ISSN 1213-6972 Journal of WSCG http://www.wscg.eu Vol.28, No.1-2, 2020

Regions Based Semi-fragile Watermarking Scheme for Video Authentication

Amal Hammami
Research Groups in Intelligent Machines
University of Sfax
National Engineering School of Sfax
Sfax, 3038, Tunisia
amal.hammami@enis.tn

Amal Ben Hamida
Research Groups in Intelligent Machines
University of Sfax
National Engineering School of Sfax
Sfax, 3038, Tunisia
amal.benhamida@enis.tn

Chokri Ben Amar
Research Groups in Intelligent Machines
University of Sfax
National Engineering School of Sfax
Sfax, 3038, Tunisia
chokri.benamar@ieee.org

Henri Nicolas
Bordeaux Computer Science Research Laboratory
University of Bordeaux 1
Talence, 33405, France
henri.nicolas@u-bordeaux.fr

ABSTRACT

In this paper, we propose a new semi-fragile watermarking scheme in the frequency domain for surveillance videos authentication. Our system starts operating by generating a binary watermark based on a novel watermark construction process. This latter combines Speeded Up Robust Features (SURF) and Maximally Stable Extremal Regions (MSER) detectors to extract frames relevant features that can resist common attacks while being fragile to intentional manipulations. Furthermore, the watermark security is improved using torus automorphism mapping. For the embedding process, Regions of Interest (ROI) are detected and then used as watermark holders. These regions are decomposed into different frequency sub-bands using Singular Value Decomposition (SVD) as well as Discrete Wavelet Transform (DWT). Then, the watermark is embedded in selected bands following an additive method. A blind detection is conducted to extract the hidden signature from the watermarked video. Evaluation results show that the proposed scheme is suitable for authentication purpose since it efficiently discriminates malicious manipulations from non-malicious ones. Besides, it preserves a high level of perceptual quality.

Keywords

Video authentication, semi-fragile watermarking, discrete wavelet transform, singular value decomposition.

1. INTRODUCTION

Recently, the ever-evolving multimedia technology and communication makes surveillance system installation further flexible as well as more cost effective. Accordingly, video surveillance cameras are broadly used for security purposes by recording daily activities in several places such as airports, hospitals and train stations [Kha15, Abe14, Ben14].

However, the progress in digital technologies field leads also to the development of powerful video processing tools that facilitate the recorded videos content illegal modification by fraud person. As a result, content-authentication becomes an increasingly important requirement for video security protecting especially in surveillance context where video can be involved as a legal proof in forensic investigations.

Video watermarking has emerged as an appropriate technique to tackle this issue. Fundamentally, this authentication approach consists in embedding a secret information, which is referred as a watermark in the host video [Bpa14, Jos17, Mko12]. When needed, the embedded information is extracted from the watermarked video to check whether it has been tampered or not, thereby to verify its content integrity and authenticity. An efficient watermarking technique should provide a trade-off between several

requirements mainly robustness, imperceptibility and capacity [Aga19, Mch14].

In literature, several video watermarking schemes are proposed. Depending on the watermark selection holders, these video watermarking approaches are dived into two categories. The first one is frame by frame watermarking where the authentication signature is hidden in all regions in each video frame. Conversely, in the schemes dedicated for the second class only regions of interest (ROI) are watermarked. These ROI are identified based on specific criteria in such way to ensure that their modification will lead to a detectable change. ROI based techniques are recognized as very compression resilient approaches that provide a high level of imperceptibility [Ker17]. Moreover, watermarking schemes can be classified into two sets according to the insertion domain. The first category represents the spatial domain techniques in which the watermark embedding is performed by directly modifying frame pixels values. These techniques exhibit a low complexity while preserving a poor robustness [Ara19]. The second type is the frequency domain based techniques. In this case, the video frame is firstly transformed to a new domain. Then, the watermark bits are hidden into the transformed coefficients. Frequency domain based watermarking techniques are more efficient and ensure better robustness and higher invisibility compared to the spatial domain ones [Gup16, Mas17].

SVD and DWT as well as Lifting Wavelet Transform (LWT) and Discrete cosine transform (DCT) are the most used transform domain methods. Indeed, in [Bha18] a LWT based watermarking video scheme is introduced. In this scheme, the watermark bits are hidden in the quantified LH3 coefficients resulting from the application of the LWT to a selective set of frames. Simulation results prove the robustness and the imperceptibility of this technique. In [Him18], a watermarking technique combining DWT and SVD is presented. After being ciphered by a chaotic logistic function, the watermark is embedded only within key-frames. This scheme is robust against various attacks and it exhibits good imperceptibility level. A content-based authentication technique using DCT is proposed in [Far16]. In this scheme, frame index and invariant features extracted from intra macroblocks form the authentication code. Next, this latter is inserted into Quantized coefficients of the DCT performed on an arbitrary chosen Group of Pictures. This watermarking scheme is immune to non-malicious attacks but sensitive to content changing ones. Likewise, another semi-fragile watermarking scheme for surveillance video authentication is presented in [Man16]. In this approach, only scenes with major changes are implied in the watermarking process. The signature is generated from the highest informative block of the DCT coefficients and inserted in the lowest one.

Taking into account the above highlighted advantages and drawbacks of each watermarking category, we propose in this paper a ROI based semi-fragile watermarking scheme in the frequency domain using SVD and DWT for video authentication. The rest of this paper arrangement is as follows: section 2 provides a detailed description of the proposed watermarking scheme. Next, we present and discuss the obtained results in section 3. Finally, section 4 concludes this work.

2. PROPOSED SCHEME

The proposed video watermarking scheme involves three main components namely the watermark construction, the watermark embedding and the watermark extraction. These processes mechanisms are discussed in the following subsections. The originality of this work includes:

1) The proposed watermark construction strategy that allows to obtain a to-be-embedded watermark that can resist common attacks while being fragile to intentional manipulations. This is achieved thanks to the use of two efficient features detectors Speeded Up Robust Feature (SURF) and Maximally Stable Extremal Regions (MSER).

2) The suitable choice of the more appropriate regions ROI for signature insertion since they are the most targeted regions by malicious attacks in a video frame and each forgery on their content will be detectable.

3) The proposed frequency domain embedding process used to conceal the signature into the host video that involves two different domain transform techniques namely the SVD and the DWT. This watermark insertion method is designed upon the balance amongst the imperceptibility and the semi-fragility requirements consideration.

2.1 Watermark Construction Process

In the proposed scheme, the host video is initially divided into sequences of N frames. N is used as a first watermarking key and set to the number of frames per second (FPS) in each video. Then, as illustrated in Figure 1, an authentication watermark is generated from the first frame in the considered sequence using relevant features extracted from video frames. Next, regions of Interest (ROI) are detected. Indeed, moving objects are identified as the most important regions in the frame especially in video surveillance context [Ker17, Tbo12]. A technique that involves an adaptive improved version of Gaussian Mixture Model (GMM) [Cst19] for background subtraction and several morphological filters is used to accurately isolate the moving objects in every video frame [Abe13, Ben13]. Key points are further extracted from these ROI using SURF detector which is invariant to geometrical transformations and additive noise [Hba08]. To enhance the watermark robustness, we opt for

combining the SURF detector and the MSER one [Jma04]. MSER detector allows to determine connected pixels with intensity values that exhibit a negligible variation over several thresholds ranges. MSER regions are immune to illumination variation, rotation, scaling and translation [Ali18]. After performing MSER, only SURF key points hold in MSER sets are selected for the further steps and the remainder points are discarded. Considered points coordinates are converted to binary codes and then concatenated in one sequence. To increase the scheme security, this latter is scrambled using one dimensional Torus isomorphic mapping [Fzh19] which is a typical chaotic map operating following the formula:

$$X' = (K \times X) \bmod (L) + 1 \quad (1)$$

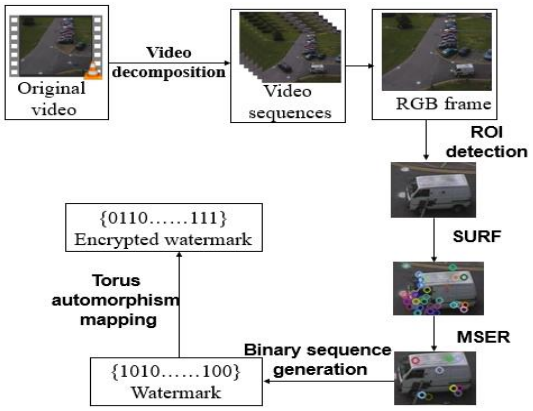


Figure 1. The proposed watermark construction process schematic framework.

Where mod denotes the modulus function. X' and X are the original bit position and the encrypted one. K is the second watermarking key, which should be a prime integer, and L is the binary sequence length.

Finally, the encrypted binary sequence is used as a watermark.

2.2 Watermark Embedding Process

The embedding procedure framework is presented in Figure 2. As already mentioned, the host video is decomposed in sequences containing N frames and a watermark is constructed for every sequence and embedded within each frame of the given sequence following the described procedure below. To start with, the RGB frame is converted to the YUV space color and its three constituent planes namely Y, U and V are separated. Only Y component is selected for the watermarking since it is more difficult to perceptually notice changes on luminance component as compared to chrominance ones. Following, the watermark is hidden in each ROI, recognized as already described in the previous subsection, which is an efficient choice for the authentication purpose as these regions hold on the most relevant information in the frames and every forgery on their content will be detectable; thus, each ROI is split into non-overlapping blocks.

To enhance the watermarking capacity, we adopt the 4x4 size instead of the generally used 8x8 size since one watermark bit is hidden in each block.

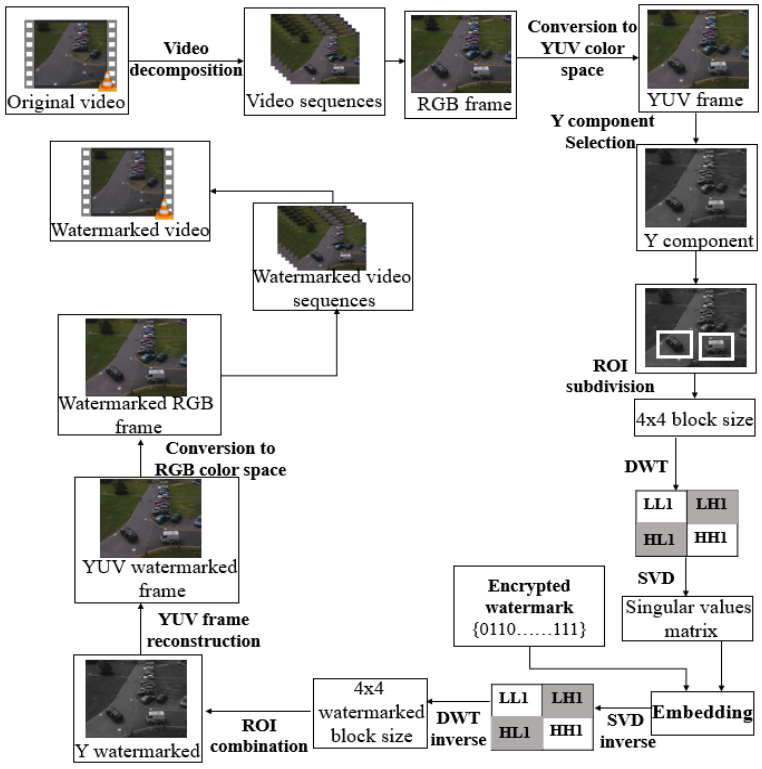


Figure 2. The proposed watermark construction process schematic framework.

As the proposed watermarking scheme operates in the frequency domain, each block undergoes one level DWT. This to avoid the visual degradation and the complexity cost yielded by multilevel DWT using. Providing the best compromise between the robustness and the imperceptibility makes the mid frequency sub bands the most appropriate for the watermark insertion. Hence, SVD is applied to these sub-bands. Due to its stable nature, the singular values matrix S is the most convenient location for watermarking. Finally, the watermark embedding is achieved by exploiting an additive blind method [Ham19]. This method allows the watermark strength control and optimization in order to well establish the trade-off between the robustness and the imperceptibility using the following equations:

If W=0

$$\begin{cases} S'(0,0) = S(0,0) + k_\alpha \\ S'(1,1) = S(0,0) \end{cases} \quad (2)$$

Otherwise

$$\begin{cases} S'(0,0) = S(1,1) + k_\beta \\ S'(1,1) = S(1,1) \end{cases} \quad (3)$$

With

$$k_\alpha = \frac{S(0,0)+S(1,1)}{\alpha} \quad (4)$$

$$k_\beta = \frac{S(0,0)+S(1,1)}{\beta} \quad (5)$$

With W is the to-be-embedded bit, S and S' are the original and the watermarked versions of S matrix. α and β are two scaling factors. Their values are fixed based on several experiments which demonstrate that the couple (2, 4) gives the best compromise between the imperceptibility and the robustness [Ham19]. Hence α=2 and β=4 are the used values in this work.

Finally, the inverse of each used function is performed to obtain the watermarked frame.

2.3 Watermark Extraction Process

The general architecture of the blind detection process is depicted in Figure 3. It starts operating with the same steps of the embedding process. After decomposing the watermarked video in sequences using the same watermarking key N, the frame is converted to YUV space and the Y plane is extracted. Once the ROI are detected and divided into 4x4 blocks, DWT and SVD are applied. The resulting singular values matrix coefficients are then scanned to extract the embedded information according to the following equation:

If $S''(0,0)-S''(1,1) > \frac{k_\alpha + k_\beta}{2}$

$W'' = 0$

Otherwise (6)

$W'' = 1$

Where S" and W" denoted the extracted singular values matrix and the extracted watermark bit. Hence, from each frame F_j in a given sequence a watermark denoted W_{Fj} will be extracted.

Let denote $\Omega_i = \{W^i_{F1}, W^i_{F2}, ..., W^i_{FN}\}$ a sample space. With W^i_{Fj} is the i-th bit in W_{Fj}. A global watermark W_E is built by determining each of its bits W^i_E as follows:

If $p(W^i_{Fj}=1) > p(W^i_{Fj}=0)$

$W^i_E = 1$

Otherwise (7)

$W^i_E = 0$

With p the probability function.
Besides, the generation process is performed under the first watermarked frame in the given sequence in order to obtain the reconstructed watermark W_R.
W_E and W_R are compared to verify the watermarked video authenticity.

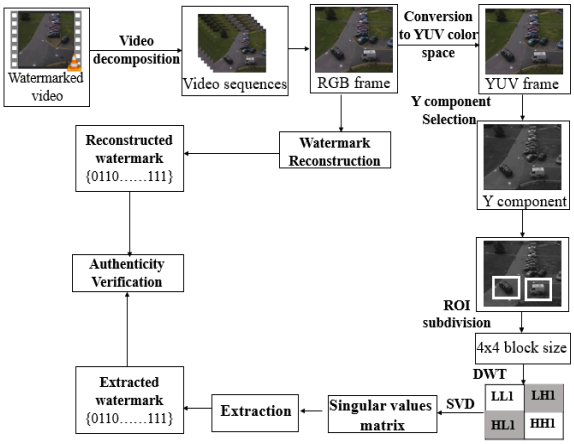


Figure 3. The proposed watermark extraction process schematic framework.

3. EVALUATION RESULTS

The proposed scheme performance is investigated in terms of imperceptibility and robustness. Various surveillance as well as common videos that comprise at least one moving object are used. These videos include test.avi, camera2.avi, video1.avi, akiyo.avi, news.avi and coastguard.avi. The first three sequences belong to PETS benchmark datasets. The last three videos are often employed to evaluate previous existing approaches.

3.1 Imperceptibility Assessment

To evaluate the visual distortion yielded by the watermarking scheme, the Peak Signal to Noise Ratio (PSNR) is used (Nta18, Kad16). The PSNR values corresponding to every test video are calculated using equation (8) and presented in Figure 4.

$$\text{PSNR} = 10 \log \left(\frac{255^2}{\text{MSE}} \right) \quad (8)$$

Where MSE designed the Mean Square Error.

As clear from Figure 4, the obtained PSNR values vary between 48.7431 dB and 73.425 dB which indicates the high similarity between the original videos and the watermarked ones. Moreover, the original frames and the corresponding watermarked ones, illustrated in Figure 5, confirm that the two frames versions are perceptually identical. In fact, the suitable choice of the ROI as well as the selection of the singular values matrix of the SVD transform allow guarantying this high invisibility level.

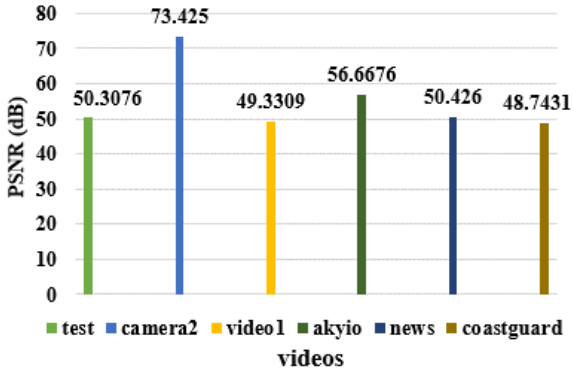
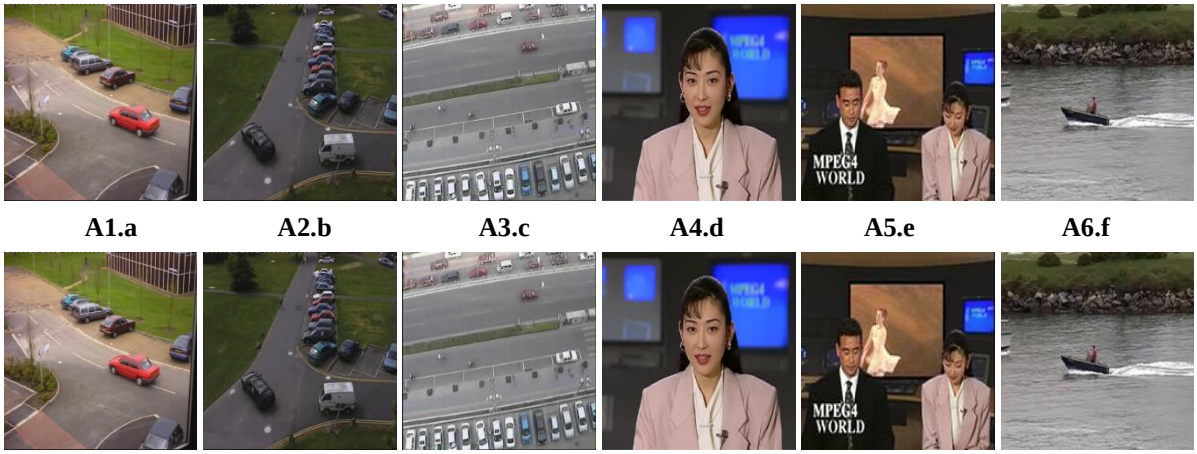


Figure 4. PSNR values for several watermarked videos.



A1.a **A2.b** **A3.c** **A4.d** **A5.e** **A6.f**

B1.a **B2.b** **B3.c** **B4.d** **B5.e** **B6.f**

Figure 5. Samples of (A) Original frames and their (B) watermarked versions from different used videos. (a) test.avi, (b) camera2.avi, (c) video1.avi, (d) akiyo.avi, (e) news.avi, (f) coastguard.avi.

Videos / Attacks	Test	Camera2	Video1	Akiyo	News	Coastguard
Salt & Pepper	0.0217	0.0018	0.0412	0.0315	0.0106	0.0330
Gaussian noise (0.01)	0.0091	0.0008	0.0414	0.0330	0.0053	0.0329
Gaussian noise(0.02)	0.0105	0.0008	0.0404	0.0340	0.0061	0.0372
Median Filter (3x3)	0.0158	0.0011	0.0390	0.0268	0.0058	0.0310
Median Filter (5x5)	0.0153	0.0004	0.0254	0.0192	0.0088	0.0326
MJPEG compression	0.0184	0.0010	0.0398	0.0009	0.0009	0.0329
Rotation (10°)	0.0215	0.0006	0.0312	0.0244	0.0155	0.0363
Rotation (20°)	0.0209	0.0012	0.0310	0.0328	0.0087	0.0537
Rotation (45°)	0.0149	0.0010	0.0408	0.0307	0.0056	0.0485
Brightness (+10%)	0.0140	0.0019	0.0440	0.0335	0.0061	0.0331
Brightness (+20%)	0.0181	0.0012	0.0392	0.0322	0.0062	0.0329
Brightness (-10%)	0.0237	0.0008	0.0396	0.0326	0.0061	0.0329
Brightness (-20%)	0.0189	0.0013	0.0398	0.0327	0.0065	0.0328
Contrast (x2)	0.0080	0.0108	0.0291	0.0325	0.0093	0.0341
Contrast (x0.5)	0.0122	0.0007	0.0416	0.0314	0.0046	0.0346

Table 1. The BER values under various unintentional attacks

3.2 Robustness Assessment

Bit error rate (BER), which is calculated via equation (9), is the metric used to evaluate the robustness of the technique and its ability to verify the content authentication (Asi15).

$$BER = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{W_R(i,j) \oplus W_E(i,j)}{m \times n} \quad (9)$$

With W_E and W_R are the extracted watermark and the reconstructed one.

The proposed scheme is designed to be capable to discriminate between unintentional attacks and intentional ones. To achieve this purpose, a threshold T is required. Since small BER values reflect the high immunity to a considered attack, the threshold T value is empirically fixed to 0.1.

The authentication decision is done based on the following assumptions:

If BER < T

The video is authentic.

Otherwise

The video is intentionally tampered.

As already mentioned, the scheme robustness is tested against two sets of attacks i.e. unintentional attacks and intentional ones. Table 1 exhibits the BER values obtained under unintentional attacks including (noise adding, filtering, rotation, MJPEG compression and brightness and contrast variation). From this table, it is evident that the proposed approach is immune to Gaussian noise as well as salt and pepper attacks since the obtained BER values are below the preset threshold T=0.1. The combination of SURF and MSER detectors as well as using the DWT, which are noises immune, guarantee this high resilience.

Furthermore, our watermarking scheme exhibits a good robustness against rotation attack. In fact, the obtained BER values vary between 0.0006 and 0.0537 for different rotation degrees. This robustness is achieved due to the utilization of SURF detector when designing the watermark and the involvement of SVD during the embedding process which are both rotation invariant. For median filter attack, the resulting BER values are ranged between 0.0004 and 0.0390 thereby inferior to T. Thus, the proposed scheme can withstand this kind of attack.

According to the BER values tabulated in Table 1, the embedded information is successfully extracted after applying MJPEG compression attack. The watermark insertion in the DWT mid frequency sub bands, which allows to avoid information loss during compression process, explains this high robustness. The last non-malicious considered attack is the brightness and contrast adjustment. Again, the BER values obtained by varying the brightness as well as the contrast ratios prove the robustness of our watermarking scheme since they are inferior to threshold T. This resilience is reached thanks to the use of MSER detector, which is immune to illuminance changes.

Similarly, the proposed scheme robustness is investigated under malicious attacks including (cropping, objects deletion and objects insertion attacks). For cropping attack, resulting BER values are displayed in Table 2. As can be seen from this table, The BER values, which are superior to the threshold T=0.1, demonstrate that the watermarked video is deliberately manipulated.

Concerning object manipulations attacks, we intentionally delete or add an object to the frames content of randomly chosen sequences as shown in Figure 6. BER values relative to object deletion and object insertion are respectively presented in Figure 7 and Figure 8. According to these figures, resulting BER values are significantly higher than the threshold 0.1. Therefore, the proposed scheme can effectively detect these two malicious attacks. This efficient ability is provided owing to the choice of the moving object as watermarking best location.

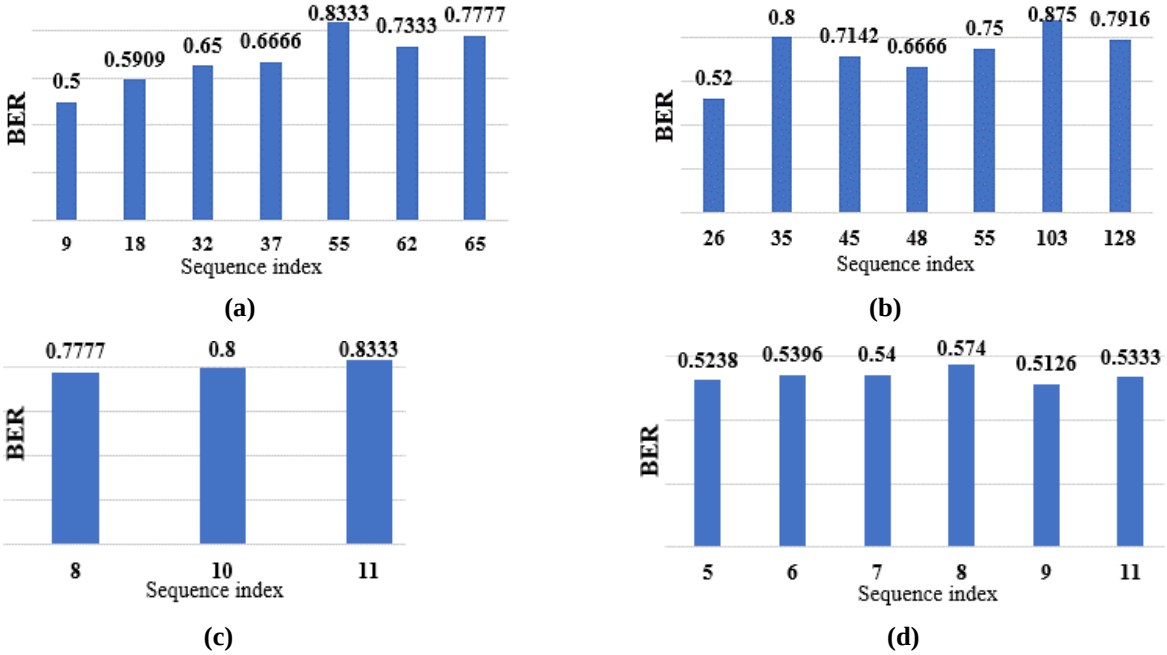
From all results, it can be concluded that our proposed scheme is suitable for authentication purpose where the discrimination between content preserving manipulations and content changing attacks is a prominent requirement.

Video / Window size	Test	Camera2	Video1	Akiyo	News	Coastguard
[20*20]	0.3484	0.2656	0.3840	0.1066	0.2502	0.1203
[40*40]	0.3608	0.3626	0.3840	0.1133	0.1984	0.1240
[60*60]	0.3884	0.4019	0.3840	0.1305	0.2233	0.1223
[80*80]	0.3531	0.4159	0.3840	0.1590	0.1378	0.1245
[100*100]	0.2712	0.41104	0.3840	0.1814	0.2700	0.1325

Table 2. The BER values under cropping attack with different window sizes

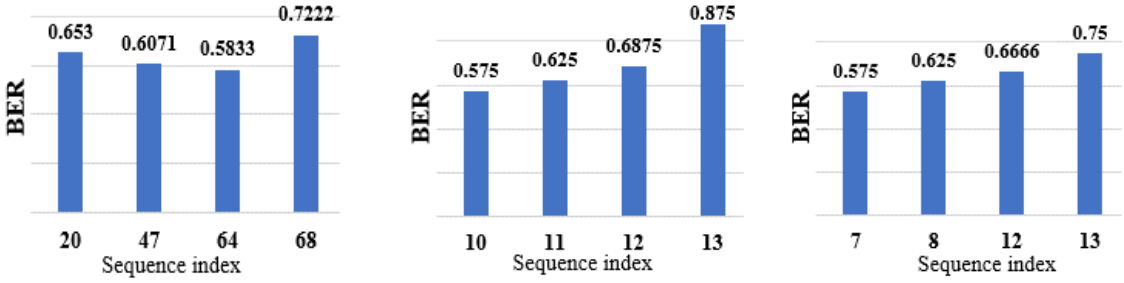
(a) (b) (c)

Figure 6. Sample of (a) original frame and its intentionally attacked versions by (b) object deletion and (c) object insertion.



(a) (b) (c) (d)

Figure 7. BER under object deletion attack for (a) test.avi, (b) camera2.avi, (c) video1.avi, (d) news.avi.



(a) (b) (c)

Figure 8. BER under object insertion attack for (a) test.avi, (b) akiyo.avi, (c) coastguard.avi.

3.3 Comparative Study

This section provides a comparison between the proposed watermarking scheme performance and the techniques proposed in Refs [Far16] and [Bha18] under different attacks. The technique presented in [Far16] operates using DCT by inserting the watermark into DCT coefficients. In [Bha18], a LWT based scheme is proposed where the watermark bits are concealed in the LH3 coefficients. Table 3 depicts BER values obtained after carrying out various attacks on the two watermarked videos versions resulting from the application of our approach and the technique presented in [Far16] to news.avi. Table 3 analysis reveals that the proposed system outperforms the technique in [Far16] in terms of robustness against all attacks listed in this table. The reason behind the proposed scheme robustness is the utilization of two domain transform techniques DWT and SVD instead

of one unique transformation which allows to better strengthen the resilience to common manipulations. Furthermore, the proposed watermark construction process which involves two noises immune features detectors namely SURF and MSER yields a signature characterized by a high survival level against several attacks. Performances comparison outcomes with [Bha18] are displayed in Table 4. Based on BER values reported in this table, it can be inferred that our technique exhibits better robustness compared to the work of [Bha18]. Concerning the imperceptibility performances, our watermarking scheme exceeds the method in [Bha18] as indicate the PSNR values given in Table 4. The main reason for this higher perceptual quality is the suitable choice of the watermark holders. In fact, the exploitation of SVD characteristics and DWT sub-bands ones to conceal watermark bits into the frame areas where human eye is less sensitive to the change preserves better output watermarked video quality.

Attacks	Ref [Far16]	Proposed scheme
Gaussian noise(0.01)	0.0581	0.0053
Gaussian noise(0.02)	0.0598	0.0061
MJPEG compression	0.0244	0.0009
Brightness (+10%)	0.0466	0.0061
Brightness (+20%)	0.0628	0.0062

Table 3. Robustness comparison with Ref [Far16]

	News		Akiyo	
	Ref [Bha18] **PSNR**=41.5(dB)	Proposed scheme **PSNR**=50.42(dB)	Ref [Bha18] **PSNR**=41.2(dB)	Proposed scheme **PSNR**=56.66(dB)
Gaussian noise (0.01)	0.0791	0.0053	0.0742	0.0330
Salt & pepper	0.0303	0.0106	0.0322	0.0315
Median Filter (3x3)	0.0117	0.0058	0.0098	0.0268
Median Filter (5x5)	0.0371	0.0088	0.0371	0.0192
MJPEG compression	0.0009	0.0009	0.0009	0.0009

Table 4. Imperceptibility and robustness comparison with Ref [Bha18]

4. CONCLUSIONS AND FUTURE SCOPE

In this paper, a semi-fragile watermarking approach is proposed for video content authentication. It initially involves a content based authentication signature generation process using both of SURF and MSER detectors. After that, the watermark bits are hidden in the host video frames following a ROI-SVD-DWT based embedding method. The proposed technique ensures a high imperceptivity level. Moreover, the simulation results prove that the proposed semi-fragile scheme appropriately suits the content authentication goal. In fact, it successfully detects content changes attacks while tolerating incidental manipulations. In coming future works, we will extend the proposed approach to handle temporal attacks and forgery localization.

5. ACKNOWLEDGEMENTS

The research leading to these results received funding from the Tunisian Ministry of Higher Education and Scientific Research under the grant agreement number LR11ES48.

6. REFERENCES

[Abe13] A. Ben Hamida, M. Koubaa, H. Nicolas and C. Ben Amar, "Video pre-analyzing and coding in the context of video surveillance applications," In: IEEE International Conference on Multimedia and Expo Workshops, pp. 1-4, 2013.

[Abe14] A. Ben Hamida, M. Koubaa, C. Ben Amar and H. Nicolas, "Toward scalable application-oriented video surveillance systems," In: Science and Information Conference, pp. 384-388, 2014.

[Aga19] Agarwal, N., Singh, A.K. and Singh, P.K., "Survey of robust and imperceptible watermarking," Multimedia Tools and Applications, 78(07), pp. 8603-8633, 2019.

[Ali18] Ali I.H. and Salman S., "A performance analysis of various feature detectors and their descriptors for panorama image stitching," International Journal of Pure and Applied Mathematics, 119(15), pp. 147-161, 2018.

[Ara19] Arab F., Zamani M., Poger S., Manigault C. and Yu S., "A Framework to Evaluate the Performance of Video Watermarking Techniques," In: Proceeding of the International Conference on Information and Computer Technologies, pp. 114-117, 2019.

[Asi15] Asim N., Yasir S., Nisar A. and Aasia R., "Performance evaluation and watermark security assessment of digital watermarking techniques," Science International, 27(2), pp.1271-1276, 2015.

[Ben13] Ben Hamida A., Koubaa M., Nicolas H. and Ben Amar C, "Spatio-temporal video filtering for video surveillance applications," In: IEEE International Conference on Multimedia and Expo Workshops, pp. 1-6, 2013.

[Ben14] Ben Hamida A., Koubaa M. and Ben Amar C Nicolas H, "Parallelepipedic shape modeling for moving objects in video surveillance systems," In: Science and Information Conference, pp. 379-383, 2014.

[Bha18] Bhardwaj, A., Verma, V.S. and Jha, R.K., "Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform," Multimedia Tools and Applications, 77(15):19659-19678, 2018.

[Bpa14] B. P. Aditya, U. G. K. Avaneesh, K. Adithya, Akshay Murthy, R. Sandeep and B. Kavyashree, "Invisible semi fragile watermarking and steganography of digital videos for content authentication and data hiding," International Journal of Image and Graphics, 19(03),pp. 1950015-1-19, 2019.

[Cst19] C. Stauffer C and W.E.L Grimson, "Adaptive background mixture models for real-time tracking," In: Computer Society Conference on Computer Vision and Pattern Recognition, pp. 246-252, 1999.

[Far16] Farfoura M.E., Horng S.J. and Guo J.M., "Low complexity semi-fragile watermarking scheme for H.264/AVC authentication," Multimedia Tools and Applications, 75(13), pp. 7465–7493, 2016.

[Fzh19] F. Zhang and Y. Zou, "Reducible mapping class of the canonical Heegaard splitting in a mapping torus," Topology and its Applications, 258, pp. 425-432, 2019.

[Gup16] Gupta G., Gupta V.K and Chandra M., "Review on Video Watermarking Techniques in Spatial and Transform Domain," In: International Conference on Information Systems Design and Intelligent Applications, pp. 686-691, 2016.

[Ham19] Hammami A., Ben Hamida A. and Ben Amar C., "A Robust Blind Video Watermarking Scheme Based on Discrete Wavelet Transform and Singular Value Decomposition," In: International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Application, pp. 597-604, 2019.

[Hba08] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," Computer Vision and Image Understanding, 110(3), pp. 346-359, 2008.

[Him18] Himeur Y. and Boukabou A., "A robust and secure key-frame based video watermarking system using chaotic encryption," Multimedia Tools and Applications, 77(7), pp. 8603-8627, 2018.

[Jma04] J. Matas, O. Chum, M. Urban and T. Pajdla, "Robust wide-baseline stereo from maximally stable extremal regions," Image and Vision Computing, 22(10), pp. 761-767, 2004.

[Jos17] Joshi A.M., Gupta S., Girdhar M., Agarwal P. and Sarker R., "Combined DWT–DCT-Based Video Watermarking Algorithm Using Arnold Transform Technique," In: Proceedings of the International Conference on Data Engineering and Communication Technology, pp. 455–463, 2017.

[Kad16] Kadu S., Naveen C., Satpute V. R. and Keskar A.G., "Discrete wavelet transform based video watermarking technique," In: International Conference International Conference on Microelectronics, Computing and Communications (MicroCom), pp. 1-6, 2016.

[Ker17] Kerbiche A., Ben Jabra S., Zagrouba E. and Charvillat V., "Robust Video Watermarking Approach Based on Crowdsourcing and Hybrid Insertion," In: International Conference on Digital Image Computing: Techniques and Applications, pp. 1–8, 2017.

[Kha15] Khalid Tahboub, Neeraj Gadgil, Javier Ribera, Blanca Delgado, and Edward J. Delp. "An intelligent crowdsourcing system for forensic analysis of surveillance video", In: Proceeding of the 27th IS&T/SPIE on Video Surveillance and Transportation Imaging Applications, pp. 94070-I-19, 2015.

[Man16] Manikandan V.M., Masilamani V., "Real-Time Scene Change Detection and Entropy Based Semi-Fragile Watermarking Scheme for Surveillance Video Authentication," In: International Symposium on Big Data and Cloud Computing Challenges, pp. 101-110, 2016.

[Mas17] M. Asikuzzaman and M. R. Pickering, "An overview of digital video watermarking," IEEE Transactions on Circuits and Systems for Video Technology, 28(9), pp. 2131-2153, 2017.

[Mch14] M. Charfeddine, M. El'Arbi and C. Ben Amar, "A new DCT audio watermarking scheme based on preliminary MP3 study," Multimedia Tools and Applications, 70(3), pp. 1521-1557, 2014.

[Mko12] M. Koubaa, M. Elarbi, C. Ben Amar and H. Nicolas, "Collusion, MPEG4 compression and frame dropping resistant video watermarking," Multimedia Tools and Applications, 56(2), pp. 281-301, 2012.

[Nta18] N. Tarhouni, M. Charfeddine and C. Ben Amar, "Discrete wavelet transform based video watermarking technique," In: International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision, pp. 78-86, 2018.

[Tbo12] T. Bouchrika, M. Zaied, O. Jemai and C. Ben Amar, "Ordering computers by hand gestures recognition based on wavelet networks," In: 2nd International Conference on Communications Computing and Control Applications, pp. 1–6, 2012.