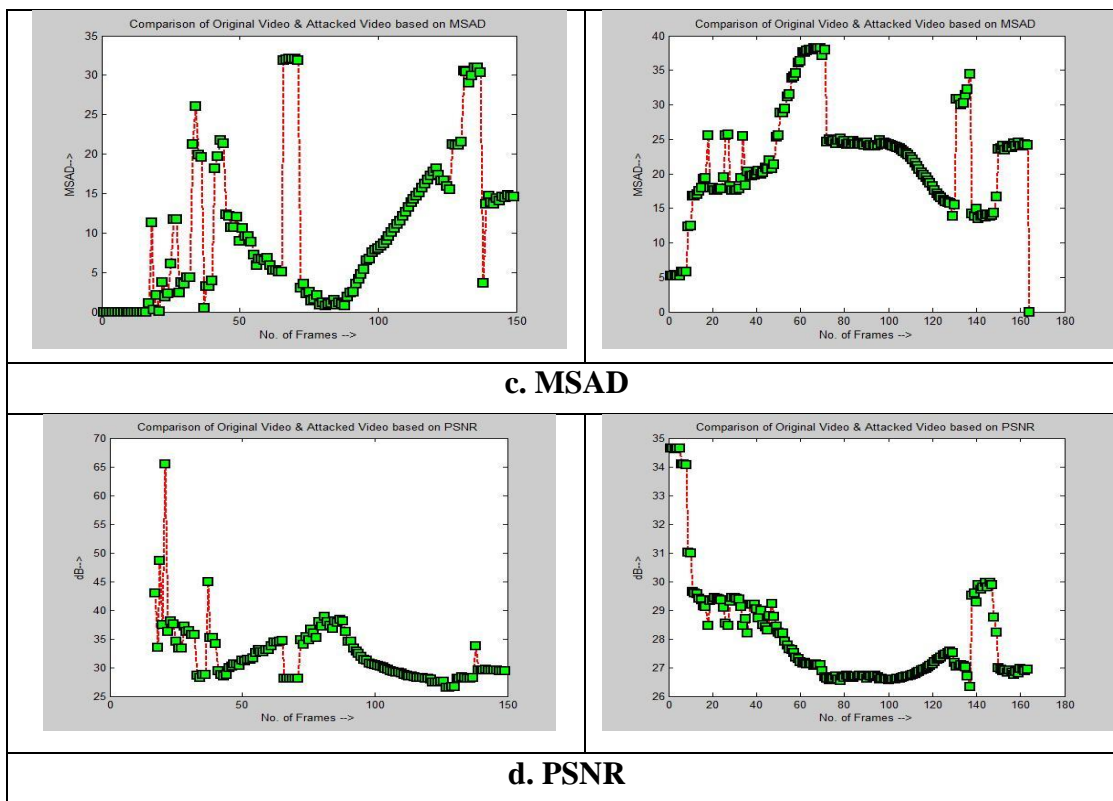


Fig. 6(a-d) Plot of PSNR, MSE, MSAD and SSIM for Ambiguity attack

5.3 Transformed Domain Attack: After applying this attack on the watermarked video, we obtain the several attacked watermark video frames some of which are discussed with the metrics MSAD and PSNR.

Attacks	MSAD	PSNR
Rotation by 45°		

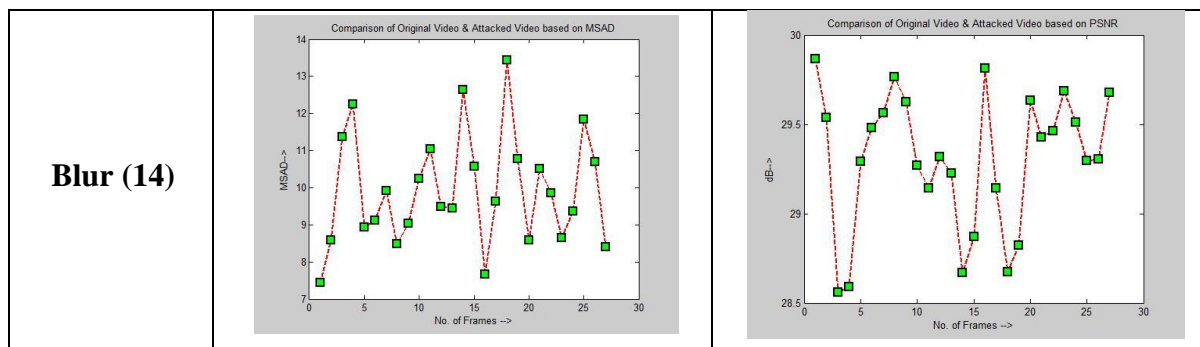


Fig. 7 Plot of MSAD & PSNR for Transformed Domain Attacks using Rotation and Blurring Attack.

5.4 Temporal Domain Attacks:

In this category of attacks, video frames are attacked based on their temporal sequence. Figure 8 shows the demonstration of results after applications of temporal domain attacks such as frame averaging and change of frame rate.

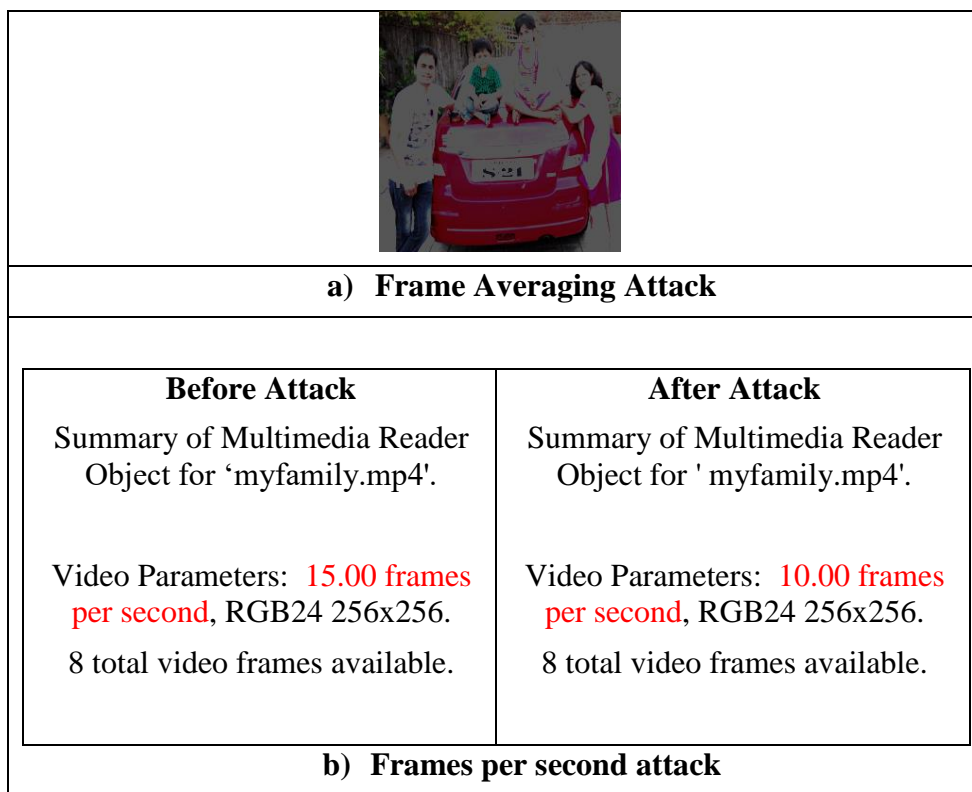


Fig. 8 Temporal domain attacks

Figure 9 shows the comparison of the watermarked video and attacked video after frame averaging and scene swapping attack.

Attack	PSNR	SSIM
---------------	-------------	-------------

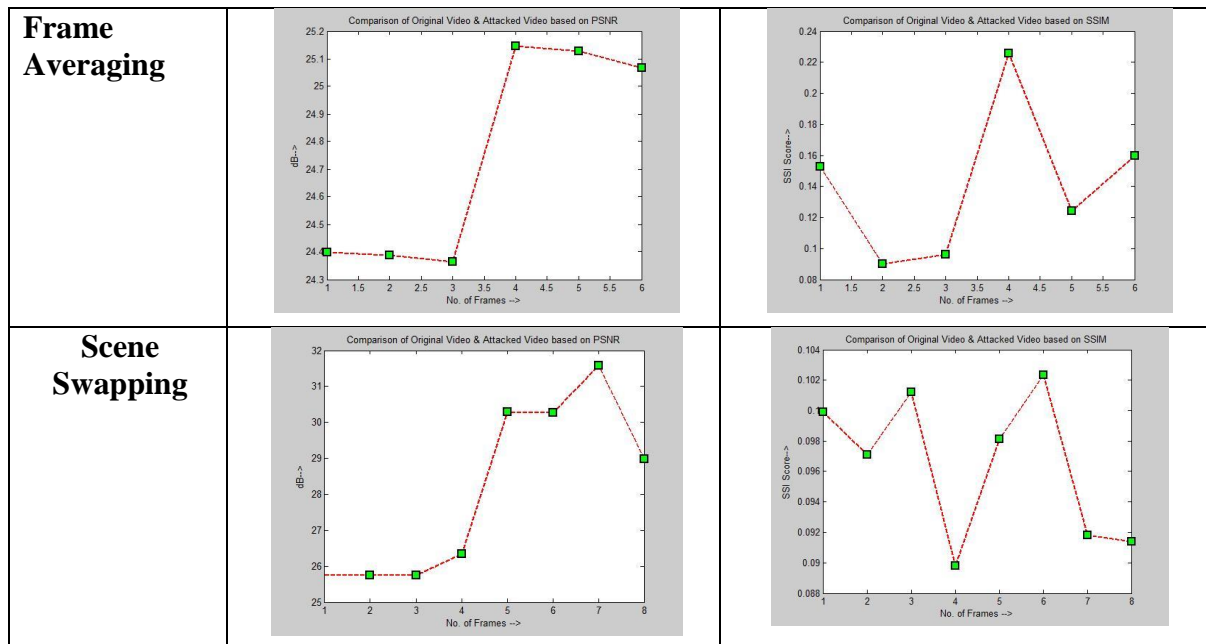


Fig. 9 Fidelity based comparison on PSNR and SSIM for input watermarked video with attacked watermark video after applying the temporal domain attacks.

5.5 Spatio-Temporal Attacks:

In spatio-temporal attacks, initially key-frame are extracted and all the spatial domain category attacks are applied to extracted key-frames. Figure 10 shows the graph of PSNR and SSIM of some attacks.

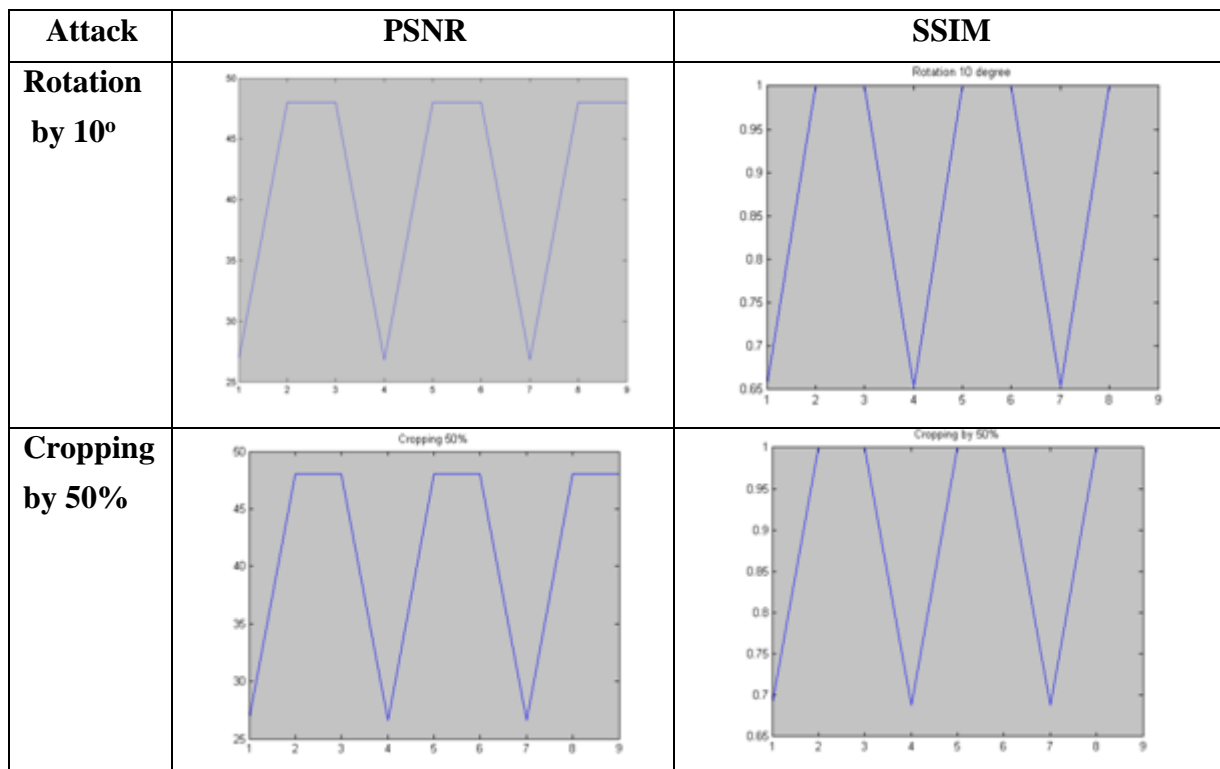
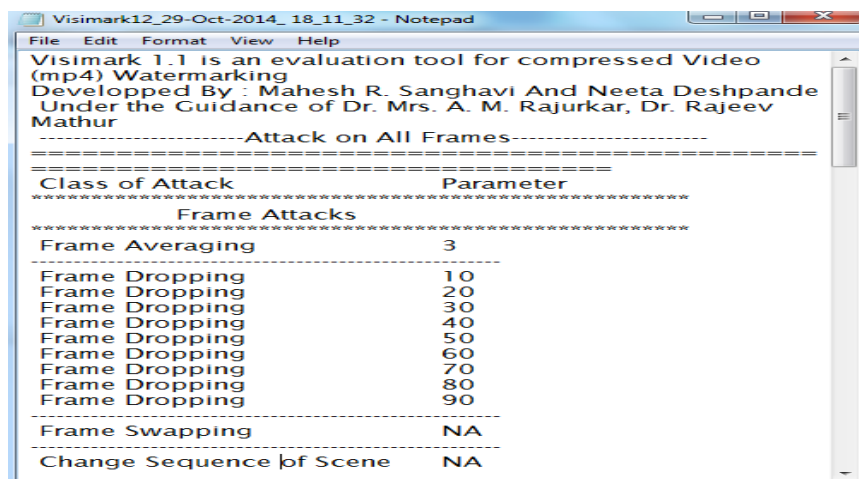


Fig. 10 Comparison of fidelity based on PSNR and SSIM for spatio-temporal attacks

5.6 Attack Report

Figure 11 shows the snapshot of the attack report generated after the addition of extended features like ambiguity attack and improved frame dropping attack.



```

Visimark12_29-Oct-2014_18_11_32 - Notepad
File Edit Format View Help
Visimark 1.1 is an evaluation tool for compressed Video
(mp4) Watermarking
Developed By : Mahesh R. Sanghavi And Neeta Deshpande
Under the Guidance of Dr. Mrs. A. M. Rajurkar, Dr. Rajeev
Mathur
-----Attack on All Frames-----
=====
Class of Attack          Parameter
-----
***** Frame Attacks *****
-----
Frame Averaging          3
-----
Frame Dropping           10
Frame Dropping           20
Frame Dropping           30
Frame Dropping           40
Frame Dropping           50
Frame Dropping           60
Frame Dropping           70
Frame Dropping           80
Frame Dropping           90
-----
Frame Swapping           NA
-----
Change Sequence of Scene NA

```

Fig. 11 Snapshot of text report after applying attacks.

Figure 12 shows the frame by frame comparison between two supplied videos i.e. the watermarked video frame and attacked watermark video frame after blurring attack.



Fig. 12 Comparison of two frames on the basis of PSNR, MSE, MSAD, Delta and SSIM for Blurring Attack

5.7 NC Values after watermark extraction by user's algorithm:

Usually higher values of NC indicates that the watermark is successfully extracted from the attacked watermark video. To test the robustness based on NC value Visimark2_0 needs the watermark extraction algorithm and original watermark. Here, for testing purpose the extraction algorithm used is, the video

watermarking scheme based on DWT-SVD is implemented and tested using this tool.

After applying this extraction algorithm, the watermark recovered from the different attacked video is shown in figure 13. This indicates that the scheme is robust to the attacks like salt and pepper noise, speckle noise, affine, average filtering, blurring, contrast stretching, cropping.

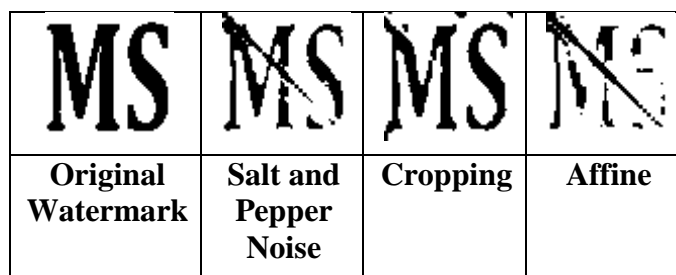


Fig. 13 The recovered watermark after applying various attacks.

From the textual report presented in the figure 14, average NC value after applying the frame averaging attack on the input watermarked video is 0.87 which indicates that the supplied extraction algorithm is robust to frame averaging attack.

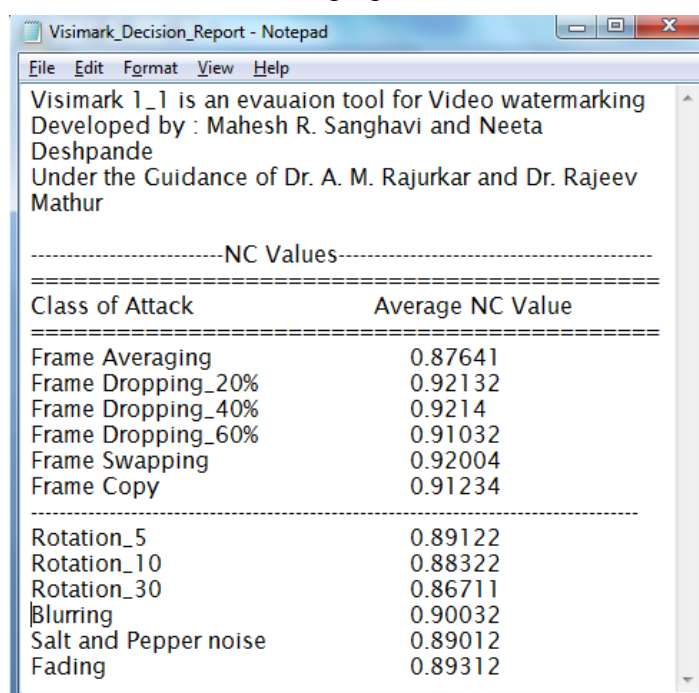
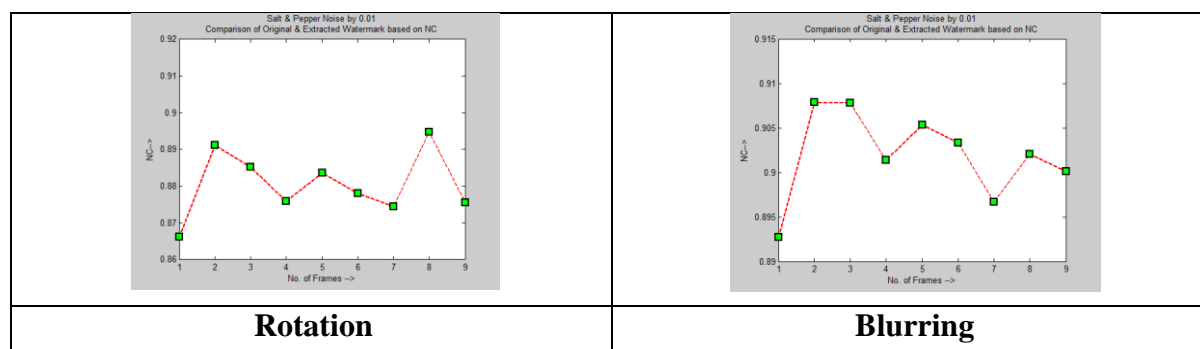


Fig. 14 Snapshot of average NC values

The same applies for frame dropping, frame swapping, frame copying, and rotation attacks and so on. Figure 15 depicts the graphical representation of the comparison between the attacked watermark video and input watermarked video.



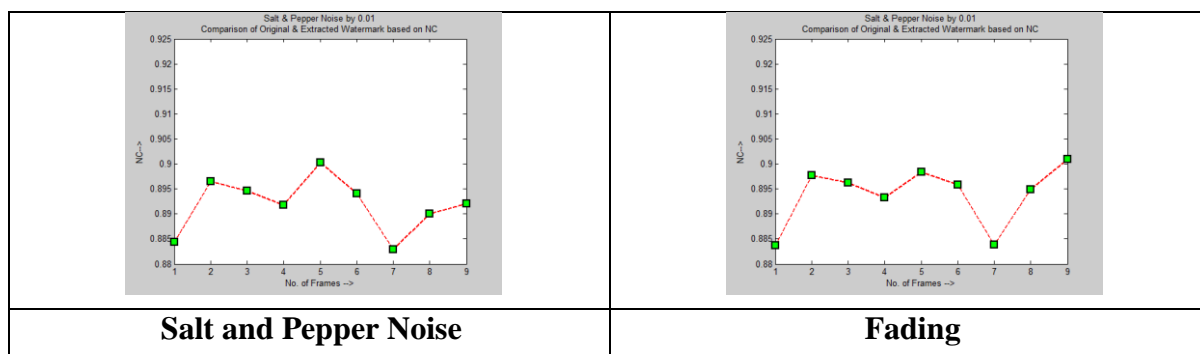


Fig. 15 Robustness test based on NC values between input watermarked video with attacked watermark video after applying attacks

5.8 Decision report

Figure 16 shows the decision report prepared by Visimark2_0 for the watermarking scheme used for testing the robustness. It indicates the robustness of the scheme to frame averaging, frame dropping, frame swapping, frame copying, rotation attacks and so on with their permissible threshold.

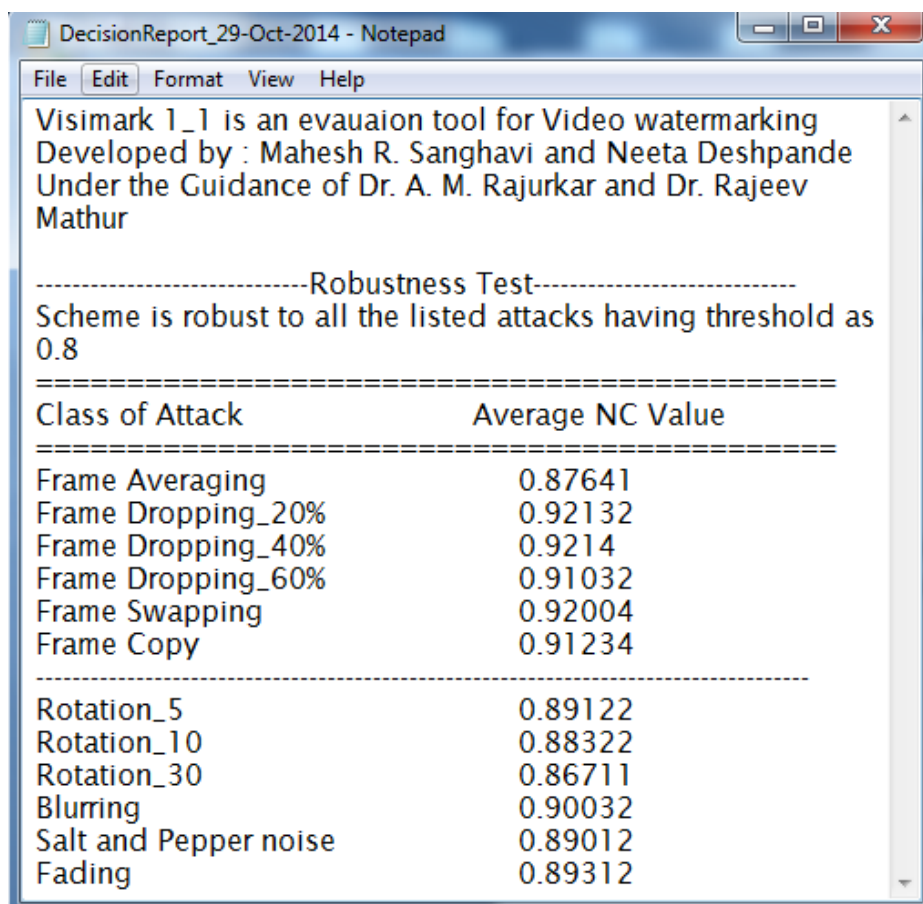


Fig. 16 Snapshot of decision report

Table 5 shows the assessment of the offered Visimark2_0 regarding attacks elaborated in Table 4.

Table 5 Assessment of various Tools with Offered Visimark 2_0

Parameters/ Tools	Stirmar k (Audio & Image)	Ch eck ma rk	Opti mark	Matma rk	Open Water mark	Mesh Bench mark	Visima rk 1_0	Proposed Visimark 2_0
Developed in Language	C++	Mat lab	C++	C++	Java	C++	Matlab	Matlab
Media	Image & Audio	Ima ge	Imag e	Audio	Image	Image	Image / Video (avi)	Image / Video (avi & mp4)
Signal Processing Attacks & Watermark Disabling Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Watermark Removal Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ambiguity Attack	No	No	Yes	No	No	No	No	Yes
Video Attacks	No	No	No	No	No	No	Yes	Yes

Table 6 shows the major comparison of Visimark 1_0 and Proposed Visimark 2_0. By observing table values it is clear that Visimark 2_0, added various new category of attacks such as Attacks in Transform Domain, Ambiguity Attacks, Improved Frame Dropping Attacks, Key frame dropping attack. Also in Visimark 2_0 various new features such as improved

Graphical User Interface (GUI), additional comparison on SSIM and NC based values, provision of providing users watermark extraction algorithm and original watermark for Extraction of Watermark and it's ready to go comparisons. Visimark 2_0 reduces huge work of the research community of the digital video watermarking.

Table 6 Comparison of Visimark 1_0 and Proposed Visimark 2_0

Attacks and Evaluation Parameters	Visimark1_0	Proposed Visimark 2_0
Frame based Attacks (Averaging, Dropping, Swapping)	Yes	Yes
Scene Change Attack	Yes	Yes
Frame rate variation attack	Yes	Yes
Image Processing Attacks (Chroma Sampling, Fade & Dissolve, Motion Blurring, Inter-frame Filtering)	Yes	Yes

Attack on Transformed Domain (Scale, Crop, Rotation, Dithering, Contrast Stretching, Rotation Scale, Rotation Crop, Aspect Ratio, Shear, Linear, Affine, Blur, Bending, Warping, Projective, Collage, Noise, Filtering etc.)	No	Yes
Key frame Dropping Attack	No	Yes
Ambiguity Attack	No	Yes
Evaluated parameters	PSNR , MSAD MSE ,DELTA	PSNR , MSAD MSE ,DELTA, NC, SSIM
Provision of Inclusion of the Extraction Algorithm	No	Yes
GUI	Yes	Yes
Supported File Format	Avi	Avi, Mp4

VI. Conclusion:

Visimark 2_0 is the next version of the Visimark 1_0 with significant improvements and contributions. Unlike Visimark 1_0, Visimark 2_0 supports both the compressed video file formats like mp4 and uncompressed video file formats like avi file. Many new attacks added in Visimark 2_0, such as ambiguity, dropping key-frames, improved frame dropping and the transformed domain attacks are successfully implemented. Provision of the user's extraction algorithm is the crucial contribution of this work, which extract the embedded watermark and compare this with original watermark based on the NC values. The addition of two new graphs like NC & SSIM values in the respective folders shows some more extension to an earlier version. In the next version of the Visimark tool, the provision of selected attacks on the video will be proposed, which will help the research community for the specific attacks. Like Visimark 1_0, Visimark 2_0 will also significantly reduce the time needed for the test of robustness.

Acknowledgements:

We wish to place our earnest thankfulness to the owners of Checkmark [10] and Stirmark [8] to keep open this tool for the research communal. Checkmark and

Stirmark are the pioneer tools available for the research community to evaluate the watermarking algorithm. Revised guidelines from the files in afore-mentioned tools to encompass watermarking attacks. Also special thanks to Dr. Neeta Deshpande, Dr. Archana Rajurkar and Dr. R. R. Manthkar for contributing with me in version 1 of Visimark [13].

References:

- [1] Tanfeng Sun, Xinghao Jiang, Shusen Shi, Zhigao Lin, Guanglei Fu, "A Novel Self-adaptation Differential Energy video watermarking scheme in copyright protection", *Journal Of Multimedia*, Vol. 4, NO. 3, JUNE 2009.
- [2] Pat-pik wah chan, Micheal r Lyu, roland T chin, "Copyright protection on the web: a hybrid digital video watermarking scheme", *Proceedings of the 13th international World Wide Web conference* pp. 354 – 355, ISBN:1-58113-912-8, 2004.
- [4] Chetan K.R, Raghavendra K., "DWT based blind watermarking scheme for video authentication", *International Journal Of Computer Applications*, Vol. 4, No.10, pp. 19-26, ISSN-0975-8887, August, 2010.

- [5] J. Bloom, I. Cox, T. Kalker, J.-P. Linnartz, M. Miller, and C. Traw, "Copy Protection for DVD Video", in *Proceedings of the IEEE*, Vol. 87, No. 7, ISSN: 1267-1276, 1999.
- [6] Maurice Maes Ton Kalker, Jean-paul Linnartz, Joop Talstra, Geert Depovere, Jaap Haitzma, "Digital Watermarking for DVD Video Copy Protection: What Issues lay a Role in Designing an Effective System", *IEEE Signal Processing Magazine*, PISSN 1053-5888, eISSN 1558-0792, 2000.
- [7] Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le, "Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools", *2010 Second International Conferences on Advances in Multimedia*, pp. 67-73, ISBN 978-0-7695-4068-9/10, 2010.
- [8] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. "Attacks on copyright marking systems", In *David Aucsmith, editor, second workshop on information hiding*, Vol. 1525, pp. 218-238, Lecture notes in computer science, ISBN 3-540-65386-4, Portland, Oregon, U.S.A., 14-17 April, 1998.
- [9] Fabien A. P. Petitcolas, "Watermarking schemes evaluation", *IEEE Signal Processing*, Vol. 17, No. 5, pp. 58-64, PISSN 1053-5888 eISSN 1558-0792, September 2000.
- [10] Shelby Pereira, Sviatoslav Voloshynovskiy, Maribel Madueño, Stéphane Marchand-Maillet and Thierry Pun, "Second generation benchmarking and application oriented evaluation", In *Information Hiding Workshop III, Pittsburgh, PA, USA*, April 2001.
- [11] V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, I. Pitas, "A benchmarking protocol for watermarking methods", *2001 IEEE Int. Conf. on Image Processing (ICIP'01), Thessaloniki, Greece*, pp. 1023-1026, 7-10 October, 2001
- [12] URL: <http://www.tele.ucl.ac.be/view-project.php?language=En&name=OPENWATERMARK>, 4/11/2010
- [13] Neeta Deshpande, Mahesh Sanghavi, Archana Rajurkar, R. Manthalkar, "VisiMark 1_0 : An Assistant Tool for Evaluating robustness of Video", *International Journal of Information Technology & Computer Sciences by MECS Press*, Vol. No. 5, pp. 10-21, April, 2013.

Author's Profile:

Ms Kainjan Sanghavi: Ms Kainjan Sanghavi has completed his BE from University of Pune, Ph.D and ME from SRTM University, Nanded. She is working as an Associate Professor in SNJB's KBJ College of Engineering Chandwad. Her research interest includes image processing and internet of things.

Dr. Mahesh Sanghavi: Mr Mahesh Sanghavi has completed his BE from University of Pune, ME from SRTM University and PhD from JNU, Jodhpur & working as an Professor in SNJB's KBJ College of Engineering Chandwad. His research interest includes image processing and information security.

Dr. Neeta Deshpande: Dr. Neeta Deshpande has completed her BE from University of Pune, ME from University of Pune and PhD from SRTMU, Nanded. She is working as a Professor in RH Sapat College of Engineering, Nashik. Her research interest includes image processing, video processing etc.