Multimedia Tools and Applications (2021) 80:7479–7513
https://doi.org/10.1007/s11042-020-09982-4

Blind semi-fragile watermarking scheme for video authentication in video surveillance context

Amal Hammami[1] · **Amal Ben Hamida**[1] · **Chokri Ben Amar**[1]

Received: 23 December 2019 / Revised: 7 August 2020 / Accepted: 24 September 2020 /
Published online: 28 October 2020

Abstract

With the development of advanced multimedia editing tools, numerous unauthorized manipulations are easily doable to surveillance systems video files. Thus, video tamper detection is revealed as a big challenge for multimedia security field researchers. Indeed, we propose herein a singular value decomposition (SVD) and discrete wavelet transform (DWT) based semi fragile watermarking scheme for video content authentication. A content-based authentication signature is firstly generated by extracting reliable features from regions of interest. QR code generation technique as well as Arnold transform are used to boost the security aspect of the watermark. This latter is efficiently hidden in the wavelet middle frequency sub bands through an additive embedding algorithm and then extracted via a blind detection method. Simulation results demonstrate that the proposed scheme jointly achieves a good perceptual quality and a high watermark capacity. In addition, it is capable of distinguishing intentional attacks from incidental modifications. Indeed, the proposed watermarking scheme is very fragile to malicious tampering while allowing non-malicious processing.

Keywords Blind semi-fragile watermarking · Video authentication · Video surveillance · Singular value decomposition · Discrete wavelet transform · Quick response code

Abbreviations: Used acronyms and symbols

Acronym/Symbol	Definition
BER	Bit Error Rate
Cmax	Maximum Capacity
DCT	Discrete Cosine Transform

✉ Amal Hammami
amal.hammami@enis.tn

Amal Ben Hamida
amal.benhamida@enis.tn

Chokri Ben Amar
chokri.benamar@ieee.org

[1] REsearch Groups in Intelligent Machines, University of Sfax, National Engineering School of Sfax, Sfax 3038, Tunisia

DWT	Discrete Wavelet Transform
$Fact_{\alpha}$	Scaling factor
$Fact_{\beta}$	Scaling factor
FFT	Fast Fourier Transform
FPS	Frame per second
GMM	Gaussian Mixture Model
GOP	Group Of Pictures
HH	High Frequency sub-band
HL	Middle Frequency sub-band
LH	Middle Frequency sub-band
LL	Low Frequency sub-band
LWT	Lifting Wavelet Transform
NC	Normalized Correlation
PCA	Principal Component Analysis
PSNR	Peak Signal to Noise Ratio
QDCT	Quantized Discrete Cosine Transform
QR code	Quick Response code
ROI	Regions Of Interest
$S_{extracted}$	Extracted singular value matrix
$S_{original}$	Original version of the singular value matrix
SSIM	Structural SIMilarity index
$S_{watermarked}$	Watermarked version of the singular value matrix
T_{BER}	Threshold for BER values
T_{NC}	Threshold for NC values
ViSAR	Video Synthetic Aperture Radar
$W_{embedding}$	Watermark bit
$W_{extracted}$	Extracted watermark bit
$W_{regenerated}$	Regenerated watermark bit
$\oplus$	Exclusive OR operation

1 Introduction

Nowadays, video surveillance is broadly deployed in several sectors. In fact, surveillance cameras are increasingly installed in public places as well as private ones for instance, in street corners, commercial stores, residential areas, airports, train stations etc. Indeed, 245 million security cameras were active around the world in 2014 [26]. According to Information Handling Services (IHS), there were less than 10 million professionally installed video surveillance cameras globally in 2006 [24]. This number rises quickly to beyond 100 million in 2016. Moreover, over than130 million cameras are shipped in 2018. The main reasons for this burgeoning deployment are the public safety improvement against the crime threat growing and the property security in the society [14]. In addition, the hardware low cost in comparison to the human surveillance further enhances the video surveillance systems ubiquity [14, 22]. Furthermore, videos recorded by a video surveillance system are the subject of many analytical functions such as objects classification and identification, objects tracking and activities and behaviors analysis [7–9]. Besides, they play an important role in police and judicial investigations as legal evidences.

In the other hand, the recent revolution in computer technology field is leading to several problems for the multimedia industry in general and the video surveillance one in particular. In fact, this improvement comes across with the development of sophisticated signal and image processing software, which are able to maliciously manipulate the stored videos content without deteriorating of the visual quality. For instance, surveillance sequences can be simply doctored in such way to exculpate or incriminate an individual. Thereby, the stored videos lose their trustworthiness and credibility as legal proof in front of court low. Hence, it is a critical need that video surveillance systems integrate authentication procedures in order to guarantee data integrity and prove their true origin [72].

To overcome this challenge, a broad range of authentication techniques has already been introduced. Cryptography with different protocols is one of the most used solution to protect videos authenticity and integrity [1, 45, 62]. Nonetheless, this video authentication mechanism has some shortcomings such as computation and storage requirements. Likewise, after encrypting the digital video any visualization, analysis or visual data search requires its decryption. To deal with these weaknesses, video watermarking is introduced as a promising cryptography alternative [39, 40, 50, 51]. It is the procedure of embedding a signature called watermark in the video frames. The embedded watermark can be an image, a logo or any particular kind of information content. A video watermarking system is consisting of two processes as shown in Fig. 1. The first one is the embedding, which refers to the watermark combination with the host video. The information to be used as a watermark can be an image or a binary sequence. In addition, it can be constructed through exploiting video frames features. The watermark extraction is the second process consisting a video watermarking system. It is the process of extracting the hidden information from the eventually tampered watermarked video that will be used to ascertain the video content authenticity.

Watermarking based authentication approaches were first introduced as fragile watermarking systems. In this case, any modification of the watermarked video readily generates a mark detection failure. Thus, the watermark loss is considered as an evidence of content tampering. The main benefit of fragile watermarking is the ability of tampering localization but it is so difficult to discriminate between malicious video processing which aims to alter the video semantic content and some non-intentional processing [3, 13]. Another popular used approach is the robust watermarking. It is aptly named due to its resilience against any attacks form. Indeed, the hidden information can be recovered from tremendously attacked watermarked video [23, 48]. To exploit the advantages of both the fragile approach and the robust one, another paradigm is introduced. It is referred as semi fragile [21, 49]. This watermarking method type is designed to be robust against intentional tampering distortion and to tolerate only unintentional manipulations. A semi-fragile watermarking system has provide its efficiency for applications that require a trade-off between robustness and fragility namely for video surveillance application. Thus, we propose in this work a blind semi fragile watermarking scheme for video authentication in video surveillance context using Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Quick Response code (QR code) and Arnold Transform.

This paper remainder is organized as follows. Section 2 provides an overview of video watermarking field. The review of state of the art of video watermarking based authentication techniques is given in Section 3. Section 4 presents the proposed semi fragile watermarking scheme. Performances results and a comparison with existing techniques are reported in Section 5. Finally, conclusions are drawn and perspectives are open in the last section.

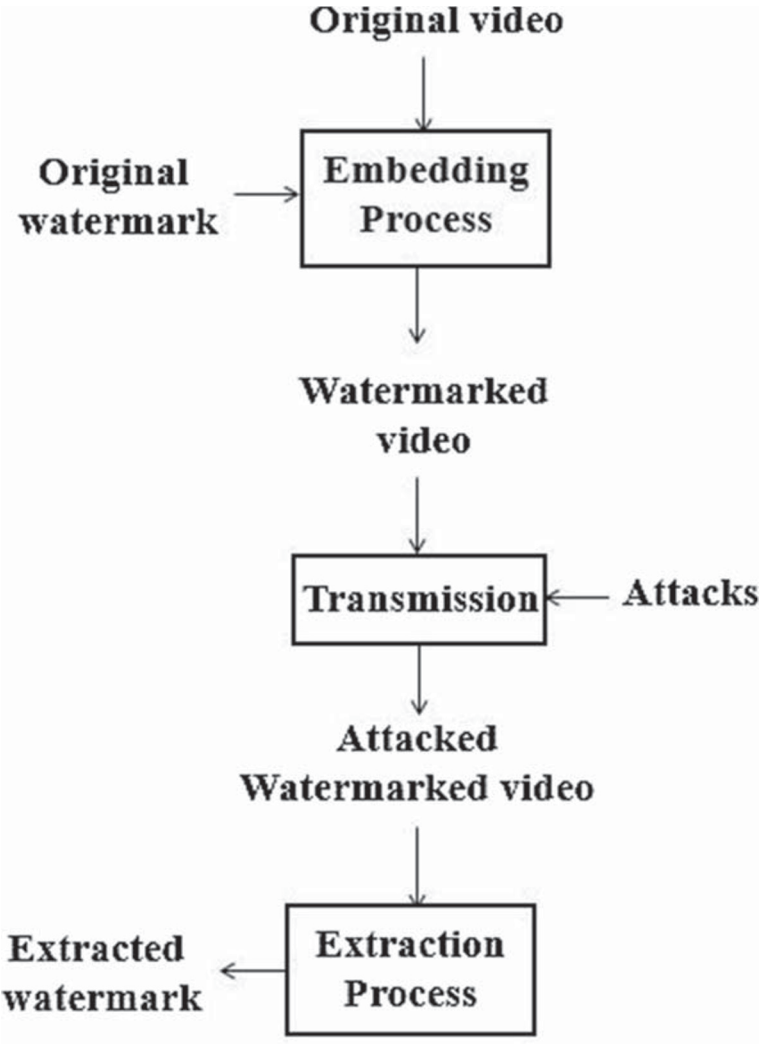


Fig. 1 Video watermarking general framework

2 Overview of video watermarking

In this section, an overview of video watermarking and its main terminologies is given. First, we define the video watermarking applications. Next, we key out the requirements in this field. Finally, we present various video watermarking techniques classifications.

2.1 Video watermarking applications

Digital watermarking has become into vogue from the late 1980s. This research area has quickly witnessed a great growth due to its important applications. Broadcast monitoring

is one of the common used video watermarking applications. It enables advertising agencies to verify whether their commercial contents are broadcasted as contracted by hiding a watermark in advertisements contents. In fact, extracting the embedded watermark enables to check that commercials have been aired during all the payed for time [32, 52]. Moreover, watermarking can be used for fingerprinting. This application allows finding illegal copies source. Indeed, the owner can embed a different watermark in each content media copy. Thus, this mark enables the intellectual property owner to identify the buyer for each legal distribution and check who has broken his license by providing the content to third parties [42, 76]. Copyright protection is a fundamental video watermarking application. In this case, specific owner information are used as a watermark in order to identify the copyright ownership as well as prevent video fraud and misappropriation. Indeed, watermark retrieving from the watermarked video allows the rightful owner to prove the video ownership when someone alleges it [18, 67]. Besides, data authentication is another popular watermarking application, which aims to confirm the watermarked video integrity and to detect the attempted altering of the original video content. The watermark, which is concealed in the host video, is designed to be affected by signal manipulations and then be used to indicate whether the watermarked video content is authentic or not [34, 69].

2.2 Video watermarking requirements

As we previously mentioned, video watermarking is exploited in wide range of applications. Consequently, every watermarking system should have its own specific properties with respect to the considered application. Mostly, three requirements are basically given for most video watermarking systems. The first one is imperceptibility or transparency, which refers to the watermarked video perceptual quality. Obviously, it depends on the embedding process. Indeed, the distortion caused by the algorithm used for watermarking should add a minor degradation to the host video perceptual quality. Therefore, the watermarked video should not be distinguishable from the original one by human eyes. The second property is robustness. It means the ability of the watermark to survive under distortions. These attacks are mainly divided into two types; unintentional and intentional ones. Unintentional attacks are processing that do not have the goal to impair or remove the watermark. Intentional attacks attempt mischievously to damage the embedded data in the watermarked video. Capacity denotes the third requirement for video watermarking system. It defines the maximum amount of information that can be hidden in the host video as a watermark. The embedded information size varies according to the targeted watermarking application. For instance, for security purpose, a big capacity is required. In contrast, for copy protection purpose one-bit capacity is generally sufficient. Imperceptibility, robustness and capacity are mutually dependent to each other. In fact, increasing the capacity leads to decrease the robustness and degrade the visual quality. Therefore, a good trade-off among all the properties listed above should be maintained when designing a watermarking system [5, 70, 71].

2.3 Video watermarking techniques classification

Video watermarking techniques can be classified based on distinct criteria. According to human perception, video watermarking techniques are divided into two classes: visible watermarking techniques and invisible ones. For the first class, the watermark is embedded in such way to be noticeable when viewing the watermarked video. For the second class, the watermark is concealed in the host video in order to be perceptively unidentifiable by

human eyes. Based on watermark detection criterion video watermarking techniques are classified as non blind, semi blind and blind. In non blind techniques, both the original video and the watermark are required during the extraction process. On the other hand, in semi blind techniques the information used as a watermark can be successfully extracted from the watermarked video without using the original video. In blind detection neither the embedded watermark nor the original host video are required for watermark extraction [5, 6].

Another criterion, which is frequently used to classify video watermarking schemes, is the working domain. Indeed, depending upon this criterion video watermarking techniques are usually divided into two categories. The first one is the spatial domain watermarking. In this type, the embedding process is achieved by directly modifying or replacing the original video frame pixel values. Spread spectrum, Least Significant Bit, correlation based technique present the most used technique in this domain [60, 61, 75]. Spatial domain based watermarking approaches are characterized by a simple implementation and a low computational complexity. However, it is denoted that these techniques have several drawbacks namely low embedding capacity and weak robustness against several attacks specially compression. The frequency domain which also referred as transform domain is the spatial domain alternative. Video watermarking technique in this case starts by converting the host frame to a new appropriate working domain. Then transform coefficients are adjusted by the watermark to obtain a watermarked frame. The common domain transformation techniques are the singular value decomposition (SVD), the Discrete Cosine Transform DCT, the Discrete Wavelet Transform (DWT) and the Lifting Wavelet Transform (LWT)[30, 54, 59]. Frequency domain based approaches have gained a tremendous exposure as compared to spatial domain based ones since they are more resilient to geometrical and compression attacks. Subsequently, they yield large capacity and better imperceptibility by respecting more advanced human visual system properties. Therefore, transform domain based approaches allow to efficiently meet the trade-off between the different watermarking system requirements [6, 11, 74].

3 Related work

Video authentication through video watermarking scheme is an appealing field, which motivates several researchers. In the literature, there is a variety of existing approaches relevant to this research area. As already noted in Section 2.3, video watermarking techniques are commonly classified, based on the embedding domain criterion, to two categories, i.e., spatial domain watermarking techniques and frequency domain ones. In the present section, we will only investigate frequency domain based watermarking schemes since this domain allows better attaining the compromise between the different watermarking requirements. Regarding the number of the used domain transformations, existing approaches dedicated to frequency domain can be mono frequency or multi frequency.

The mono-frequency based watermarking systems involve only one transform to embed the mark. In [4], Alenizi et al. propose a new DWT based video watermarking scheme for authentication purpose. The luminance Y component undergoes a DWT decomposition via randomly generated filters to increase the algorithm security. The watermark is inserted in the middle frequency sub band using an additive method with a pseudo-random sequence P, which is generated using a secret key and a constant magnitude factor α to control the watermark robustness. The simulation results show that this scheme has good performances

under different well-known attacks. However, it gives lower performance in terms of correlation when the scenes have a smooth nature and a few motions. In [29], a DCT based video watermarking is introduced. In this scheme, the watermark is concealed in the low frequency sub-band resulting of the DCT application to the changed scene specific frames. Farfoura et al. present a semi-fragile watermarking scheme for content-based authentication [19]. The authentication codes used in this scheme are composed of frames index timing information and invariant features, which are extracted from intra macroblocks. The watermark is inserted into Quantized DCT (QDCT) coefficients in a set of random chosen Group of Pictures (GOP). The advantages of this watermarking scheme are the resilience against semantic content preserving attacks as well as the sensitivity to content altering attacks. In addition, the technique shows a low computational complexity and a good imperceptibility level. Furthermore, Bhardwaj et al. introduced a robust video watermarking technique operating in the mono frequency domain [10]. In this scheme, the to-be-watermarked frames are chosen via a frame selection procedure based on the mathematical relationship between the non-watermarked video frames index, the embedding capacity and the coefficient block size. The watermark bits are hidden in the quantified LH3 sub-band coefficients resulting from the lifting wavelet transform (LWT). Experimental results demonstrate that this technique is robust to various image processing attacks with a good level of imperceptibility. Khosravi et al. propose several efficient interpolation based-watermarking schemes operating in the mono frequency domain for data management transmission in remote sensing video surveillance by video synthetic aperture radar (ViSAR). In fact, this latter provides several principal, control and managerial data which should be compressed before been transmitted. Hence, authors adopt watermarking systems based on interpolators and domain transformations such as Fast Fourier Transform (FFT), (DCT) and (DWT) to aggregate and reduce the ViSAR information size [36–38].

Conversely, multi-frequency based video watermarking techniques operate combining several transformations in the embedding process. A DWT and SVD based watermarking technique is developed in [65]. In this methodology, Fibonacci sequence is used to identify key frames which will be used for the watermarking. The watermark singular values are embedded in LH mid frequency sub band coefficients of selected frames. Based on simulation results, this technique is immune to video processing attacks and it ensures a good quality of watermarked videos. Another multi-frequency based video watermarking combining the (DWT) with the principal component analysis (PCA) is proposed by Yassin et al. in [73]. In this work, two levels DWT is used to transform the Y component to the frequency domain. The maximum coefficients of the maximum entropy principal component analysis (PCA) blocks are identified as the optimal watermarking locations. The watermark is hidden in the selected suitable coefficients quantified values. According to the experimental results, this watermarking methodology proves its robustness against different distortions specially contrast adjustment, Gaussian noise addition and JPEG coding.

In [56], Nouioua et al. introduce a novel digital video watermarking technique based on SVD which performs in the Multi-resolution Singular Value Decomposition domain. The watermark is encrypted through a Logistic Map Encryption and then hosted only in the fast motion frames in each video shot. The embedding is done following a blind Quantization Index Modulation algorithm. Authors claimed that this scheme is secure and robust to a variety of manipulations like compression, image processing and frame synchronization. Another multi-frequency based video watermarking technique is developed by Panyavaraporn for both copyright protection and content authentication purposes [58]. In this scheme, discrete wavelet transform is used as a combination with discrete cosine transform. Indeed,

the watermarking is achieved by applying DWT on the Y component of the video sequence frames then performing the DCT on the middle frequency sub bands and finally the watermark is inserted in mid-band DCT coefficients. The proposed algorithm has proven its robustness especially against compression attacks and has shown visually acceptable quality. Similarly, an enhanced watermarking approach using DWT, DCT and interpolation is proposed in [33]. In this algorithm, interpolation technique is applied, after the watermark extraction, to zoom the host frame and to get the concealed and improved information hidden in the host watermarked frame.

According to the above existing video watermarking approaches overview, it is clear that the combination of transformation domain techniques offers better resilience to different attacks than the technique involving one single transform. Consequently, in the proposed work the watermark embedding is carried out in the multi frequency domain.

4 Proposed approach

The proposed system is a blind and semi fragile video watermarking in the frequency domain based on DWT, SVD, QR code and Arnold transform for video authentication in video surveillance context.
As illustrated in Fig. 2, it involves 3 processes namely: the watermark generation, the watermark embedding and the detection process. The design of each process will be explained in the following subsections.

The main contributions in this work are:

1) The selection of proper invariant features to construct a content-based watermark that exhibits semi fragility property and allows to fulfill the task of discrimination between malicious processing actions and non-malicious ones.
2) The adoption of QR code technique and Arnold transform to deal with the watermark security and computational complexity challenges. Before being embedded in the host video frame, the watermark is processed by a QR code generator and then encrypted by Arnold transform. Therefore, the hidden information cannot be recovered in its original form even if the attacker successfully decodes the extraction algorithm.
3) The hybridization of two transformation domain techniques, namely the DWT and the SVD, and the exploitation of their complementary characteristics to enhance the watermarking system performance. In fact, The DWT sub bands properties as well as the relation between the SVD coefficients are jointly used to embed the watermark into the host video and to guarantee a blind detection during the extraction process.

4.1 Preliminaries

To better understand the details of the proposed approach, a brief overview of YUV space color, discrete wavelet transform, singular value decomposition, QR code technique and Arnold transform is provided in this section.

4.1.1 YUV color space

The YUV color spaces consists of luminance (intensity) and chrominance (color) components.YUV components are less correlated than the RGB color space ones that makes it more suitable for image and video processing applications and for watermarking in

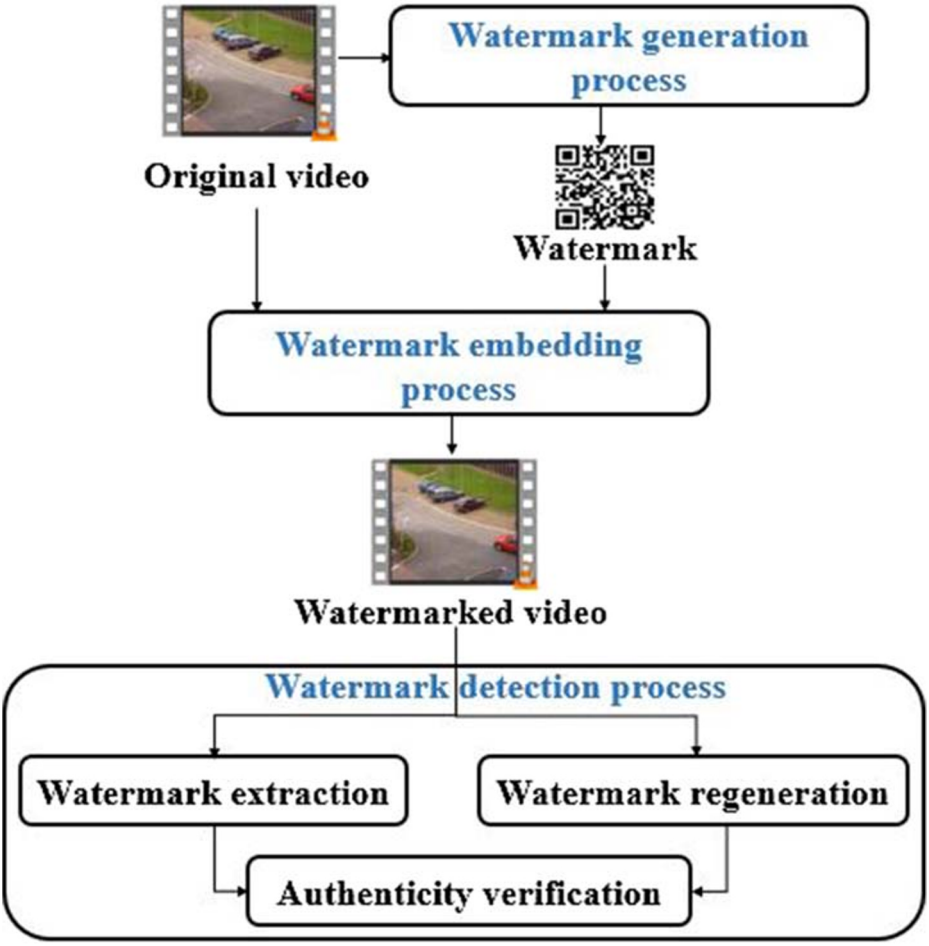


Fig. 2 The proposed approach general framework

particular. The conversion from RGB to YUV and the transformation from YUV to RGB are done using formulas (1) and (2) respectively.

$$\begin{cases} Y = 0.299 \times R + 0.587 \times G + 0.114 \times B \\ U = -0.147 \times R - 0.289 \times G + 0.436 \times B \\ V = 0.615 \times R - 0.515 \times G - 0.100 \times B \end{cases} \tag{1}$$

$$\begin{cases} R = Y + 1.140 \times V \\ G = Y - 0.395 \times U - 0.581 \times V \\ B = Y + 2.032 \times B \end{cases} \tag{2}$$

4.1.2 Singular value decomposition

SVD is a numerical transform which decomposes an mxn real matrix A into a factorization of three matrices [39, 57]:

$$A = U \times S \times V^t \tag{3}$$

Where:

$$U = \begin{bmatrix} u_{11} & u_{12} & \dots & 0 & u_{1m} \\ u_{21} & u_{22} & \dots & 0 & u_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{m1} & u_{m2} & \dots & 0 & u_{mm} \end{bmatrix} S = \begin{bmatrix} S_{00} & 0 & 0 & \dots 0 \\ 0 & S_{11} & 0 & \dots 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & S_{nn} & 0 \end{bmatrix} V^t = \begin{bmatrix} v_{11} & v_{12} & \dots & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & \dots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ v_{n1} & v_{n2} & \dots & \dots & v_{nn} \end{bmatrix}$$

U and V, that are orthogonal matrices of size mxm and nxn respectively, present the singular vectors of matrix A. S is mxn diagonal matrix and its non-zero elements arranged in descending order define the singular values of matrix A. The singular values matrix S ensures higher invisibility and more robustness against attacks as compared to U and V matrices thereby it suits the watermarking requirements. Generally, SVD is gaining more popularity in image and video processing area thanks to it attractive properties namely its conceptual stability and its maximum energy packing [43, 63].

4.1.3 Discrete wavelet transform

DWT is a mathematical tool used to hierarchically decompose an image and video frames. This tool allows separate an image into 4 frequency sub-bands i.e. low-frequency sub-band (LL) as well as high-frequency sub-band (HH) and mid frequency sub-bands (HL and LH). The process can be repeated to compute multiple levels wavelet decomposition. DWT is well known for its resilience to noise addition and compression. Also, it better modulates the Human Visual System aspects than the other domain transformation techniques. Hence, it was adopted for many practical applications in image and video processing such as image restoration and image zooming as well as transmission and compression [27, 28, 53, 55]. It is often used in watermarking schemes due to its spatial localization, frequency spread and multi-resolution modelling [2].

Figure 3 illustrates the sub-bands obtained after two decomposition levels.

4.1.4 Quick response code

Quick response code is a two dimensional matrix symbols introduced in 1994 by Denson-Wave and it is standardized by the international organization for standardization as ISO/IEC 18004:2015 [25].

A QR code is a set of black square blocks arranged in a white background. Version information, separators, timing patterns, format information, data and error correction, quiet zone, alignment patterns and position detection are the QR code basic structure elements as

Fig. 3 **a** Original image **b** 1 level DWT decomposition **c** 2 level DWT decomposition

shown in Fig. 4. It is used in a wide range of multimedia applications especially when a great information size should be transmit in a compact format. In fact, a QR code can carry up to 7089 numeric characters and up to 4296 alphanumeric characters [31]. Likewise, providing a good damage resilience and a high storage capacity are the main reasons for the QR code adoption in the watermarking field.

4.1.5 Arnold transform

Arnold transform is an invertible and iterative mapping, which permits to randomize the original pixels positions in an image. The considered iterations number is called as the Arnold's period and it depends on the original image size. The main purpose of the Arnold transform is to warp the original image semantic, which become unreadable in the scrambled version. The Arnold Transform of an nxn image is described by the following equation [58]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mod N \tag{4}$$

Where (x, y) and (x', y') are the original pixel coordinate and the scrambled one respectively and N is the image size.

Arnold transform is recognized as one of the most used image scrambling technique. It has various applications, particularly in watermarking field; it is often utilized to encrypt the watermark in order to ensure the confidentiality and to improve the security level of the watermarking scheme [64]. Indeed the watermark cannot be extracted without an accurate knowledge of the particular Arnold period K.

Figure 5 depicts an example of Arnold transform applied to an image with different periods K.

4.2 Watermark generation process

A well-designed watermark is a prominent requirement for the watermarking scheme efficiency. In the proposed watermarking system, the host video is divided into sequences of N

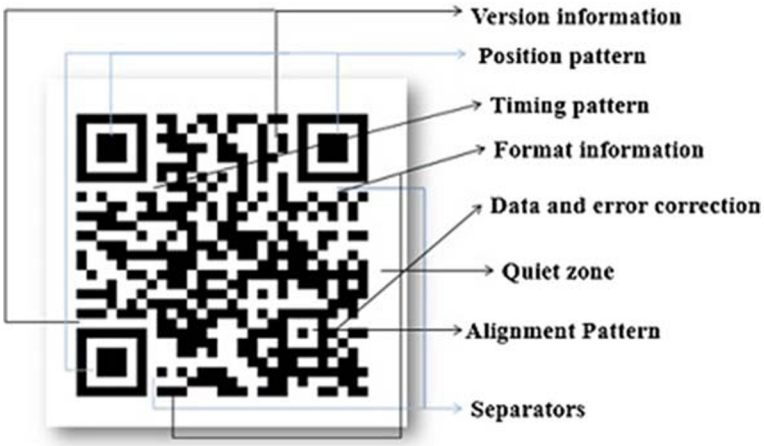
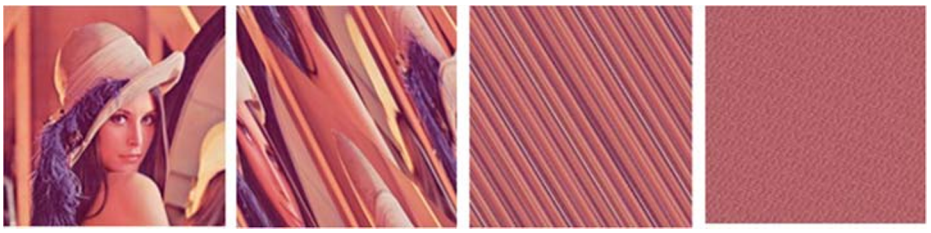


Fig. 4 Quick Response code basic structure



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

Fig. 5 **a** original image Lena **b** Arnold transform with period = 1 **c** Arnold transform with period = 3 **d** Arnold transform with period = 7

successive frames. For every video sequence, a watermark is generated from its first frame based on Algorithm 1 and then it is repeatedly inserted in each frame of the given sequence.

Algorithm 1 Watermark generation pseudo-code.

Input:
Seq: video sequence of N frames
K: Watermarking secret key
Output:
$Watermark_{scrambled}$: Scrambled watermark
begin
$FirstFrame \leftarrow Seq[1]$
$ROI \leftarrow MovingObjectDetection(FirstFrame)$
$Edge \leftarrow EdgeDetection(ROI)$
$SalientPoint \leftarrow SalientPointDetection(Edge)$
for i=1:length(SalientPoint) **do**
$CartographicMaps \leftarrow Cordiantes(SalientPoint[i])$
end for
$Watermark \leftarrow QRCodeGenerator(CartographicMaps)$
$Watermark_{scrambled} \leftarrow ArnoldTransform(Watermark, K)$
end

In order to cater to the security need, N, which defines the number of frames in each sequences is used as a first secret key. In fact, a large value of N means embedding the same watermark into a large number of consecutive frames. Conversely, small value of N denotes the watermarking of few number of frames with the same watermark. Hence, its value should be properly fixed to avoid making the watermark vulnerable to unintentional manipulations.

As illustrated in Fig. 6, the watermark generation process implies two main steps: Regions Of Interest (ROI) extraction and watermark construction. Since we focus on captured videos for surveillance purpose in public places, moving objects for instance pedestrians and vehicles are the required regions. Indeed, they are the most targeted regions by malicious attacks in a video frame and each intentionally forgery on their content should be detectable. A technique based on adaptive improved version of Gaussian Mixture Model (GMM) [68] is used to detect ROI. In order to remove noising information, morphological filtering operations such as closing and opening are achieved as explained in [7].

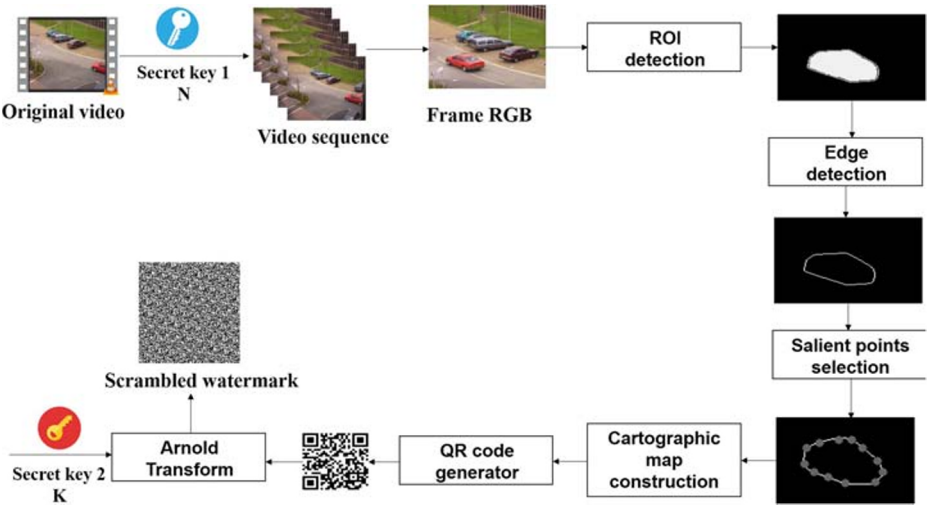


Fig. 6 The proposed watermark generation process flow chart

Then the extracted regions are exploited for the watermark construction strategy. First, the ROI extern contours are extracted. We select only salient points from moving objects edges in order to keep relevant information as well as to significantly minimize the computation time and enhance the watermark robustness. Indeed, salient points selection is done through Shi-Tomasi corner detector [66], which is resilient to several attacks. In our algorithm, the detected corner positions are considered as features. In fact, a cartographic map is constructed with the selected salient points coordinates. To provide additional security level to our system, the constructed map is processed as an input to a QR code generator. This contributes not only to enhance the security side of the system but also to conceal a large amount of information during a less embedding time. To further strengthen the security of the secret information to be hidden, the obtained QR code is encrypted using Arnold transform with a period K. Hence, this image scrambling technique ensures that the watermark extraction cannot be done without an accurate knowledge of the particular Arnold period K, which represents the second watermarking secret key in our approach. Finally, the scrambled version of the QR code is used as a watermark and hosted into the video frames.

4.3 Embedding process

As mentioned before, the host video is processed initially to be segregated into sequences of N gathered frames. All frames in each sequence are watermarked by a unique scrambled watermark, which is intrinsic to the given video sequence. The embedding process flow chart is shown in Fig. 7 and described in Algorithm 2. The RGB frame is first converted into YUV format as its components are less correlated than the RGB color space [20]. By virtue of the fact that it is better harmonized with human visual system (HVS), the luminance component Y is selected for the embedding process to strengthen the watermark imperceptibility. More precisely, the human eye is less sensitive to the luminance component Y compared to the chrominance components U and V [20].

The selected component is divided into several non-overlapping blocks of 4*4 size. The block size is chosen to maximize the number of bit to be inserted i.e., to guarantee a large

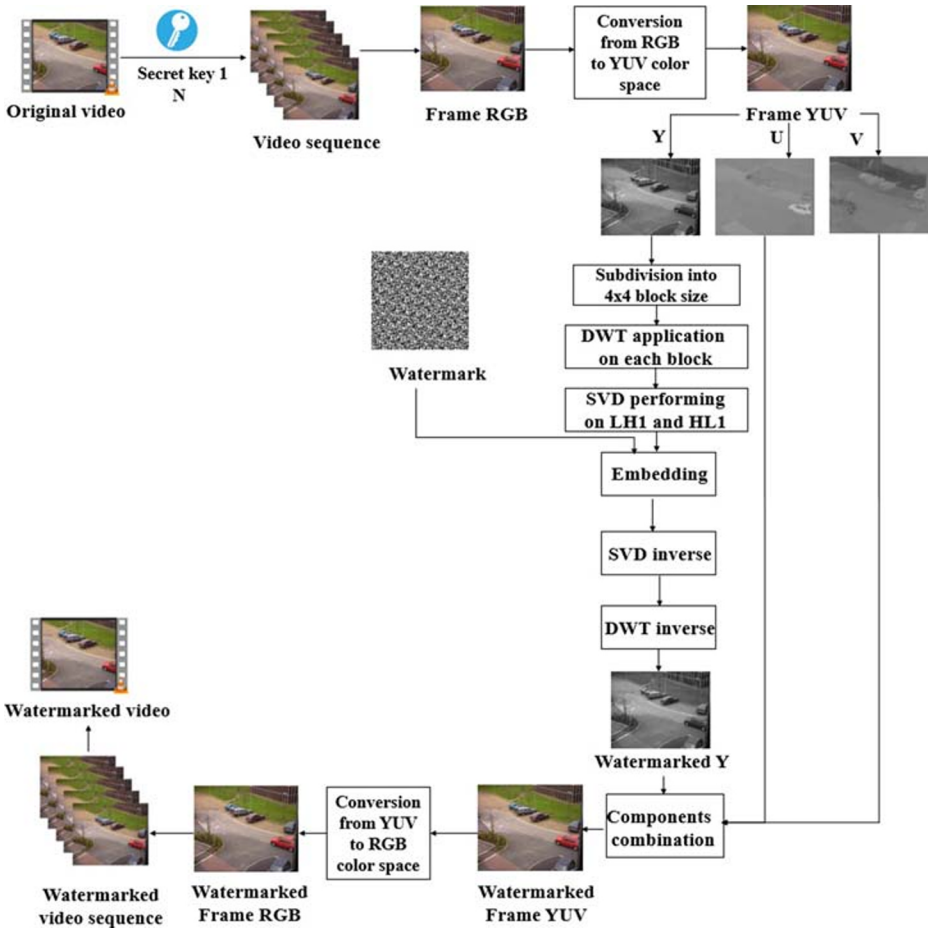


Fig. 7 The proposed watermark embedding process flow chart

capacity. Indeed, in every resulting block one bit will be concealed. Thereafter, each block is subjected to a single level discrete wavelet transform DWT. The DWT is solicited as a domain transformation technique thanks to its efficient resilience to noise addition. Moreover, it allows to more faithfully modeling the Human Visual System aspects than the other domain transformation techniques. Among the produced sub bands, only the mid frequency sub bands (LH1 and HL1) are selected as the best watermarking locus because they strike the correct trade-off between the imperceptibility and the robustness requirements. In fact, involving the low frequency sub-band (LL), which represents the most significant video frame parts, in the embedding process can increase the watermark robustness at the cost of the perceptual quality. Conversely, inserting the watermark within the high frequency sub-band (HH) guarantees a good imperceptibility but the secret embedded information risks to be lost during the compression processing since it refers to the least important information in the given video frame [46, 47].

Algorithm 2 Watermark embedding pseudo-code.

Input:
Seq: Original video sequence of N frames
W: Watermark
α, β: Watermarking factors
Output:
$Seq_{watermarked}$: Watermarked video sequence
begin
for i=1:N **do**
$RGBFrame \leftarrow Seq[i]$
$YUVFrame \leftarrow RGBtoYUV(RGBFrame)$
$Y \leftarrow getYComponent(YUVFrame)$
$index \leftarrow 0$
$Blocks \leftarrow BlocksDecomposition(Y)$
for b=1:size(Blocks) **do**
$block \leftarrow Blocks[b]$
$index \leftarrow index + 1$
$W_{embedding} \leftarrow W[index]$
$LL, HL, LH, LL \leftarrow DWT(block)$
if $index \leq \frac{length(W)}{2}$ **then**
$SelctedSubBand \leftarrow HL$
else
$SelctedSubBand \leftarrow LH$
end if
$U, S_{original}, V \leftarrow SVD(SelectedSubBand)$
$Fact_{\alpha} \leftarrow \frac{S_{original}(0,0)+S_{original}(1,1)}{\alpha}$
$Fact_{\beta} \leftarrow \frac{S_{original}(0,0)+S_{original}(1,1)}{\beta}$
if $W_{embedding} == 0$ **then**
$S_{original}(0,0) \leftarrow S_{original}(0,0) + Fact_{\alpha}$
$S_{original}(1,1) \leftarrow S_{original}(0,0)$
else
$S_{watermarked}(0,0) \leftarrow S_{original}(1,1) + Fact_{\beta}$
$S_{watermarked}(1,1) \leftarrow S_{original}(1,1)$
end if
$SelctedSubBand_{watermarked} \leftarrow U * S_{watermarked} * V^t$
if $index \leq \frac{length(W)}{2}$ **then**
$block_{watermarked} \leftarrow inverseDWT(LL, SelctedSubBand_{watermarked}, LH, HH)$
else
$block_{watermarked} \leftarrow inverseDWT(LL, HL, SelctedSubBand_{watermarked}, HH)$
end if
$Blocks_{watermarked}[b] \leftarrow block_{watermarked}$
end for
$Y_{watermarked} \leftarrow BlocksRecombination(Blocks_{watermarked})$
$YUVFrame_{watermarked} \leftarrow ComponentsRecombination(Y_{watermarked})$
$RGBFrame_{watermarked} \leftarrow YUVtoRGB(YUVFrame_{watermarked})$
$Seq_{watermarked}[i] \leftarrow RGBFrame_{watermarked}$
end for
end

Afterwards, the singular value decomposition is performed to the selected sub-bands. This operation yields 3 independent matrices namely U, S and V. Since S provides higher invisibility and more robustness against attacks as compared to the two obtained matrices U and V, it is particularly taken as the one to be watermarked. The watermark insertion is carried out by modifying the singular values of S matrices relative to the mid frequency sub-band HL1 and LH1 according to the bellow equations:

If $W_{embedding} = 0$

$$\begin{cases} S_{watermarked}(0,0) = S_{original}(0,0) + Fact_{\alpha} \\ S_{watermarked}(1,1) = S_{original}(0,0) \end{cases} \tag{5}$$

Else

$$\begin{cases} S_{watermarked}(0,0) = S_{original}(1,1) + Fact_{\beta} \\ S_{watermarked}(1,1) = S_{original}(1,1) \end{cases} \tag{6}$$

Where $W_{embedding}$ is the watermark bit, $S_{original}$ and $S_{watermarked}$ are respectively the original version of the singular value matrix and the watermarked one. $Fact_{\alpha}$ and $Fact_{\beta}$ are two scaling factors used for controlling the watermarked video visual quality as well as the watermark robustness. Their values, which depend on the coefficients of the original matrix S, are calculated using the following formulas.

$$Fact_{\alpha} = \frac{S_{original}(0,0) + S_{original}(1,1)}{\alpha} \tag{7}$$

$$Fact_{\beta} = \frac{S_{original}(0,0) + S_{original}(1,1)}{\beta} \tag{8}$$

Where α and β are two integer values.

Next, both singular value decomposition inverse and discrete wavelet transform inverse are applied to yield the watermarked luminance component Y. This latter is combined with the non watermarked chrominance components to obtain the watermarked RGB frame after re-converting the color space from YUV to RGB using (2).

The watermarked video is the result of the repetition of the above-described process to each frame in every sequence.

4.4 Detection process

Figure 8 illustrates the watermark detection general scheme that involves two processes: the regeneration process and the extraction one.

It claims that the detection is blind since only the watermarked video and the two secret keys N and K are required as the scheme inputs. The regeneration process is composed of the same steps used in the watermark generation process. The regenerated watermark is denoted by $W_{regenerated}$. In the other hand, the extraction process starts operating in analogy with the watermark embedding process as described in Algorithm 3. In fact, the watermarked video is subdivided into video sequences using the secret key N and a watermark is further extracted from each sequence. At first, a conversion from RGB to YUV color space is performed. Then the luminance component Y is decomposed to 4x4 non-overlapping blocks. After performing a single level DWT to each block, the singular value decomposition SVD is applied to the middle frequency sub bands LH1 and HL1. Finally, the hidden signature is

extracted from the singular values matrices coefficients based on the following rules:

$$\begin{cases} W_{extracted}(0,0) = 0 \quad If \quad S_{extracted}(0,0) - S_{extracted}(1,1) > \frac{Fact_\alpha + Fact_\beta}{2} \\ W_{extracted}(0,0) = 1 \quad Otherwise \end{cases} \tag{9}$$

Where $S_{extracted}$ is the extracted singular value matrix, $W_{extracted}$ is the extracted watermark bit, $Fact_\alpha$ and $Fact_\beta$ are the two scaling factors computed using (7) and (8) respectively.

Algorithm 3 Detection pseudo-code

Input:
$Seq_{watermarked}$: Watermarked video sequence of N frames
α, β: Watermarking factors
Output:
$W_{extracted}$: Extracted Watermark
$W_{regenerated}$: Regenerated Watermark
begin
for i=1:N **do**
$RGBFrame \leftarrow Seq_{watermarked}[i]$
if $i == 1$ **then**
$W_{regenerated} \leftarrow WatermarkGeneration(RGBFrame)$
end if
$YUVFrame \leftarrow RGBtoYUV(RGBFrame)$
$Y \leftarrow getYComponent(YUVFrame)$
$index \leftarrow 0$
$Blocks \leftarrow BlocksDecomposition(Y)$
for b=1:size(Blocks) **do**
$block \leftarrow Blocks[b]$
$index \leftarrow index + 1$
$LL, HL, LH, LL \leftarrow DWT(block)$
if $b \leq \frac{size(Blocks)}{2}$ **then**
$SelctedSubBand \leftarrow HL$
else
$SelctedSubBand \leftarrow LH$
end if
$U, S_{extracted}, V \leftarrow SVD(SelectedSubBand)$
$Fact_\alpha \leftarrow \frac{S_{extracted}(0,0) + S_{extracted}(1,1)}{\alpha}$
$Fact_\beta \leftarrow \frac{S_{extracted}(0,0) + S_{extracted}(1,1)}{\beta}$
if $S_{extracted}(0,0) - S_{extracted}(1,1) \geq \frac{Fact_\alpha + Fact_\beta}{2}$ **then**
$W_{extracted}[index] \leftarrow 0$
else
$W_{extracted}[index] \leftarrow 1$
end if
end for
end for
end

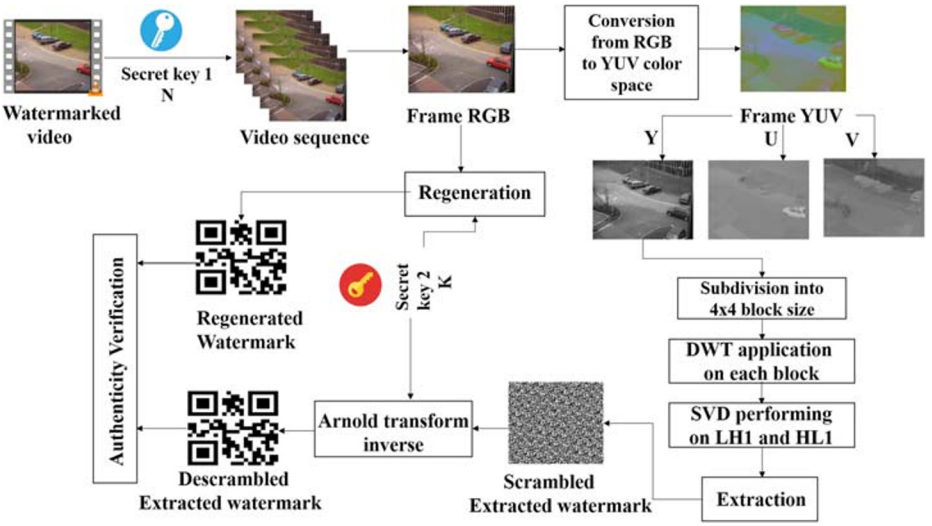


Fig. 8 The proposed watermark detection process flow chart

For tampering detection, the extracted watermark $W_{extracted}$ and the regenerated one $W_{regenerated}$ are compared. In fact, a mismatch between these two watermarks denotes an occurred alteration.

5 Experimental results

The proposed scheme is tested on various videos. The selected videos include at least one moving object and low to high movement activities amount. Details of videos for testing are indicated in Table 1. As depicted in this latter, these videos are test.avi, camera2.avi, video1.avi, foreman.avi, tempete.avi, table.avi and mobile.avi. The first three sequences belong to PETS benchmark datasets. However, the others videos are often used to evaluate previous existing works. The used videos, which hold on a different frames number, are distinguished by frame size as well as the frame per second (FPS) metric.

Table 1 Specifications of the used videos for simulation

	Specifications		
Videos	Frame size	Frame Per Second(FPS)	Total frames number
Test.avi	288×352	25	1452
Camera2.avi	288×352	25	2695
Video1.avi	240×320	25	223
Foreman.avi	176×144	30	294
Tempete.avi	352×288	30	60
Table.avi	352×240	25	100
Mobile.avi	352×288	25	100

The performance of the proposed watermarking system is assessed by analyzing its watermark capacity, imperceptibility and robustness. In the following, evaluation metrics used to measure these properties will be introduced and the obtained results will be displayed, discussed and compared to other existing approaches results.

5.1 Metrics

The watermark capacity is mostly quantified by the maximum number of bits that could be embedded in a given frame. According to our embedding algorithm, the watermark capacity C_{max} per frame is equal to the number of blocks resulting from the Y subdivision into 4×4-block size. Thus, it can be computed via the following equation:

$$C_{\max} = \frac{h \times w}{B_{size}} \tag{10}$$

Where h and w are respectively the height and the width of corresponding Y component and B_{size} presents the block size that is 4×4 in our work. The imperceptibility property is quantitatively scrutinized using Peak Signal to Noise Ratio (PSNR) as well as Structural Similarity index (SSIM) [35, 41]. While the robustness requirement is examined computing two metrics which are Normalized Correlation (NC) and Bit Error Ratio (BER) [20]. The PSNR allows checking the perceptual quality degradation of the watermarked video after the embedding process with references to the non-watermarked one. It is calculated by [31]:

$$PSNR = 20 \times \log \frac{2^d - 1}{\sqrt{\frac{1}{h \times w \times M} \times \sum_{i=0}^{h} \sum_{j=0}^{w} \sum_{k=0}^{c} (F(i,j) - F'(i,j))^2}} \tag{11}$$

Where F and F' are the original host frame and the watermarked one respectively with radiometric accuracy of d pixel and c channels. For RGB frame with 256 different gray levels, d and c values are 8 and 3 respectively. h and w are respectively the height and the width of corresponding frame.

The structural similarity index (SSIM) is used to find out the similarity between two images. This metric is based on neighboring pixel dependencies and it is computed using the following equation [31]:

$$SSIM = \frac{\sum_{j=0}^{c} (SSIM_{channel})}{3} \tag{12}$$

Where $SSIM_{channel}$ is structural similarity index per channel. It is defined as [37]:

$$SSIM_{channel} = \frac{(2\mu_x\mu_y + c)(2\sigma_{xy} + c_1)}{(\mu_x^2 + \mu_y^2 + c)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{13}$$

Where μ_x and μ_y are the average of intensities corresponding respectively to the original frame channel and the watermarked one, σ_x^2 and σ_y^2 are the variance of the intensities corresponding respectively to the original frame and the watermarked one and σ_{xy} is the covariance of original and watermarked frame, c_1 and c_2 are two factors used as division stabilizers.

Normalized Correlation (NC) measures the similarity between the original and the extracted watermarks. The NC value is derived by utilizing (14) given below [16]:

$$NC = \frac{\sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j)_{original} W(i,j)_{extracted}}{\sqrt{\sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j)^2_{original}}\sqrt{\sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j)^2_{extracted}}} \tag{14}$$

Where m and n are the watermark size. $W_{original}$ and $W_{extracted}$ are the original watermark and the extracted one respectively.

The bit error ratio evaluates the accuracy of watermark quantitatively. Hence, it refers to the number of bits received in error during the extraction process to the total number of bits in the extracted watermark. The BER value is calculated via the following formula [16]:

$$BER = \sum_{i=0}^{m}\sum_{j=0}^{n}\left(\frac{W(i,j)_{original} \oplus W(i,j)_{extracted}}{m \times n}\right. \tag{15}$$

Where, mxn is the total number of pixels of the watermark, $W_{original}$ and $W_{extracted}$ represent the original and the extracted watermark respectively and $\oplus$ is the exclusive OR operation.

For video, the PSNR, the SSIM as well as the NC and the BER values are computed as the average of their values in every video frame. For instance, the NC value of a video composed by frames is defined as:

$$NC_{video} = \frac{\sum_{i=0}^{N_F} NC_{F_i}}{N_F} \tag{16}$$

Where N_F is the total number of frames in the video. NC_{F_i} is the normalized correlation corresponding to the frame number i in the video.

5.2 Configuration of parameters used for experimentation

In our system, we have three parameters to be fixed. The first one is the frames number held in each video sequence, yielded after the host video split, already denoted by N and used as a first secret key. As highlighted before, this parameter value should be properly adjusted to ensure the watermark resilience to non malicious attacks. In order to avoid watermarking a large frames number with the same watermark, N is experimentally tuned to be as:

$$N = FPS - 5 \tag{17}$$

Where FPS denotes the frame per second metric.

Indeed, Table 2 provides resulting NC for different N values obtained in case of compression attack, which is the most important non-malicious manipulation, applied to several videos. It is clear that (17) allows obtaining the suitable N value that ensures the greater NC.

The two other factors are α and β, used in (7) and (8), which allow controlling the compromise between the watermark robustness and imperceptibility. Therefore, their suitable adjustment is crucial for the system efficiency. To this end, the PSNR is computed for different (α, β) values. According to the obtained results tabulated in Table 3, it is quite evident that the couple (2, 4) exhibits the best PSNR values. Consequently, $\alpha = 2$ and $\beta = 4$ are the considered values for the watermarking process.

Table 2 NC results for different N values under compression attack

Videos \ Attacks	5	10	15	**20**
Test	0.81299	0.82487	0.89579	**0.94797**
Camera2	0.79883	0.81274	0.89198	**0.95205**
Video1	0.88578	0.89641	0.94192	**0.96791**

Values in bold shows the best results of our proposed method

5.3 Capacity results

For each video, the capacity per frame C_{max} is calculated using the (10) and then the capacity per video is deduced by multiplying C_{max} by the number of frames in the given video. According to the obtained values represented in Table 4, it is noticeable that the proposed scheme proves its proficiency in terms of capacity. In fact, the subdivision of the luminance component Y to 4×4 non-overlapping blocks during the embedding process allows scatting a watermark with a large size in each frame.

5.4 Imperceptibility results

The proposed scheme perceptual quality is assessed through subjective and objective measures. For the subjective evaluation, non watermarked frames from some tested videos and their corresponding watermarked versions are shown in Fig. 9. It is clear that no visual artifacts can be observed between the original frames and the watermarked ones.

Concerning the objective evaluation, the different watermarked videos PSNR values are calculated and presented in Fig. 10. The resulting PSNR values exceeds 37 (dB) and reaches 47 (dB), which demonstrates that the proposed scheme preserves the watermarked video visual quality. For videos with different textures, the PSNR cannot be a compatible metric that faithfully reflects the visual quality. So, the SSIM is also employed as another objective metric since it is more accurate and consistent than PSNR. The Fig. 11 exhibits the resulting SSIM values that are approximately equal to 1. This confirms that both the host video and the watermarked one are entirely identical. Hence, based on the subjective as well as the objective evaluation, the watermark is visually transparent. Hence, the proposed scheme meets the watermarking system imperceptibility requirement. This high imperceptibility level is reached due to the selection of singular value matrix coefficients as watermark embedding holders.

Table 3 PSNR results for different (α, β) values

(α, β)	Test	Camera2	Video1	Foreman	Tempete	Table	Mobile
(2,3)	41.2887	47.0175	40.8068	37.1375	47.1993	45.7754	40.4928
(2.4)	**41.4720**	**47.2873**	**41.0848**	**37.3796**	**47.4229**	**46.0318**	**40.8082**
(3,4)	40.8062	46.6556	40.5494	37.0995	46.8126	45.3191	40.3261
(3,6)	40.9186	46.83	40.7324	37.3273	46.9562	45.4852	40.5391
(4,5)	40.4936	46.353	40.3238	36.9749	46.5382	44.9706	40.1111
(4,8)	40.5637	46.4663	40.4432	37.1347	46.6287	45.0835	40.2501
(5,6)	40.2871	46.1382	40.1581	36.8669	46.3478	44.7328	39.9423
(5,10)	40.3336	46.2163	40.2418	36.9814	46.4158	44.8112	40.0373

Values in bold shows the best results of our proposed method

Table 4 Capacity obtained for the used videos

Video name	Capacity per frame(bits)	Capacity per video(bits)
Test.avi	6336	9199872
Camera2.avi	6336	17075520
Video1.avi	4800	1070400
Foreman.avi	1584	465696
Tempete.avi	6336	380160
Table.avi	5280	528000
Mobile.avi	6336	633600

5.5 Robustness and fragility results

The proposed scheme effectiveness is evaluated against two attacks categories. The first group focuses on intentional tampering that seeks to change the video frame semantic content. The second set contains incidental attacks that preserve the frame semantics. The distinction between intentional and non-intentional modifications is achieved using a threshold. Since the robustness investigation is performed based on two metrics the NC and the BER, two different thresholds are considered and denoted by T_{NC} and T_{BER}. In this work, T_{NC} and T_{BER} are set to 0.9 and 0.1 respectively.

The set of incidental attacks holds the compression, additional noise attacks and finally brightness and contrast changing with moderate ratios. Experimental results presented in Tables 5 and 6 demonstrate that the detector is able to successfully retrieve the hidden watermark from the compressed watermarked videos. Indeed, the obtained NC values reach 0.9975 and BER values are close to 0. Obviously, the resulting NC and BER values are

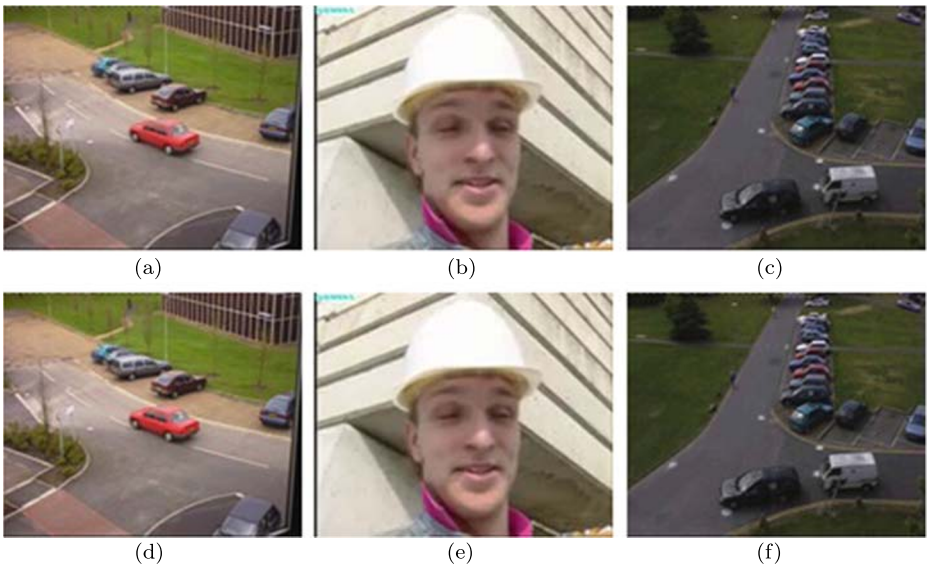


Fig. 9 *Up*: original frames **a** test.avi **b** foreman.avi **c** camera2.avi, *Down*: watermarked frames: **d** test.avi **e** foreman.avi **f** camera2.avi

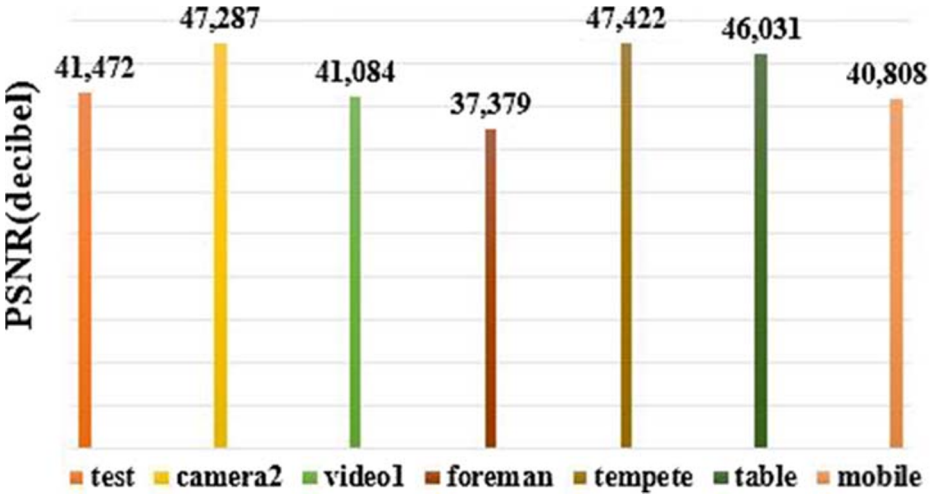


Fig. 10 Obtained PSNR values of various watermarked videos

respectively above and below their thresholds, which indicates that no malicious distortion has occurred. This high resilience level is provided thanks to the selection of the mid frequency sub bands of the discrete wavelet transform as locations for the watermark embedding. This choice allows avoiding a potential information loss during compression process.

Furthermore, the proposed watermarking system robustness is investigated in the presence of Gaussian noise and salt and pepper attacks. As well seen from simulation results tabulated in Table 5, the minimum obtained NC is 0.92471 after adding white Gaussian noise of mean zero and standard variances and 0.95386 after conducting salt and peppers attack. As shown in Table 6, the maximum BER is below 0.1. The above results indicate that the procured NC values are superior to the relative threshold T_{NC} and the BER values

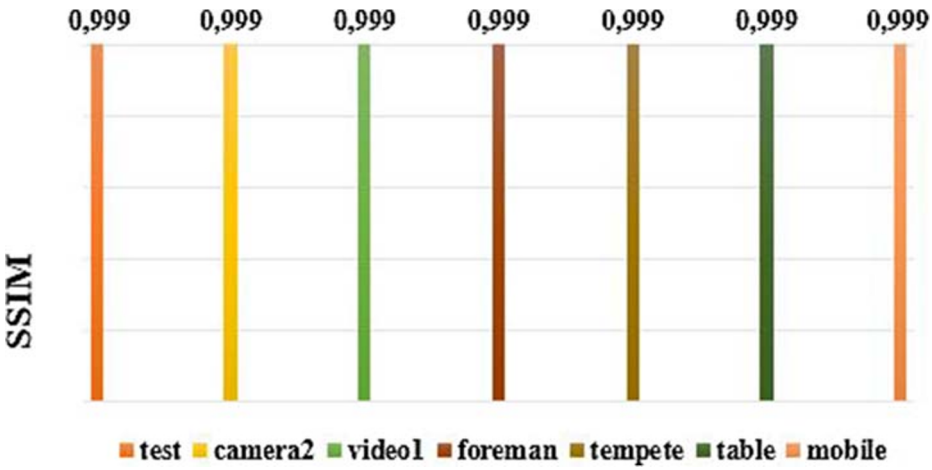


Fig. 11 Obtained SSIM values of various watermarked videos

Table 5 NC values obtained for the used videos under non-intentional manipulations

Attacks / Videos	Compression	Salt& pepper	Gaussian noise (0.01)	Gaussian noise (0.05)	Gaussian noise (0.1)
Test	0.94797	0.98842	0.97722	0.95960	0.95686
Camera2	0.95205	0.97607	0.97979	0.95169	0.95508
Video1	0.96791	0.99229	0.98408	0.96705	0.95979
Foreman	0.9975	1	0.96674	0.95956	0.95456
Tempete	0.95284	0.95487	0.95634	0.95337	0.95322
Table	0.92113	0.95386	0.93581	0.92672	0.92471
Mobile	0.96777	0.97325	0.96977	0.96620	0.96506

do not exceed the T_{BER}. Hence, the watermark can be correctly extracted after applying white Gaussian noise and salt and pepper to all the watermarked video frames. Using the discrete wavelet transform that is immune to noise adding, improves the robustness of the scheme against these two manipulations. Analyzing the results presented in Table 7, it can be noticed that the proposed technique efficiently survives the adjustment of both brightness and contrast since the obtained NC and BER values are respectively above and below their predefined thresholds. In fact, using moderate ratios does not affect the frame semantic content.

The effectiveness of the proposed watermarking scheme is assessed against intentional manipulations namely: rotation, cropping, filtering, object removing, object insertion and high variation of brightness and contrast level.

First, each frame is rotated by different angles. It is observed from Tables 8 and 9 that BER varies between 0.46031 and 0.51988 and NC is ranged between 0.65343 and 0.71645 for all tested videos when varying the rotation degree from 5 to 90 with a step of 5. From these results, it is clear that NC is inferior than 0.9 and BER is superior than 0.1. Hence, we conclude that the watermarked video is deliberately tampered.

In addition to rotation, the tested videos are subjected to cropping with different window sizes. Results are depicted in Table 10. In this case, the maximum NC and the minimum BER are 0.70400 and 0.46938 respectively. From these results, it is noticed that the detector fails in recovering the embedded watermark since the achieved BER values are extremely above the threshold 0.1 and NC values are below the relative threshold 0.9. Afterward, sensitivity to frame filtering is tested. Therefore, watermarked video frames are subjected to

Table 6 BER values obtained for the used videos under non-intentional manipulations

Attacks / Videos	Compression	Salt& pepper	Gaussian noise (0.01)	Gaussian noise (0.05)	Gaussian noise (0.1)
Test	0.05496	0.01143	0.02326	0.04322	0.04655
Camera2	0.05027	0.02418	0.02041	0.05110	0.04732
Video1	0.03265	0.00752	0.01605	0.03540	0.04395
Foreman	0.0009	0	0.03508	0.04294	0.04883
Tempete	0.04988	0.04761	0.04648	0.04988	0.04988
Table	0.09977	0.05102	0.07596	0.09183	0.09467
Mobile	0.03344	0.02721	0.03117	0.03514	0.03628

Table 7 NC and BER values obtained for the used videos under brightness and contrast adjustment

Videos	Tempete		Table		Mobile	
Metrics / Attacks	NC	BER	NC	BER	NC	BER
Brightness(+10 %)	0.96300	0.03854	0.96728	0.03401	0.97917	0.02097
Brightness(+20 %)	0.96300	0.03854	0.96728	0.03401	0.97917	0.02097
Brightness(−10 %)	0.96300	0.03854	0.96728	0.03401	0.97917	0.02097
Brightness(−20 %)	0.96301	0.03860	0.96728	0.03401	0.97917	0.02097
Contrast(x2)	0.96301	0.03860	0.96728	0.03401	0.97917	0.02097
Contrast(x0.5)	0.96301	0.03860	0.96728	0.03401	0.97917	0.02097

Table 8 NC values obtained after rotation attack

Rotation degree	Test	Camera2	Video1	Foreman	Tempete	Table	Mobile
5	0.67547	0.68218	0.68184	0.70217	0.70774	0.70636	0.69160
10	0.67736	0.68770	0.68191	0.70542	0.70049	0.70546	0.69345
15	0.67468	0.68097	0.68360	0.70536	0.69929	0.70258	0.68507
20	0.67685	0.68153	0.67399	0.70541	0.70097	0.70505	0.69342
25	0.68125	0.68811	0.67560	0.70265	0.70592	0.70817	0.69602
30	0.68646	0.67936	0.66746	0.70665	0.70177	0.70424	0.68717
35	0.65762	0.67615	0.66185	0.69782	0.70773	0.69906	0.69795
40	0.66031	0.67930	0.67006	0.70772	0.70531	0.70221	0.69277
45	0.65343	0.66954	0.66580	0.70512	0.70652	0.68348	0.68859
90	0.68387	0.69145	0.68544	0.70817	0.71645	0.70111	0.69240

Table 9 BER values obtained after rotation attack

Rotation degree	Test	Camera2	Video1	Foreman	Tempete	Table	Mobile
5	0.50963	0.51133	0.50938	0.47796	0.46825	0.47392	0.49149
10	0.51452	0.51091	0.50619	0.47571	0.48752	0.48639	0.49093
15	0.51720	0.51540	0.50504	0.47941	0.48185	0.49206	0.50340
20	0.51757	0.51308	0.51561	0.48470	0.47959	0.48639	0.48809
25	0.50766	0.50681	0.50910	0.49176	0.47505	0.47902	0.49093
30	0.50625	0.51184	0.51293	0.48329	0.47505	0.48412	0.49886
35	0.51988	0.51739	0.51050	0.49423	0.46371	0.48582	0.48129
40	0.51532	0.51154	0.49283	0.47911	0.46145	0.47619	0.48469
45	0.51347	0.51073	0.50213	0.48122	0.46258	0.49149	0.48582
90	0.50418	0.51126	0.49380	0.47759	0.46031	0.49149	0.49943

Table 10 NC and BER values obtained for the used videos under cropping attack

Size	[10×10]		[40×40]		[100×100]	
Metrics / Videos	NC	BER	NC	BER	NC	BER
Test	0.66212	0.49353	0.68870	0.50429	0.69464	0.50583
Camera2	0.65978	0.49947	0.69333	0.50803	0.69655	0.50717
Video1	0.65748	0.49390	0.67713	0.51388	0.69428	0.50102
Foreman	0.69335	0.48597	0.70400	0.49788	0.70286	0.50573
Tempete	0.68209	0.46938	0.70344	0.48185	0.69732	0.50793
Table	0.67167	0.47789	0.69164	0.50737	0.69607	0.50680
Mobile	0.67890	0.47222	0.70300	0.49433	0.69577	0.51473

median filter with median radius of 2×2 and 3×3. The NC and BER values corresponding to these manipulations are given in Figs. 12 and 13. It is observed that the BER values are greater than 0.4 and attain 0.51528. In addition, NC values lie between 0.68971 and 0.72964. By comparing these results to the preset thresholds $T_{NC} = 0.9$ and $T_{BER} = 0.1$, it is evident that the watermarked videos are regarded as non-authentic.

The next considered malicious attacks are object deletion and insertion. These two attacks are among the common tampering that must be detectable by an efficient semi-fragile watermarking scheme notably in video surveillance context. Therefore, an object is intentionally removed from watermarked frames of randomly selected sequences of the test videos. To provide a better illustration, Fig. 14 depicts an example of a watermarked frame and its maliciously tampered version from a used video. The resulting values of the two authentication metrics BER and NC relative to the test.avi and camera2.avi videos are respectively presented in Tables 11 and 12. As we can see from these results, the minimum BER is higher than the threshold 0.1, and the maximum NC is lower than the preset threshold 0.9 for the two considered videos. Therefore, the watermarking scheme proves its ability to successfully detect these malicious tampering attacks. Likewise, to test object insertion

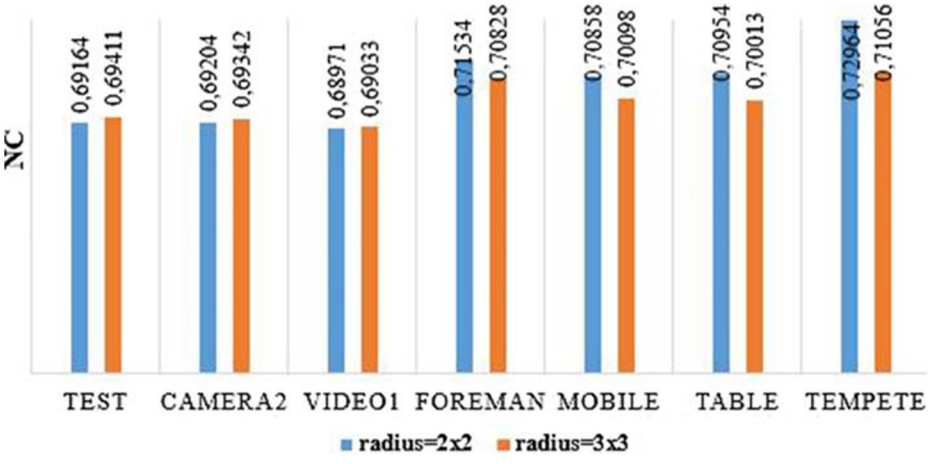


Fig. 12 NC values obtained for the used videos after median filtering attack

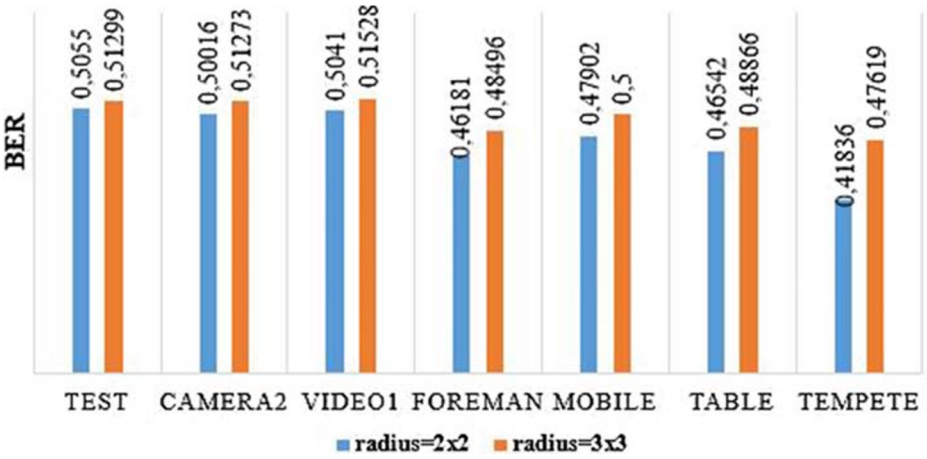


Fig. 13 BER values obtained for the used videos after median filtering attack

Fig. 14 test.avi video: **a** watermarked frame **b** attacked frame after object insertion **c** attacked frame after object deletion

Table 11 NC and BER values obtained for test.avi under object deletion attack

Seq. Index	NC	BER
7	0.64372	0.35671
8	0.68762	0.30240
10	0.67791	0.30560
19	0.47626	0.47165
20	0.46890	0.51927
22	0.47161	0.48979
30	0.62476	0.36147
41	0.62823	0.36028
72	0.47636	0.47845

Table 12 NC and BER values obtained for camera2.avi under object deletion attack

Seq. Index	NC	BER
27	0.48165	0.37120
29	0.47289	0.37098
30	0.47530	0.36147
42	0.51681	0.33760
45	0.48354	0.50793
46	0.64559	0.34080
86	0.49604	0.55102
87	0.46844	0.52154
111	0.47434	0.51247

attack, watermarked frames of arbitrarily chosen sequences are corrupted by introducing an external object to their visual content as shown in Fig. 14. The obtained BER values show high values contrary to NC that exhibit low values as we can see from Tables 13 and 14, which summarizes the resulting measurements values relative to the two previously used videos. Thus, the watermarked videos are deemed as maliciously attacked.

Finally, the fragility of the proposed scheme to brightness change and contrast adjustment with high variation ratios is checked. Unlike brightness and contrast varying with moderate ratios, these types of modifications are identified as malicious because they permit the attacker to hide several semantic details from frames. Figure 15 displays example of watermarked frames after being attacked by strongly increasing and decreasing the luminance and the contrast levels. The BER and NC values tabulated in Table 15 indicate that the videos are unauthentic for the different ratios. Again, the detector properly identifies the intentional tampering.

5.6 Comparison of our proposed scheme with existing authentication approaches

The proposed technique performances are compared to the existing works presented in [10, 19, 29, 56, 65, 73] with respect to watermark capacity, imperceptibility and robustness. As previously described in Section 3, [10, 19, 29] are mono frequency domain approaches

Table 13 NC and BER values obtained for test.avi under object insertion attack

Seq. Index	NC	BER
7	0.62816	0.36266
17	0.62969	0.36320
19	0.53038	0.50113
21	0.49277	0.53741
27	0.65422	0.32937
31	0.67218	0.32000
43	0.60585	0.37931
52	0.49270	0.48526
60	0.49014	0.51020

Table 14 NC and BER values obtained for camera2.avi under object insertion attack

Seq. Index	NC	BER
23	0.44379	0.51020
26	0.50754	0.36640
27	0.45734	0.38400
29	0.48206	0.34720
42	0.51681	0.33760
44	0.50762	0.50793
46	0.48451	0.36644
110	0.54194	0.50113
127	0.59632	0.37928

involving DCT, QDCT and LWT respectively. Nonetheless, our proposed scheme as well as the ones presented in [56, 65, 73] carry out in the multi frequency domain. In fact, our technique and [65] jointly involve the SVD and the DWT for the watermarking. However, [56, 73] use the combinations (DWT,PCA) and (SVD, MR-SVD) respectively. The comparative comparison between the proposed method and [19] is provided in Tables 16 and 17. This latter demonstrates a comparison in terms of robustness while Table 16 depicts a comparison in terms of capacity and imperceptibility requirements. Referring to Table 17, it can be seen that our scheme, which exhibits the lowest BER values, performs better than the method in [19] under Gaussian noise, salt and pepper, compression and brightness variation attacks. Similarly, the values of the quality measure PSNR illustrated in Table 16 indicate that our technique noticeably outperforms the watermarking technique [19] with respect to capacity and imperceptibility requirements. Indeed, the proposed scheme provides a PSNR average equals to 47.727 db while offering a watermarking capacity 4 times greater than the aforementioned method one. This demonstrates that the watermark embedding holders in our work are selected correctly and ensure a good watermarked video quality despite the high capacity.

The comparison between our scheme and those in [10, 29, 56, 65, 73] is given in Tables 18 and 19. Analyzing this latter, it can be seen that our scheme robustness against Gaussian noise attack is superior to those in [10, 29, 56, 73]. However, the method in [65] provides a NC value which is slightly better than our approach. From Table 19, it is well proven that our technique and the ones [10, 29, 56, 65] are resilient to salt and pepper attack.

(a) (b) (c)

Fig. 15 test.avi: video **a** watermarked frame **b** attacked frame after brightness increasing **c** attacked frame after brightness decreasing

Table 15 NC and BER values obtained for the used videos under brightness and contrast varying attacks with high ratios

Videos	Test		Camera2		Video1	
Metrics / Attacks	NC	BER	NC	BER	NC	BER
Brightness(+80 %)	0.73588	0.25342	0.78163	0.21808	0.70928	0.43704
Brightness(+100 %)	0.71475	0.27813	0.74990	0.24784	0.70399	0.47024
Brightness(−80 %)	0.74618	0.25027	0.72288	0.26781	0.74409	0.25176
Brightness(−90 %)	0.69872	0.46339	0.69865	0.49453	0.69765	0.50141
Contrast(x10)	0.69840	0.45310	0.70270	0.46808	0.69765	0.50141
Contrast(x20)	0.69858	0.46182	0.69849	0.49461	0.69765	0.50141
Contrast(x0.1)	0.72487	0.31141	0.75991	0.30577	0.80773	0.20204
Contrast(x0.05)	0.71301	0.35716	0.73161	0.37003	0.76570	0.28232

Table 16 Capacity and imperceptibility comparison between our method and the work proposed in [19]

	[19]			Our approach		
	Tempete	Table	Mobile	Tempete	Table	Mobile
Watermark capacity	1584	1320	1584	6336	5280	6336
Watermarked video PSNR	34.475	34.111	40.808	47.722	46.726	–

Table 17 Robustness comparison between our method and the scheme proposed in [19] (BER)

	Tempete		Table		Mobile	
Attacks	[19]	Our approach	[19]	Our approach	[19]	Our approach
Gaussian noise(0.01)	0.0724	0.0464	0.0886	0.0759	0.0719	0.0311
Gaussian noise(0.02)	0.0876	0.0487	0.1057	0.0821	0.0923	0.0351
Compression	0.1772	0.0498	0.1373	0.0997	0.1636	0.0334
Brightness(+10 %)	0.0603	0.0385	0.0921	0.0340	0.0660	0.0209
Brightness(+20 %)	0.0697	0.0385	0.0959	0.0340	0.0678	0.0209

Table 18 Capacity and imperceptibility comparison for Foreman video between our method and the works proposed in [10, 56, 65, 73] and [29]

	[56]	[10]	[73]	[65]	[29]	Our approach
Watermark capacity	90	99	–	–	–	1584
Watermarked video PSNR	41.83	40.2	45.41	35.03	43.06	37.45

Table 19 Robustness comparison for Foreman video between our method and the works proposed in [10, 56, 65, 73] and [29] (NC)

Attacks	[56]	[10]	[73]	[65]	[29]	Our approach
Gaussian noise	0.9008	0.8105	0.5625	0.979	0.928	0.9667
Salt & pepper	1	0.921	–	0.9636	0.998	1
Compression	0.8485	0.9980	0.8809	0.9857	0.928	0.9975
Contrast adjustment	–	–	0.7363	0.9732	–	0.9748

Both our method and the scheme presented in [56] ensure the best performance. Regarding the compression, the scheme introduced in [10] and the proposed one show a comparable robustness level. However, the methods presented in [56, 73] provide a poor resilience to this attack. From the same table, it can be inferred that our technique is more robust to contrast adjustment than the methods in [65, 73].

As far as imperceptibility is concerned, the watermarking approaches in [10, 29, 56, 73] are more imperceptible than the proposed one because the capacity in the present scheme is noticeably high in comparison with the methods [10] and [56] as shown in Table 18. Besides, the two previously cited approaches and the ones introduced in [29, 73] use a watermark holders selection strategies. Consequently, the video perceptual quality is slightly affected since very few frames or blocks are chosen for the watermark embedding process and remaining frames and blocks are unused. Moreover, the proposed method exhibits a better imperceptibility level compared to [65] as shown in Table 18.

6 Conclusion and future works

In this paper, a blind semi fragile watermarking scheme for video content authentication in the multi SVD-DWT domain was proposed. The scheme starts operating with a watermark generation process that is built based on extracted features from regions of interest and QR code technique. After being encrypted by Arnold transform, the authentication watermark is embedded into the singular value matrix coefficients relative to the mid frequency sub-bands of the discrete wavelet transform. Involving these sub-bands in the watermarking allows lessening the visual degradation effect while ensuring a high resilience to common image processing attacks. On the verification side, a blind detection is performed for extracting the hidden watermark that is compared to the regenerated one in order to detect occurred forgeries. Results of simulation experiments, which are conducted on various surveillance videos as well as standard ones, show that the proposed semi-fragile watermarking scheme has the ability to differentiate intentional attacks from non-intentional ones. In fact, achieved NC and BER values, which are above 0.9 and below and 0.1 respectively, prove that our detector withstands moderate content preserving modifications such as common image processing. However, it exhibits a high fragility to semantic content changing alterations such as cropping and objects manipulations by providing NC and BER values extremely inferior and superior to 0.9 and 0.1 respectively. Moreover, the proposed scheme successfully satisfies the trade-off between the capacity and the imperceptibility by achieving a large capacity within a negligible perceptual quality compromising as shown by the obtained PSNR and SSIM high values. The future work may focus on tampering localization and self-recovery, which consists in recovering the original content within the tampered areas. In addition,

the proposed watermarking scheme fragility to spatio-temporal attacks can be improved by exploiting other pertinent features during the watermark generation process.

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

Compliance with Ethical Standards

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Abood OG, Guirguis SK (2018) A survey on cryptography algorithms. Int J Sci Res Publ 8(7):495–512
2. Agarwal P, Choudhary A (2014) Protecting video data through watermarking: a comprehensive study. In: 5th international conference-confluence the next generation information technology summit, pp 657–662
3. Ait Sadi K, Guessoum A, Bouridane A, Khelifi F (2016) Content fragile watermarking for H.264/AVC video authentication. Int J Electron 104(4):673–691
4. Alenizi F, Kurdahi F, Eltawil A, Aljumah A (2015) DWT-Based watermarking technique for video authentication. In: International conference on electronics, circuits, and systems (ICECS), pp 41–44
5. Asikuzzaman M, Pickering MR (2018) An overview of digital video watermarking. IEEE Trans Circ Sys Video Technol 28(9):2131–2153
6. Bartolini F, Tefas A, Barni M, Pitas I (2001) Image authentication techniques for surveillance applications. Proc IEEE 89(10):1403–1418
7. Ben Hamida A, Koubaa M, Nicolas H, Ben Amar C (2013) Video pre-analyzing and coding in the context of video surveillance applications. In: International conference on multimedia and expo workshops (ICMEW), pp 1–4
8. Ben Hamida A, Koubaa M, Nicolas H, Ben Amar C (2014) Toward scalable application-oriented video surveillance systems. In: Science and information conference, pp 384–388
9. Ben Hamida A, Koubaa M, Nicolas H, Ben Amar C (2016) Video surveillance system based on a scalable application-oriented architecture. Multimed Tools Appl 75(24):17187–17213
10. Bhardwaj A, Verma VS, Jha RK (2018) Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform. Multimed Tools Appl 77(15):19659–19678
11. Boreiry M, Keyvanpour MR (2017) Classification of watermarking methods based on watermarking approaches. In: Artificial intelligence and robotics (IRANOPEN), pp 73–76
12. Bouchrika T, Zaied M, Jemai O, Ben Amar C (2012) Ordering computers by hand gestures recognition based on wavelet networks. In: 2nd International Conference on Communications Computing and Control Applications (CCCA), pp 36–41
13. Chang Y-C, Wang J-T, Chang Y-T, Yu S-S (2016) An error-detecting code based fragile watermarking scheme in spherical coordinate system. In: International symposium on computer, consumer and control (IS3C), pp 287–290
14. Chaudhary S, Berki E, Nykanen P, Zolotavkin Y, Helenius M, Kela J (2016) Towards a conceptual framework for privacy protection in the use of interactive 360 video surveillance. In: 22nd international conference on virtual system & multimedia (VSMM), pp 1–10
15. Charfeddine M, El'Arbi M, Ben Amar C, Ben Amar C (2014) A new DCT audio watermarking scheme based on preliminary MP3 study. Multimed Tools Appl 70(3):1521–1557
16. El'Arbi M, Koubaa M, Charfeddine M, Ben Amar C (2011) A dynamic video watermarking algorithm in fast motion areas in the wavelet domain. Multimed Tools Appl 55(3):579–600
17. El'Arbi M, Ben Amar C, Nicolas H (2006) In: IEEE International Conference on Multimedia and Expo (ICME), pp 1577–1580
18. Deljavan Amiri D, Amiri A, Meghdadi M (2019) HVS-Based scalable video watermarking. Multimedia Systems 25(3):1–19
19. Farfoura ME, Horng S-J, Guo JM (2016) Low complexity semi-fragile watermarking scheme for H.264/AVC authentication. Multimed Tools Appl 75(13):7465
20. Hammami A, Ben Hamida A, Ben Amar C (2019) 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

21. Hammami A, Ben Hamida A, Ben Amar C, Nicolas H (2020) Regions based semi-fragile watermarking scheme for video authentication. In: International conference in Central Europe on computer graphics, visualization and computer vision, pp 96–104
22. Hasnaoui M, Mitrea M (2012) Semi-fragile watermarking for video surveillance applications. In: 20th European signal processing conference (EUSIPCO), pp 1782–1786
23. Himeur Y, Boukabou A (2018) A robust and secure key-frame based video watermarking system using chaotic encryption. Multimed Tools Appl 77(7):8603–8627
24. IHS Web page. [Online]. Available: https://technology.ihs.com
25. ISO 18004 Web page. [Online]. Available: https://www.iso.org/standard/62021.html
26. Jenkins N (2015) 245 million video surveillance cameras installed globally in 2014 [Online]. Available: https://technology.ihs.com/532501/245-million-video-surveillance-cameras-installed-globally-in-2014
27. Jindal H, Kasana SS, Saxena S (2016) A novel image zooming technique using wavelet coefficients. In: Proceedings of the international conference on recent cognizance in wireless communication and image processing, pp 1–7
28. Jindal H, Kasana SS, Saxena S (2018) Underwater pipelines panoramic image transmission and refinement using acoustic sensors. International Journal of Wavelets, Multiresolution and Information Processing 16(01):1850013
29. Joshi AM, Mishra V, Patrikar RM (2016) FPGA prototyping of video watermarking for ownership verification based on H.264/AVC. Multimed Tools Appl 75(6):3121
30. Joshi AM, Gupta S, Girdhar M, Agarwal P, Sarker R (2017) Combined DWT-DCT-based video watermarking algorithm using arnold transform technique. In: International conference on data engineering and communication technology, pp 455–463
31. Jumana W, Huang Dong J, Sarah S, Saad H, Hiyam H (2015) An immune secret QR-code sharing based on a twofold zero watermarking scheme. International Journal of Multimedia and Ubiquitous Engineering 1(4):399–412
32. Kalker T, Depovere G, Haitsma J, Maes MJ (1999) Video watermarking system for broadcast monitoring. In: The international society for optical engineering, pp 103–112
33. Kaur S, Jindal H (2017) Enhanced image watermarking technique using wavelets and interpolation. Int J Image Graph Signal Process 9(7):23–35
34. Kaur G, Kasana SS, Sharma MK (2019) An efficient authentication scheme for high efficiency video coding/H.265. Multimed Tools Appl 78(15):21245–21271
35. Khosravi MR, Yazdi M (2018) A lossless data hiding scheme for medical images using a hybrid solution based on IBRW error histogram computation and quartered interpolation with greedy weights. Neural Comput Appli 30:2017–2028
36. Khosravi MR, Samadi S (2019) Reliable data aggregation in internet of ViSAR vehicles using chained dual-phase adaptive interpolation and data embedding. IEEE Internet of Things Journal 7(4):2603–2610
37. Khosravi MR, Samadi S (2019) Efficient payload communications for IoT-enabled ViSAR vehicles using discrete cosine transform-based quasi-sparse bit injection. EURASIP J Wirel Commun Netw 2019:262
38. Khosravi MR, Samadi S (2019) Modified data aggregation for aerial viSAR sensor networks in transform domain. In: 25th international conference on parallel and distributed processing techniques and applications (PDPTA), pp 87–90
39. Kim C, Shin D, Leng L, Yang C-N (2018) Separable reversible data hiding in encrypted halftone image. Displays 55:71–79
40. Kim C, Shin D, Leng L, Yang CN (2018) Lossless data hiding for absolute moment block truncation coding using histogram modification. J Real-Time Image Proc 14(1):101–114
41. Kim C, Yang CN, Leng L (2020) High-capacity data hiding for ABTC-EQ based compressed image. Electronics 9:644
42. Kirovski D, Malvar H, Yacobi Y (2002) Multimedia content screening using a dual watermarking and fingerprinting system. In: ACM international conference on multimedia, pp 372–381
43. Koohpayeh T, Abd A, Kohpayeh S (2018) A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Syst Appl 112(1):208–228
44. Koubaa M, Elarbi M, Ben Amar C, Nicolas H (2012) Collusion, MPEG4 compression and frame dropping resistant video watermarking. Multimed Tools and Appl 56(2):281–301
45. Kumar S, Kumar M, Budhiraja R, Das MK, Singh S (2018) A cryptographic model for better information security. J Inf Secur Appl 43:123–138
46. Leng L, Zhang JS, Khan MK, Chen X, Alghathbar K (2010) Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain. Int J Phys Sci 5(17):2543–2554

47. Leng L, Li M, Kim C, Bi K (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. Multimed Tools Appl 76:333–354
48. Li L, Li X, Qiao T, Xu X, Zhang S, Chang CC (2018) A novel framework of robust video watermarking based on statistical model. In: International conference cloud computing and security (ICCCS), pp 160–172
49. Li J, Li X, Guo Y, Xu X, Liu S (2018) Semi-fragile video watermarking algorithm based on energy relation. In: International conference on virtual reality (ICVR), pp 95–101
50. Liao X, Li K, Yin J (2017) Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform. Multimed Tools Appl 76:20739–20753
51. Liao X, Qin Z, Ding L (2017) Data embedding in digital images using critical functions. Signal Process Image Commun 58:146–156
52. Liu L, Li X (2010) Watermarking protocol for broadcast monitoring. In: International conference on E-business and E-government, pp 1634–1637
53. Mander K, Jindal H (2017) An improved image compression decompression technique using block truncation and wavelets. Int J Image Graph Signal Proc 9(8):17–29
54. Mishra A, Agarwal C, Chetty G (2018) Lifting wavelet transform based fast watermarking of video summaries using extreme learning machine. In: International joint conference on neural networks, pp 1–7
55. Mittal A, Jindal H (2017) Novelty in image reconstruction using dwt and clahe. Int J Image Graph Signal Proc 9(5):28–34
56. Nouioua I, Amardjia N, Belilita S (2018) A novel blind and robust video watermarking technique in fast motion frames based on SVD and MR-SVD. Security and Communication Networks 2018(10):1–17
57. Othmani M, Bellil W, Alimi A.M. (2010) A new structure and training procedure for multi-mother wavelet networks. Int J Wavelets Multiresolut Inf Process 8(1):149–175
58. Panyavaraporn J (2017) DWT/DCT watermarking techniques with chaotic map for video authentication. In: Ninth international conference on digital image processing (ICDIP)
59. Ponnisathya S, Ramakrishnan S, Dhinakaran S, Ashwanth PS, Dhamodharan P (2017) CHAOTIC map based video watermarking using DWT and SVD. In: International conference on inventive communication and computational technologies, pp 45–49
60. Preda RO, Vizireanu N (2011) New robust watermarking scheme for video copyright protection in the spatial domain. UPB Sci Bull 73(1):93–104
61. Priya P, Tanvi G, Nikita P, Ankita T (2014) Digital video watermarking using modified LSB and DCT technique. Int J Res Eng Technol 4(3):630–634
62. Rafik H (2017) A novel pseudo random sequence generator for image-cryptographic applications. J Inf Secur Appl 35:119–127
63. Sadek RA (2012) SVD based image processing applications: state of the art, contributions and research challenges. Int J Adv Comput Sci Appl 3(7):26–34
64. Saikrishna N, Resmipriya MG (2016) An invisible logo watermarking using arnold transform. In: International conference on advances in computing & communications (ICACC), pp 808–815
65. Sathya SPA, Ramakrishnan S (2018) Fibonacci based key frame selection and scrambling for video watermarking in DWT-SVD domain. Wirel Pers Commun 102:2011–2031
66. Shi J, Tomasi C (1994) Good features to track. In: Conference on computer vision and pattern recognition, pp 593–600
67. Shukla D, Sharma M (2018) A novel scene-based video watermarking scheme for copyright protection. J Intell Syst 27(1):47–66
68. Stauffer C, Grimson WEL (1999) Adaptive background mixture models for real-time tracking. In: Computer society conference on computer vision and pattern recognition, pp 246–252
69. Sujatha CN, Sathyanarayana P (2019) DWT-based blind video watermarking using image scrambling technique. In: Information and communication technology for intelligent systems, pp 621–628
70. Swaraja K, Karuna G, Kora P, Meenakshi K (2019) Video watermarking fundamentals and overview. In: International conference on intelligent computing and communication technologies (ICICCT), pp 379–385
71. Tyagi S, Singh HV, Agarwal R, Gangwar SK (2016) Digital watermarking techniques for security applications. In: International conference on emerging trends in electrical electronics & sustainable energy systems (ICETEESES), pp 379–382
72. Upadhy S, Singh SK (2011) Video authentication- an overview. Int J Comput Sci Eng Surv 2(4):75–96
73. Yassin NI, Salem NM, Adawy MIE (2014) QIM Blind video watermarking scheme based on wavelet transform and principal component analysis. Alex Eng J 53(4):833–842
74. Yu X-Y, Wang C-Y, Zhou X (2018) A survey on robust video watermarking algorithms for copyright protection. Appl Sci 8(10):1891

75. Zhang D, Li Y (2010) A non-blind watermarking on 3D model in spatial domain. In: International conference on computer application and system modeling, pp 267–269
76. Zebbiche K, Ghouti L, Khelifi F, Bouridane A (2006) Protecting fingerprint data using watermarking. In: NASA/ESA conference on adaptive hardware and systems, pp 451–456