manuscript No.
(will be inserted by the editor)

A new efficient anaglyph 3D image and video watermarking technique minimizing generation deficiencies

Saoussen BEN JABRA · Ezzeddine ZAGROUBA · Mohamed BEN FARAH*

Received: date / Accepted: date

Abstract 3D Anaglyph system is among the most popular 3D displaying techniques thanks to its simplicity and the cheap glasses that it uses. Anaglyph generation and watermarking are two essential techniques that attracted researchers in 3D anaglyph domain where several techniques have been proposed. However, most of the previous anaglyph watermarking studies focused on the robustness and the visual difference between original and marked content and they have not considered the three deficiencies caused by the generation step, which are the distortion of colors, the retinal rivalry and the ghosting effect. In this paper, we propose the first watermarking technique that protect 3D anaglyph content before its transmission by embedding the signature simultaneously with generation step. In this technique, three signatures were embedded before, during and after the generation process using different domains to obtain robustness to several manipulations, especially against malicious attacks. Moreover, the chosen generation process avoids generation deficiencies and allows obtaining high visual quality of the marked content. The experimental results illustrate robustness against attacks such as compression and collusion where the minimum value of NC is close to 0.7 and the maximum value of BER is close to 0.2. Besides, the suggested technique provides high invisibility where PSNR and SSIM values are respectively close to 58 and 0.9, and it minimizes the generation deficiencies.

Keywords 3D anaglyph watermarking · color distortions · signature robustness · ghosting effect · collusion attack · retinal rivalry.

Saoussen BEN JABRA
University of Sousse, National Engineering School of Sousse, LimTic Lab., Sousse-Tunisia
E-mail: saoussen.bj@gmail.com

Ezzeddine ZAGROUBA
University Tunis El Manar, Higher Institute of Computer Science, LimTic Lab., Ariana-Tunisia

Mohamed BEN FARAH
Department of Networks and Cyber Security, Birmingham City University, Birmingham B4 7XG, UK
*Corresponding author: mohamed.benfarah@bcu.ac.uk

1 Introduction

3D content is more easily accessible and transmitted through the networks nowadays than ever. Among the different 3D displaying techniques, e.g., glasses dependent or auto-stereoscopic, the anaglyph is the cheapest way that allows making the 3D visual experience achievable with no special hardware but only simple colored glasses. However, this popularity of 3D anaglyph images and videos makes them available to everyone introducing serious problems of security. Watermarking was proposed as a solution to these problems [1]. In fact, it consists of two stages: signature embedding and signature detection. During the first one, an invisible and robust signature is embedded in the original 3D anaglyph content to protect it while, the second stage consists in verifying the presence of the embedded signature in a given content after applying different types of attacks [2]. Various 2D image and video watermarking schemes have been proposed in the literature [3, 4, 5]. However, regarding 3D content, particularly 3D anaglyph content, the field is still in its early stages of development. Indeed, only a limited number of studies have been suggested due to the diversity of 3D displays and the complexity of 3D data.

All existing 3D anaglyph image and video techniques are decomposed into three steps which are: extraction of left and right views from the given original 3D anaglyph,

signature embedding into one or two views, and marked 3D anaglyph generation. This final step is done by simply superimposing two marked views. Based on our knowledge, no technique considers generation deficiencies when reconstructing the marked anaglyph. In fact, the simplest way to generate a 3D anaglyph image is to superimpose the cyan channel and the red one coming respectively from left and right view. This generation technique is not efficient and mainly suffers from three deficiencies, i.e., the distortion of colors, the retinal rivalry and the ghosting effect. These last ones cause different problems such as the color difference between original and perceived scenes and visual fatigue and this can affect the invisibility of the marked anaglyph content. Hence, the watermarking process should consider these problems at the embedding process as well as at invisibility assessment. In fact, signature invisibility is usually evaluated by calculating the difference between original and marked content using different metrics such as PSNR and SSIM but without considering generation deficiencies.

This paper proposes a robust and invisible watermarking technique dedicated for 3D anaglyph images and videos based on hybrid insertion. As the 3D anaglyph video is composed of a sequence of 3D anaglyph images, the suggested approach can be used for both 3D anaglyph images and videos by applying the proposed image watermarking on the set of frames composing the video. The originality of this technique consists in embedding the signature during the generation step in order to avoid generation deficiencies and to obtain a high visual quality of the marked 3D anaglyph. Indeed, instead of extracting the two views from the original 3D image anaglyph, the proposed approach takes as an input the two views before generating the 3D anaglyph image. Signature embedding is applied three times: The first one is a Discrete Wavelet Transform (DWT) based embedding that is applied on the two original views before beginning the generation process. The second one is a Least Significant Bit (LSB) embedding that is applied during the generation process. Finally, a Discrete Cosine Transform (DCT) based watermarking is applied after the last step of the generation process. This allows obtaining robustness against most attacks, besides a high level of invisibility. Unlike the existing techniques which generate the marked anaglyph image by a simple addition of the right and left marked views, the proposed approach takes into consideration generation deficiencies by embedding signature at same time of generation steps. This allows profiting from the advantages of the chosen generation method which minimizes the color distortions, the retinal rivalry and the ghosting effect.

The remaining of this paper is organized as follows: In section 2, the existing anaglyph 3D image and watermarking techniques are provided, while section 3 deals with the comparative study and the motivations of the proposed work. Next, the various steps of the proposed technique are outlined in detail. Section 5 presents the demonstrations of invisibility and robustness through experiments. Finally, the obtained results are compared with the existing 3D anaglyph image and video watermarking techniques.

2 Literature Review

In recent years, several techniques for anaglyph 3D image and video Watermarking [6] have been proposed. These techniques were classified based on two main criteria: the embedding target and the insertion domain [7]. In fact, the embedding target can be the red image (left view) or the cyan one (right view) extracted from an original anaglyph image. For videos, red and cyan images will be extracted from each frame composing the video. To enhance invisibility, the majority of researchers have opted for the cyan image as the ideal carrier for embedding the signature. This choice is based on the Human Visual System's (HVS) limited perception of blue color variations. Concerning the second criterion, different domains have been used to embed the signature, such as spatial domain, the DCT, and the DWT. For images and videos, the DWT domain has been used more than other domains thanks to its robustness against attacks.

The authors in [8,9,10] propounded DWT-based 3D anaglyph image watermarking techniques, where the signature was embedded only in the cyan image in [8]; whereas in [9,10], the signature embedding target was all images that composed the anaglyph 3D images (red, cyan and depth images). This multi-insertion guaranteed robustness against various attacks, while insertion in cyan images allowed obtaining high invisibility. The authors in [11] also proposed a DWT-based 3D anaglyph image watermarking where, the signature was embedded by changing the diagonal elements of every block of the jacket matrix applied to the middle-level sub-band blocks of the original image. This technique guaranteed high invisibility with robustness against various attacks thanks to the characteristics of the multi levels of DWT decomposition. Another technique based on the DWT was put forward in [12] and was composed of two stages: training and testing. In fact, in the first stage, the DWT was applied on the original anaglyph image, and then the genetic algorithm was performed to optimize the cœfficient bits of the low and high fre-

quency bands (LH and HL). This stage utilized the back propagation neural network.

DCT, FrFT, Singular Value Decomposition SVD and Principal Component Analysis (PCA) transformations were also used in [13,14,15,16]. The authors in [13] chose the DCT domain and the quantization of index modulation as an embedding target. This technique allowed obtaining a high level of invisibility but, it was not robust against many attacks. On the other hand, the scheme proposed in [14] embedded the signature in the right view extracted from the original anaglyph image using the FrFt transformation. The marked view would be superimposed with the original other views to obtain the marked image. In [15], the signature was encrypted using the Arnold transformation and embedded in the selected sub-bands of the non-subsampled transformed contourlet anaglyph image applying the PCA. This technique presented a high level of invisibility and it was robust against various attacks. The technique in in [16] tries to extract a robust feature to embed the watermark by applying DWT, Hadamard and SVD transforms. In fact, the cover image undergoes a DWT transformation, while the watermark image is scrambled using the Arnold transform. The watermark is then concealed within the Hadamard transformed blocks of the Anaglyph image, leveraging the singular values acquired through the application of SVD. [17] suggested two anaglyph 3D image watermarking schemes using the SSM and the adaptive Dither modulation with Watson's improved perception model to embed the signature. Finally, [6] proposes a non-blind 3D scheme based on Digital Shearlet Transform (DST) and Maximum Noise Fraction (MNF). First, the original anaglyph image is projected into the digital Shearlet domain. Next, the DST coefficients undergo a transformation into the MNF space. An information-theoretic approach is utilized to identify the most suitable candidate for watermarking from all the MNF bands. In the end, the watermark is embedded into the appropriate MNF band using a comprehensive insertion-based method. These techniques demonstrated a satisfactory level of visual quality and resilience against diverse attacks.

Concerning anaglyph 3D videos, the DWT is also the most used domain to embed signature. In fact, [18, 19] proposed two techniques where the signature was embedded in the selected high frequency cœfficients obtained after applying the 4-level DWT on the blue channel. The second technique embedded the signature when a scene change was detected but the first on uses all frames. These techniques presented a high level of invisibility, but they were not robust against malicious attacks and especially against collusion which has been the most dangerous attack for video watermarking. The first schemes that considered this attack was put forward in [20,21]. They were based on a multi-sprite generation. In fact, a sprite was generated from each set of 25 frames and the signature was embedded in each sprite by applying the DWT and the spatial domain. These techniques showed a good level of invisibility and robustness against collusion, compression and additional attacks such as geometric and temporal attacks. The difference between this last scheme and those suggested in [22] was that in [21] the signature was not embedded in all generated sprites but only in the ones which were not similar in order to enhance the invisibility of the marked video. Furthermore, a robust anaglyph 3D video watermarking based on cyan mosaic was recently proposed to resist the collusion attack [23]. In fact, the signature was embedded in the mosaic generated from only the cyan video composed of cyan views of the different frames of the original video. The embedding was done using a DCT based technique into Krawtchouk moments. This allowed increasing the compromise between invisibility and robustness against usual and malicious attacks.

In order to maximize robustness against attacks, two hybrid schemes were put forward in [24,25]. In fact, the work of [24] consisted in decomposing an original video into a set of Group of Pictures (GOP). Three types of images (blue, red or depth images) were after extracted from each GOP, and the signature was embedded into these images using three different insertion domains. The suggested scheme was robust against usual attacks and against compression. The authors in [25] proposed also a hybrid embedding scheme that combined two different domains: the spatial domain by applying the LSB and a frequency domain by applying the DWT and the DCT to embed the signature. Moreover, the suggested technique embedded two varied signatures where each one was inserted in a different domain and a different channel. This makes the signature robust against MPEG-4 and H264-AVC video compression.

Based on the literature review, generation deficiencies has not been considered in the proposed techniques. In fact, the classic way to generate an anaglyph image is to superimpose two views in different colors. Based on color filtering, the colored glasses will separate these two views from the composite one for each eye. Despite its simplicity, this technique is not efficient and suffers from three deficiencies which are the effect of ghosting, the distortion of color, and the retinal rivalry. The first problem is the main problem of most 3D displaying techniques and it is caused by the light-wavelength filtering. This provokes undesired images which will be mixed with the required ones. Concerning the color dis-

tortion, it causes dissimilarity between the colors of the original scene and colors seen through red-cyan glasses. Finally, the retinal rivalry causes visual fatigue and discomfort in case of long viewing. It is due to the difference in the colored object brightness and it means that similar objects do not have the same colors for the left and right eyes.

Several anaglyph image generation techniques have been proposed in order to minimize these three deficiencies and they can be classified based on three criteria: the color space, the deficiency type to minimize and the views used at the anaglyph generation step. This classification was proposed in [7] which showed that, for the first criterion, the CIEXYZ or CIELAB color space can be used in the anaglyph generation [26,27] as well as the RGB space [28]. Concerning the second criterion, each class of the proposed techniques is dedicated to minimize one type of the generation deficiencies [28, 29], or all simultaneously [30]. Finally, according to the third criterion, the anaglyph generation can use either the left and right images [26,31] or only a single image, either right, or left, plus the depth map [32].

Moreover, several methods dedicated to generate 3D anaglyph videos have been proposed. As anaglyph 3D videos can be considered as a sequence of 3D anaglyph images, 3D anaglyph image generation techniques can be applied on all frames that compose the scene to generate 3D anaglyph videos [33,34] and the same classification criteria can be also used for video anaglyph generation techniques.

Table 1 summarizes the advantages of the existing 3D anaglyph image and video generation techniques by giving the deficiencies that reduces each method. This table shows that [30] is the only generation technique which minimizes simultaneously the effect of ghosting, the distortion of colors, and the retinal rivalry. Indeed, this technique consists in matching perceptual color appearance attributes which can accurately define the color perception of the HVS and using the CIELAB color space which is perceptually uniform. Concerning the other existing techniques, each one reduces one of the three generation problems, and the efficiency depends on the used color space and the utilized image. In fact, the techniques which use depth information in addition to either the right or left image guarantee a good representation of the generated image.

Table 1: Comparison of anaglyph 3D image and video generation techniques

Technique	Content type	Deficiencies to reduce
[26]	Image	Color distortions
[27]	Image	Color distortions
[30]	Image	Color distortions Retinal rivalry Ghosting effects
[28]	Image	Ghosting effects
[29]	Image	Ghosting effects
[32]	Image	Color distortions Ghosting effects
[33]	Video	Color distortions Ghosting effects
[34]	Video	No indication

3 Comparative study and motivation

Table 2 illustrates a comparative study between existing techniques of anaglyph 3D images and videos watermarking based on invisibility and robustness. Concerning anaglyph 3D images, most watermarking techniques are invisible with a PSNR greater than 40 dB, except for [14] based on FrFt transformation which had a PSNR close to 27 dB. The majority of these techniques are robust against usual attacks such as filtering, noise and geometric attacks while some techniques resist compression attacks. Regarding anaglyph 3D videos, a limited number of techniques have been proposed in the literature and they present a high level of invisibility and robustness against most usual attacks. However, they are usually not robust against the most dangerous attacks such as collusion (type 1 and 2). In fact, only [20, 21,22,23] resisted to this attack by using either a sprite image as an embedding target or a complex embedding scheme to make the signature hard to extract. Finally, the comparative study shows that the hybrid embedding using different embedding domains as suggested in [24,25], maximizes robustness against different attacks.

Based on the comparative study we can notice that:

- The existing anaglyph 3D image and video techniques usually proceed as follows: Take the anaglyph content as an input, extract the two views, embed the signature into the obtained views, and finally generate the marked anaglyph by simply superimposing the two marked views. Researchers have not considered the generation deficiencies at the invisibility assessment. This can destroy the visual quality of the marked anaglyph content and make errors at the detection step.
- All anaglyph 3D image watermarking or generation techniques can be applied for anaglyph 3D videos which will be considered as a set of anaglyph 3D images.
- Every class of watermarking techniques presents its own advantages and deficiencies. Therefore, apply-

Table 2: Comparison of anaglyph 3D image and video watermarking techniques

Technique	Media	Invisibility	Robustness	Ref
DWT + Jacket Matrix + anaglyph image	image	++ 51	Filtering +noise + geometric attacks + intensity adjustment + histogram equalization + JPEG	[11]
DWT + AES encryption method + anaglyph image	image	++ 53	Filtering +noise + geometric attacks + histogram equalization + JPEG	[12]
DCT + QIM + anaglyph image	image	+ 40	NA	[13]
frft + cyan image	image	- 27	NA	[14]
Spread Spectrum + Watson perception model + anaglyph image	image	+ 41	Filtering +noise + geometric attacks + JPEG	[17]
PCA + nonsubsampled contourlet transform + anaglyph image	image	+++ 69	Filtering +noise + geometric attacks + intensity adjustment + histogram equalization + JPEG	[15]
DWT + SVD + Hadamard transform + anaglyph image	image	++ 54	Geometric attacks + noise + cropping + filtering	[16]
DST + MNF + anaglyph image	image	+++ 61	Filtering +noise + geometric attacks histogram equalization + cropping + JPEG	[6]
DWT + cyan image	video	+++ 65	Geometric attacks + noise + filtering	[18]
DWT + scene change detection + cyan image	video	+++ 69	Geometric attacks + noise + filtering	[19]
DWT + GOP + cyan image + red image + depth image	video	+++ 72	Geometric attacks + noise + filtering + frame suppression + MPEG4	[24]
LSB + DCT + DWT + cyan image + red image	video	+++ 70	Geometric attacks + noise + filtering + frame suppression + MPEG4 + H264	[25]
DWT + MIDSB + multi-sprite + anaglyph image	video	++ 58	Geometric attacks + noise + filtering + frame suppression + MPEG4 + collusion	[20]
DWT + LSB + multi-sprite + anaglyph image	video	++ 59	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + collusion	[21]
LSB + DWT + Mosaic + anaglyph image	video	+++ 70	Geometric attacks + noise + cropping + frame-based attacks + enhancement attacks + filtering + MPEG4 + collusion	[22]
DCT + cyan mosaic + krawtchouk moments	video	+++ 65	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + H264 + collusion	[23]

ing a hybrid embedding provides robustness against the maximum of attacks.

– To obtain robustness against the collusion attack (type 1 or 2), which presents the most dangerous attack for videos, two solutions can be applied. The first one is to embed the signature into sprites generated from original frames, while the second solution consists in applying a complex embedding scheme that makes the signature extraction hard.

4 Proposed approach

In this paper, We put forward a new anaglyph 3D image watermarking technique which embeds the signature at the generation stage. This allows to minimize the three deficiencies of the anaglyph generation and to maximize the robustness against usual and dangerous attacks. The proposed watermarking is based on multiple embeddings: the first one is a DWT based embedding which insert the signature before the generation process, the second one is an LSB based embedding that is applied during the generation step, and the last one is DCT based watermarking that will be applied after the generation process.

The proposed approach will be then adopted for the anaglyph 3D video by applying the suggested scheme on all frames that compose the original video. Since the suggested approach is based on multi-embedding and multi-domains, it is considered as a complex scheme and it allows obtaining robustness against the collusion attack.

The systematic framework of the proposed schema is shown in Figure 1 and it is decomposed in several stages. In fact, given the right and left views (R_1,G_1, B_1) and (R_r,G_r,B_r), they will be marked first using a DWT based scheme. Then, the generation process will be triggered using as an input the obtained marked views (R'_1,G'_1, B'_1) and (R'_r,G'r$'_r$,B'_r).

This process is based on the generation technique pro-

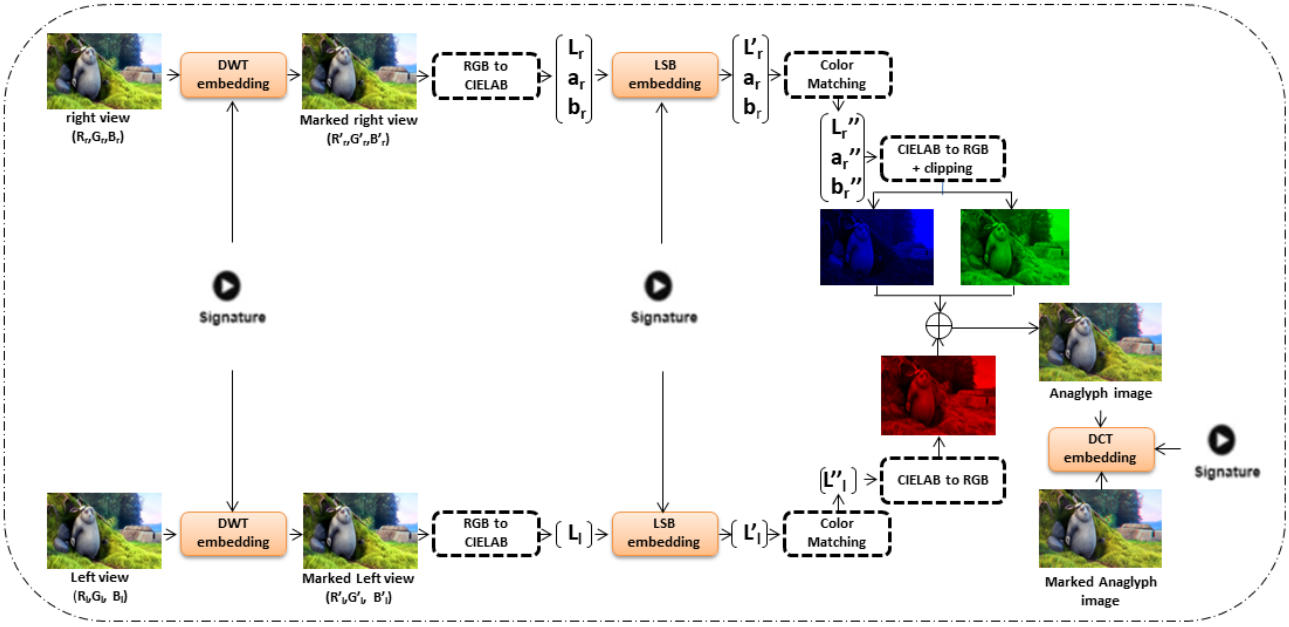

Fig. 1: Flowchart of the proposed embedding.

posed in [30], and it is decomposed into three steps. At the first step, the two marked views will be converted from the RGB to the CIELAB color space to obtain (L_1,a_1,b_1) and (L_r,a_r,b_r). Before the generation second step, an LSB based embedding will be applied on only the lightness cœfficient of the two views L_1 and L_r in order to maximize robustness. The LSB based embedding is chosen thanks to its high level of invisibility. Then, the marked lightness L'_1 and L'_r are used to calculate the three perceptual color appearance attributes for each pixel position, including its lightness, saturation and hue, which will be matched to those of the perceived anaglyph.
Finally, we convert them back into RGB and we superimpose the three obtained images (green and blue image from left view and red image for right view) to obtain the anaglyph image. This last one will be marked by applying a DCT embedding to obtain the marked anaglyph 3D image. The main algorithm of the proposed approach is given by Algorithm 1 and the detailed information on each processing module will be given below.

Algorithm 1: Mark (V_1,V_2,S_1,S_2,S_3,β)

/* This is the general algorithm of embedding, it returns the marked Anaglyph image A$''$ */
/* V_1 is the original right view */
/* V_2 is the original left view */
/* V'_1 is the right view after DWT embedding */
/* V'_2 is the left view after DWT embedding */
/* β is an invisibility factor */
/* S_1 is the first signature */
/* S_2 is the second signature */
/* S_3 is the third signature */
$V'_1 \leftarrow$ DWT embedding(V_1,S_1,β)
$V'_2 \leftarrow$ DWT embedding(V_2,S_1,β)
$(L_r,a_r,b_r) \leftarrow RGB2lab(V'_1)$
$(L_l,a_l,b_l) \leftarrow RGB2lab(V'_2)$
$L'_r \leftarrow LSB(L_r, S_2)$
$L'_l \leftarrow LSB(L_l, S_2)$
L_r",a_r",b_r" $\leftarrow$ colormatching(L'_r,a_r,b_r)
L_l",a_l",b_l" $\leftarrow$ colormatching(L'_l,a_l,b_l)
$V_{blue}, V_{green} \leftarrow$ lab2RGB(L_l")
$V_{red} \leftarrow$ lab2RGB(L_r",a_r",b_r")
$A' \leftarrow V_{red} + (V_{bleu}, V_{green})$
A" $\leftarrow$ DCT(A',S_3,β)

4.1 Dwt embedding

As mentioned above, the first stage of the proposed approach consists in embedding the signature into left and right views by applying a DWT based schema. This last one allows obtaining robustness against usual attacks and compression. Furthermore, it gives a high visual quality of the marked image. The chosen schema consists in adding high frequencies of the signature to those of the original view. The high frequencies are chosen because the HVS is insensitive to these components, and they provide a good trade-off between capacity and invisibility. In fact, the general algorithm (Algorithm 2) of the chosen DWT embedding is as follows:

1. The signature is first spread based on the view size.

2. The 3^{rd} level of the wavelet transform is applied to the signature and the original views. This level is obtained by first decomposing sub-component LL_1 critically sampled to LL_2, HL_2, LH_2, and HH_2 and then the process will be applied for sub-component LL_2 in order to obtain LL_3, HL_3, LH_3 and HH_3.
3. The marked cœfficients ($C^{'}{}_i$) are obtained by adding the high frequency cœfficients HH_3 and HL_3 of signature (W_i) to those of original view (C_i) using the equation below:

$$C_i^{'} = C_i + \beta * W_i \quad (1)$$

where β is an invisibility factor used to increase signature invisibility.
4. The marked views are finally obtained by applying the 3^{rd} level of the DWT Inverse (I-DWT) to the marked cœfficients.

Algorithm 2: DWT embedding (V,S, β)

```
/* The function returns the marked view V' */
/* V is the original view */
/* β is an invisibility factor */
S ← imresize(S,size(V))
for i ← 1 to 3 do
    if i = 1 then
        LL_Si, HL_Si, LH_Si, HH_Si ← DWT(S)
        LL_Vi, HL_Vi, LH_Vi, HH_Vi ← DWT(V)
    else
        LL_Si, HL_Si, LH_Si, HH_Si ← DWT(LL_Si)
        LL_Vi, HL_Vi, LH_Vi, HH_Vi ← DWT(LL_Vi)
W_i ← HH_S3
for each coefficient C_i of HH_V3 do
    C'_i ← C_i + β × W_i
V' ← IDWT(LL_V3,LH_V3, HL_V3,HH'_V3)
```

4.2 RGB to CIELAB conversion

Given the two marked RGB views, the first step of the anaglyph generation stage will be applied. The lightness of the marked right and left views will be matched to alleviate the retinal rivalry effect. In addition, the generation process explicitly takes the ghosting reduction into account [30]. At the first step of the generation, the RGB values of the marked two views will be converted into L∗ a ∗b values of the CIELAB color space. L, a and b values of the right and left views are calculated as proposed in [30].

4.3 LSB embedding

Giving the CIELAB values L, a, and b calculated during the first step of the generation, the spatial domain and the substitute mode are chosen to embed the signature into only the L value of the left and right view. This allows improving invisibility, robustness and processing complexity reduction. In fact, the L value is the most invariant and robust value in the CIELAB color space because it represents the lightness value, but any manipulation on lightness can degrade the visual quality of the corresponding image. For this reason, an LSB embedding is chosen to guarantee a high level of visual quality. The LSB embedding technique is a widely recognized and conventional method employed for inserting a watermark in a host medium. This technique is favored for its simplicity and the high level of invisibility it offers [35]. The process involves inserting the mark bits into the least significant positions. In fact, it proceeds as follows (Algorithm 3):

1. Given the signature and the different cœfficients of the L value, they are converted to a binary format.
2. The embedding is done as follows: If the signature bit and the least significant bit (LSB) of the L value are same, this last one will be set to 0; else, it takes the value 1.
3. The marked L will be reconstituted based on the marked LSBs.

Algorithm 3: LSB embedding (L, S)

```
/* The function returns the marked L' */
/* L is the lightness of CIELAB coefficients */
S ← binary(S)
L ← binary(L)
for each coefficient of L do
    if LSB(S) = LSB(L) then
        LSB(L) ← 0
    else
        LSB(L) ← 1
```

4.4 Color matching and RGB conversion

After LSB insertion, the marked L value and the original a and b values will be used to generate the anaglyph image A. First, it consists in getting the CIELAB values of the left and right views of the perceived anaglyph A L_{Al}, a_{Al}, b_{Al}, L_{Ar}, a_{Ar}, b_{Ar} which produce comparable values for lightness, saturation, and hue as those computed from L_l; a_l; b_l; L_r; a_r ; b_r. In order to present

the left image, the red channel is used and the other two green and blue channels are utilized to present the right one. Therefore, it is necessary to deliberately select the L *a*b values of the perceived anaglyph in such a way that, upon conversion back to RGB, the three-dimensional vector L_{Al}; a_{Al}; b_{Al} an be effectively represented by a solitary red value R_{Al}, and L_{Ar}; a_{Ar}; b_{Ar} can be represented by G_{Ar}; B_{Ar}. To obtain L_{Al}, a_{Al}, b_{Al}, L_{Ar}, a_{Ar}, b_{Ar}, the left and right views will be processed differently as described in [30]. Only the red channel is utilized to present the left view in the ultimate anaglyph. After color matching, the CIELAB values will be converted to RGB values by applying the parameterizations proposed in [30] in order to guarantee color space conversion and ghosting reduction.

4.5 DCT embedding

Given the generated anaglyph image, the DCT domain is chosen to embed the third signature in order to improve robustness against attacks. In fact, the chosen schema is decomposed into different steps (Algorithm 4). First, the DCT transformation is applied on the given anaglyph image and the N cœfficients are selected based on key L which identifies the start cœfficient where N represents the length of the signature. The second step consists in the addition of the binary signature to the selected N cœfficients according to the following equation:

$$\begin{cases} C_w(i) = C(i), & \text{if W(i)=0;} \\ C_w(i) = C(i) \times (1+a), & \text{if W(i)=1, i=1..N.} \end{cases} \quad (2)$$

where C(i) represents the selected cœfficients from the anaglyph image, W is the binary signature to embed, a is the invisibility cœfficient, and C_w(i) represents the marked cœfficients.
Finally, the DCT inverse will be calculated to generate the marked image. To fix the key L value, our choice is based on the fact that the first cœfficients of the DCT matrix represent the lowest frequencies and those placed at the end are the highest. Therefore, key L will determine the nature of the cœfficient to be embedded. Since the low frequencies are more sensible to modifications and more robust than high frequencies, key L is defined based on the ratio between the DCT matrix and the signature sizes using the following equation:

$$L = f \times (\frac{M}{N}) \quad (3)$$

where M is the size of the DCT matrix, N represents the size of the signature, and f is the cœfficient to select the position. F is chosen by testing the effect of the variation in its value with the invisibility cœfficient 'a' on the invisibility and the robustness results. The obtained values show that the visual quality is enhanced with a robustness reduction when the position of insertion is moved to the last cœfficients. Thus, the parameters are chosen as follows: f = 4 and $\beta = 0.001$ to obtain the best compromise between invisibility and robustness.

Algorithm 4: DCT embedding (A, S, β)

```
/* The function returns the marked anaglyph A' */
/* A is the anaglyph image */
/* β is an invisibility coefficient */
C ← DCT(A)
for each coefficient C_i of A_DCT do
    if W(i) = 0 then
        C'_i ← C_i
    else
        C'_i ← C_i * (1+β)
A' ← IDCT(C'_i)
```

Finally, table 3 describes the meaning and the values of the different variables used in the proposed approach.

Table 3: Variables description

Variable	Meaning	Value
β	Invisibility coefficient to minimize invisibility degradation	0,001
M	DCT matrix size	= host image size
N	Signature size	64*64
L	Embedding Key for DCT based scheme	depends on M and N
f	Embedding location to maximize security and invisibility	4
LL,LH,HL,HH	low, mean and high DWT frequencies	DWT results

4.6 Detection scheme

Given an anaglyph image, the detection stage consists in verifying the presence or absence of at least one of the embedded signatures. The scheme is decomposed in different steps, as shown in Figure 2. Indeed, at the detection stage the inverse steps of the embedding and generation process are applied as follows:

1. First, the DCT detection schema will be applied on the input anaglyph image. The presence of key L is necessary at this step. The two first steps of DCT

detection are similar to those of the embedding, where the DCT transformation will be calculated from the original anaglyph image and key L will be used to select the cœfficients chosen at the embedding. The signature will be then extracted from the selected cœfficients.
2. If DCT detection succeeds to extract the embedded signature, the detection step is completed and the extraction succeeds; else, the channel separation will be applied to detect the right and left channels and the CIELAB conversion will be applied as done in the embedding stage.
3. Given the two channels, the RGB conversion will be applied to obtain the L, a and b values of the two views.
4. L_r and L_1 will be used as inputs for LSB detection, which consists in extracting the embedded signature by reading the least significant bits and comparing the detection signature with the embedded one.
5. If LSB detection succeeds to extract the embedded signature, the detection step will be considered as completed and the signature will be extracted; else, the CIELAB values will be converted to the RGB to obtain the two views in the RGB color space. The conversion will be done as defined at the embedding stage.
6. Finally, DWT detection will be applied on the obtained views where the first two steps of DWT detection are similar to those of the DWT embedding. In fact, after spreading the signature based on the view size, the 3_{rd} level of the wavelet transform will be applied to the signature and the original views in order to obtain LL_3, HL_3, LH_3 and HH_3. Then, the signature will be obtained by subtracting it from the high frequency cœfficients HH_3 and HL_3 of the marked views. If the detected signature is similar to the embedded one, detection succeeds; else, it fails.

4.7 Application of the proposed approach to anaglyph 3D video

Since an anaglyph 3D video is considered as a sequence of anaglyph 3D images, any image generation or watermarking technique can be adopted for a video. Hence, we propose in this paper to apply the suggested watermarking technique to an anaglyph 3D video. The obtained video watermarking will profit from the advantages of the proposed image watermarking. Indeed, it will preserve invisibility and robustness against usual and malicious attacks guaranteed by the hybrid insertion. Besides, it will be robust to the video attacks such as temporal attacks and especially to collusion attack since the used embedding scheme is considered as a complex technique.
Figure 3 illustrates the general scheme of the embedding and detection steps.

In fact, given a set of stereo pair images, the embedding proceeds as follows:

1. The proposed watermarking technique will be applied for each stereo pair images to obtain a set of marked anaglyph 3D images.
2. The marked anaglyph 3D video will be obtained by reconstructing the set of obtained marked images.

Given an anaglyph 3D video, the detection step proceeds as follows:

1. The given video will be decomposed in a set of anaglyph 3D images.
2. The detection scheme suggested for anaglyph 3D images will be applied for every frame.
3. If detection succeeds for at least one of all frames the signature will be extracted; else, detection fails.

5 Experimental results

To evaluate the proposed watermarking technique, two primary criteria are employed: invisibility, which takes into account any generation flaws, and robustness against both common and malicious attacks.

5.1 Dataset collection

Multiple experimentations are conducted on a collection of chosen anaglyph 3D videos and images. [36]. As the input of the proposed video watermarking is a set of stereo Pairs composing the video, a dataset of stereo pairs was constructed by applying a technique inspired from different methods which consist of reversing anaglyph videos into stereo pairs [37,38]. The used videos were collected from different works and from YouTube to obtain a variable dataset where the chosen videos are qualified by different characteristics like the background texture, the total time, the movement type and the resolution. We noted that the frame rate for all videos is 30 frames per second and all videos have mp4 extension and are in raw format (without compression).

Since our approach is also dedicated to images, we should evaluate the image watermarking on a set of test images having different characteristics. For this reason, we select 50 frames (100 stereo pairs) from the 10 chosen videos. The choice is done randomly: 5 frames from each video including the first and the last frames from each video.

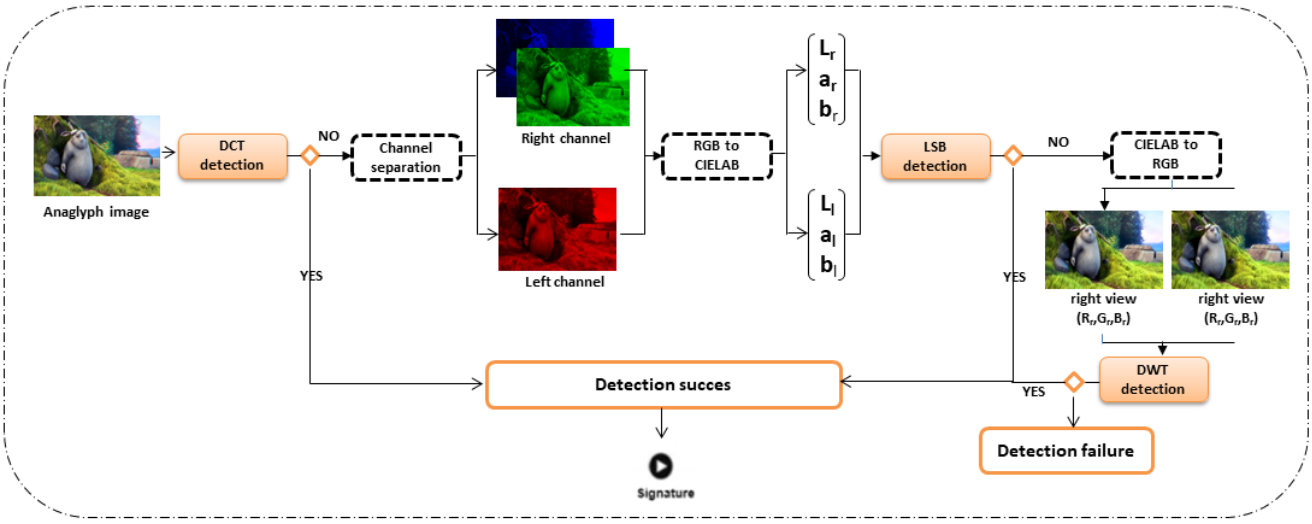

Fig. 2: Flowchart of proposed detection.

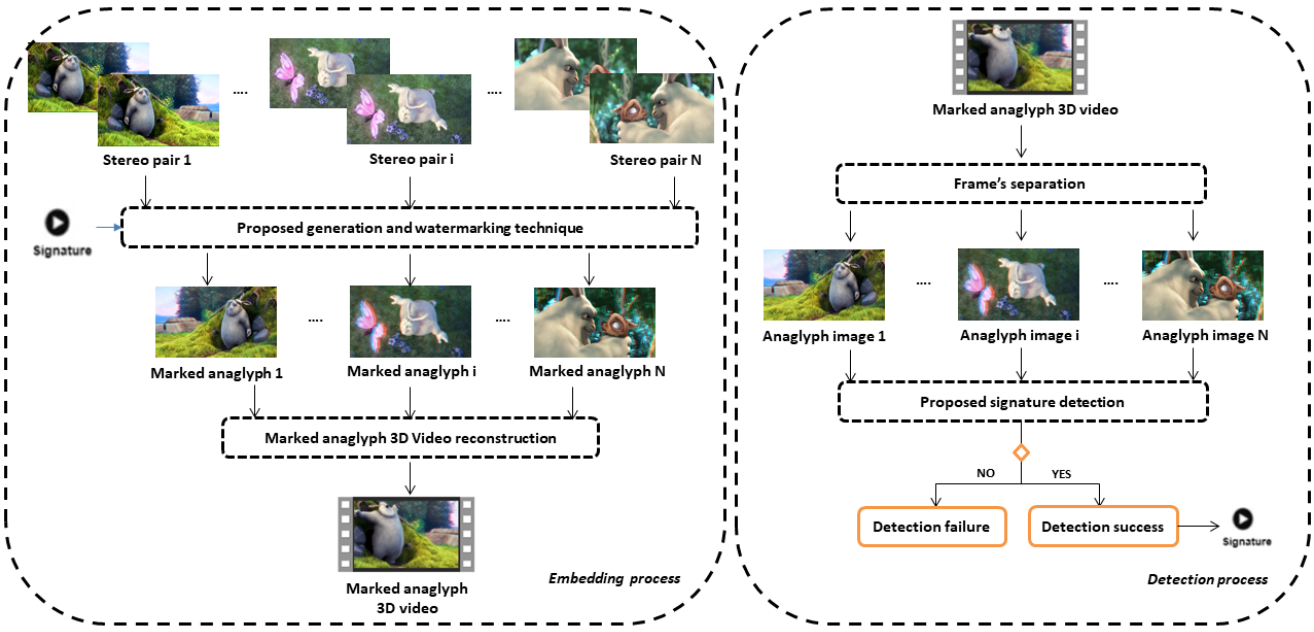

Fig. 3: General scheme of watermarking and generation for anaglyph 3D video.

Table 4 depicts the characteristics for every video. Moreover, we test two different resolutions (32×32 and 64×64) for the three embedded signatures. 6 images are then chosen as signatures to test the effect of the signature size on watermarking efficiency.

5.2 Invisibility evaluation

Invisibility is an important criterion for the assessment of any watermarking technique. However, all authors don't consider the visual alteration of generation process and they simply superimposing the two marked views to obtain the marked anaglyph 3D image. The originality of the proposed approach is to embed the signature during the generation process to avoid this alteration. Hence, invisibility evaluation will consider generation problems, which are the effect of ghosting, the distortion of colors, and the retinal rivalry. Added to that, signature invisibility will be assessed by measuring the difference between original and marked anaglyph 3D images. We use two types of invisibility evaluation: qualitative evaluation which is based on the visual ap-

Table 4: Video test characteristics

Video	Total time (second)	Resolution	Type	Movement	Background
[V1]	43	1080 × 720	Animation	Medium	Textured
[V2]	634	1920 × 1440	Movie	Medium	Uniform
[V3]	204	1080 × 720	3D Racing	Rapid	Textured
[V4]	197	1080 × 720	Nature	Medium	Textured
[V5]	58	480 × 360	Sport	Slow	Textured
[V6]	326	640 × 320	Documentary	Rapid	Uniform
[V7]	254	1280 × 720	Space scene	Medium	Uniform
[V8]	69	1280 × 720	Movie	Rapid	Uniform
[V9]	452	480 × 360	Documentary	Slow	Textured
[V10]	108	1080 × 720	Animation	Slow	Uniform

pearance of the generated marked anaglyph 3D image and video and quantitative evaluation where different metrics are calculated to prove signature invisibility.

Qualitative evaluation : Two criteria are considered: The first one is the image quality regarding specific visual factors, e.g., chrominance accuracy, retinal rivalry, and ghosting effect, while the second criterion is signature invisibility. To qualitatively assess these two criteria, the videos obtained after applying the suggested approach are provided to 25 participants who are non-experts and who have normal vision (with or without corrective glasses). We note that normal vision means that participants don't have a color vision deficiency or color blindness which make them unable to distinguish certain shades of colors. All participants used colored glasses which are the NVIDIA 3D Vision Discover red-cyan glasses.

The invisibility test is blind, where every participant is asked to evaluate the visual quality of two videos selected from the 10 test videos as well as the quality of 10 selected frames (5 frames per test video). Concerning generation evaluation, we are inspired from the method proposed in [30] where the original stereo pairs and generated marked anaglyph frames are provided to participants who should give three quality scores for each anaglyph image evaluating its chrominance accuracy, retinal rivalry and ghosting effect. Therefore, these three visual phenomena are explained to each participant by using some examples. Then, the original image is shown to each participant to memorize its color and evaluate the chrominance accuracy of the anaglyph images. The chrominance accuracy is evaluated first, followed by the retinal rivalry and the ghosting effect. For watermarking evaluation, we generate anaglyph frames and anaglyph videos by applying the suggested approach without signature embedding steps to obtain an anaglyph video without signatures. Hence, each participant will provide four scores (one for watermarking quality and 3 for generation phenomena) which should be between 1 and 5 where 5 means that the visual quality of the generated marked anaglyph is excellent, and where 1 means bad quality.

Figure 4 presents several frames of the test video "bunny" (right view, left view, and generated anaglyph with and without signature) and shows that there is no visual difference between images with and without signatures. Moreover, the generated marked anaglyph frames do not present visual degradation.
In figure 5 the different average scores awarded by the participants to the different frames and videos test are given. This figure shows that only three participants (7, 12 and 21) give 3 and 2 as a score to retinal rivalry criteria and explain their choice by the visual fatigue and the discomfort that they feel when they watch the anaglyph images. This may be because these three participants wear corrective glasses. Concerning the two other visual phenomena (chrominance accuracy and ghosting effect), all scores are between 4 and 5, which proves that the generation process resolves these two problems. Finally, for the watermarking score, most scores awarded by participants to the 10 frames or to the two videos are equal to 5, and this confirms that no significant degradation exists between marked and non-marked frames and videos.

Quantitative evaluation This type of invisibility evaluation consists in quantitatively proving the invisibility

Fig. 4: Examples of original stereo pairs and their corresponding anaglyph: right view on 1_{st} column, left one on the 2_{nd}, generated anaglyph without signature on 3_{rd}, and generated marked anaglyph on last column.

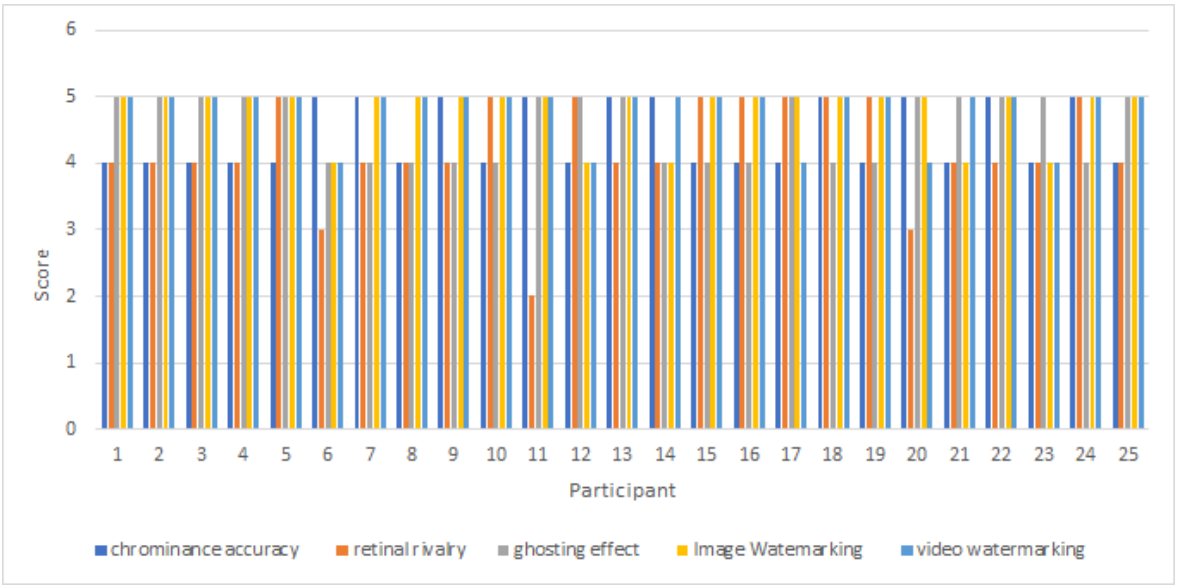

Fig. 5: Average scores awarded by participants.

of the embedded signature by measuring the mean Peak Signal to Noise Ratio (PSNR). The PSNR is calculated between different frames generated without signatures, which are called original frames, and those generated with signatures, called marked frames. The PSNR and the mean PSNR are measured as follows:

$$(Mean - PSNR)_{dB} = \frac{1}{N} \times \sum_{i=1}^{N} PSNR_i \tag{4}$$

where N is the number of frames composing the video, and $PSNR_i$ presents the PSNR of each frame and is calculated as follows:

$$(PSNR)_i = 10 \times \log_{10}(\frac{max_i^2}{MSE}) \tag{5}$$

In this equation, maxi is the maximum pixel value of the original frame i, and MSE presents the mean square error between the original and marked frames calculated based on the following equation, where I is the original

frame, I′ is the marked one, and (M,N) presents the size of the frame:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I^{'}(i,j)]^2 \quad (6)$$

Figure 6 presents the average PSNR (Peak Signal-to-Noise Ratio) values obtained for the 10 test videos employed. It is observed that a high level of invisibility is achieved when the mean PSNR exceeds 40 dB. The obtained values validate that the proposed watermarking method for anaglyph 3D images and videos ensures excellent visual quality using the two signatures. The minimum mean PSNR value is approximately 48 dB (respectively about 46 dB) for the first (second) signature, while the maximum value is around 57 dB (respectively about 56 dB).

Despite its simplicity, PSNR or MPSNR cannot sometimes provide subjective evaluation results. For this reason, we calculated SSIM or MSSIM to prove the visual quality of the marked image or video quality. The MSSIM is defined as follows:

$$MSSIM = \frac{1}{k} \sum_{k=1}^{K} SSIM(f_k, f_{kw}) \quad (7)$$

$$SSIM(f_k, f_{wk}) = \frac{(2\mu_{f_k}\mu_{f_{kw}} + C_1)(2\sigma_{f_k f_{kw}} + C_2)}{(\mu_{f_k}^2 + \mu_{f_{kw}}^2 + C_1)(\sigma_{f_k}^2 + \sigma_{f_{kw}}^2 + C_2)} \quad (8)$$

where μ_{f_k} and $\mu_{f_{kw}}$ are the mean values of the original image and the marked one, respectively; σ_{f_k} and σ_{f_k} are the variances of the original image and the marked one. $\sigma_{f_k f_{kw}}$ denotes the covariance of the original image and the marked one; and C_1 and C_2 are two stability constants.

Figure 7 depicts the obtained SSIM values for 20 images. It is evident that the minimum SSIM value is approximately 0.8, which substantiates the superior visual quality achieved by the proposed approach.

5.3 Robustness evaluation

Two types of attacks are applied to evaluate signature robustness. In fact, since the suggested approach is dedicated to image and video content, 2D manipulations and attacks specific to videos are tested. In addition to assessing invisibility, the robustness of the proposed approach against attacks can be evaluated both qualitatively and quantitatively. Qualitative evaluation involves determining whether the signature can be successfully detected under a specific attack, while quantitative evaluation entails measuring the Bit Error Rate (BER) and the Normalized Correlation (NC) between the original and extracted signatures. If the proposed approach demonstrates successful signature detection and achieves low BER and high NC values, it is considered robust against the given attack. The initial criterion quantifies the level of dissimilarity between the original and extracted signatures, while the second criterion enables the estimation of similarity between the two marks. The NC and BER are computed based on the following equations:

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) \times W^{'}(i,j)}{\sum_{i=1}^{M} \sum_{j=1}^{N} [W(i,j)]^2} \quad (9)$$

$$BER = Number\ of\ Error\ bits\ /\ Number\ of\ Total\ bits \quad (10)$$

In the equations, W(i,j) and W′(i,j) represent the pixel values of the original and extracted marks, respectively, while (M,N) denotes the size of the mark. The values of these two metrics range between 0 and 1, where the suggested approach is considered robust if the NC is close to 1 and the BER is close to 0.

Image watermarking evaluation In order to evaluate the proposed anaglyph 3D image approach, several usual and malicious attacks dedicated to images are tested on 50 frames selected from the 10 chosen videos. Concerning the usual attacks, we first apply geometric manipulations, which are the rotation (10°, 45° and 90°) with different angles, scaling (up-scaling and down-scaling) and translation (on lines and columns). Then, different noises, viz. the salt & pepper noise with density of 0.01, the Gaussian noise with a variance of 0.01 and the Poisson noise and cropping using various percentages (10%, 20% and 25%), are applied to the marked images. The signature is successfully detected after these manipulations and the obtained NC and BER, which are respectively close to 1 and 0, quantitatively confirm this robustness. Afterwards, robustness is verified after applying various types of filtering, like the median and Gaussian filters, where the BER is almost about 0.06 and the NC value is about 0.9. Robustness against these usual attacks is obtained thanks to the use of the DWT and DCT domains which are invariant to these manipulations and to the LSB embedding which is invariant to translation.

Figure 8 shows BER values obtained after different types of scaling while Figure 9 illustrates NC values obtained after cropping attack with different percentages for 10 examples of the test images. The obtained values prove the robustness of the proposed approach against these

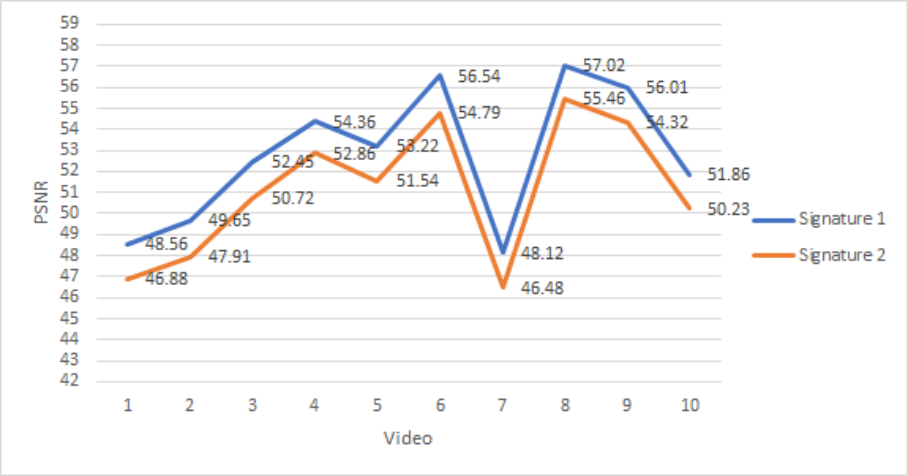

Fig. 6: Mean PSNR values for the 2 tested signatures.

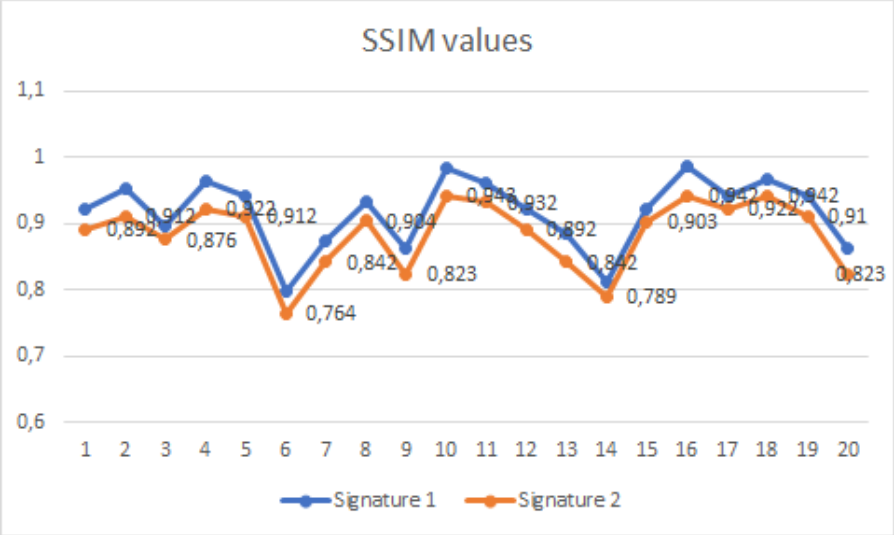

Fig. 7: SSIM values obtained for 20 test images.

two usual attacks. Then, the JPEG and JPEG 2000 compression is applied as a malicious attack using different quality factors (90, 80, 70 and 50). Next, we summarize the average NC values for the 50 test images. The obtained values prove the robustness of the suggested watermarking against these two compression standards. This is obtained thanks to the embedding based on the DCT transform, which is used in the JPEG standard, and on the DWT transform, which is used in JPEG2000.

Table 5 depicts the BER and NC measurements obtained after applying the tested attacks. For every attack, we indicate the signature (S1 or S2 or S3) which is extracted. We note that S1 is the signature that is embedded before generation with a DWT schema, S2 is the signature embedded during generation with an LSB schema and S3 is the signature inserted after generation using a DCT based technique. Table 5 shows that after translation, scaling down and noises, S2 is the signature which is successfully detected because the DCT transformation is not robust to these manipulations. However, S3 is detected after the rotation, scaling up, cropping (10%) and JPEG compression due to the invariance of the DCT transform to these manipulations. Finally, detection cannot extract S3 and S2, but it succeeds in extracting S1 in case of noises and JPEG2000 compression thanks to the characteristics of the DWT.

Video watermarking robustness Since the video watermarking is based on the same hybrid scheme proposed to images, we can confirm that the suggested video watermarking is also robust against attacks men-

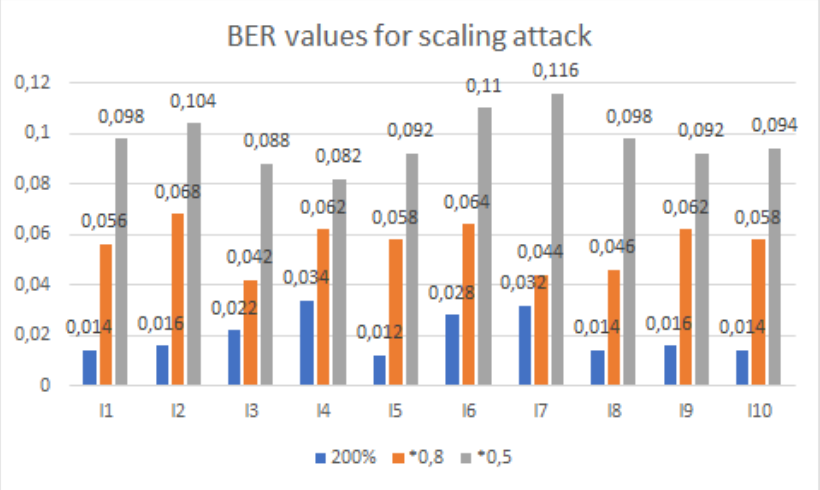

Fig. 8: BER values for different types of scaling attack.

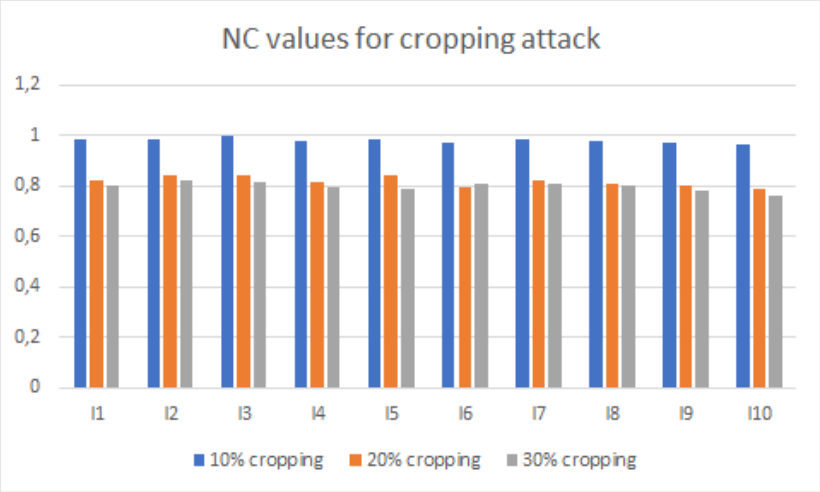

Fig. 9: NC values for cropping attacks with various percentages.

tioned in Table 5. However, we need to verify the robustness against attacks dedicated to video content, such as frame-based attacks, temporal attacks and collusion. First, the frame-based attacks are tested by applying frame dropping until 30%, frame swapping, and frame change rates from 25fps to 15fps. The suggested approach is robust against these attacks. This efficiency is achieved thanks to the repetition of the embedding in all frames composing the original video. Then, temporal attacks are tested by applying the two most popular video compression standards, MPEG-4 and H264/AVC, using a variable bit rate from 2Mbps to 256kbps. The Mediacoder Software application is used to simulate real cases and transcode marked videos to various formats. The NC and BER values obtained after applying MPEG and H264 compression are illustrated in figure 10 and they prove the robustness of the proposed approach against compression even with a low bit rate. This is obtained thanks to the use of the DCT and DWT transformations which are used in compression standards.

Finally, the collusion attack is tested. This malicious manipulation presents a very dangerous attack, which must be considered by researchers when embedding signatures into video content. Indeed, this attack involves reconstructing the original video from the marked version without prior knowledge of the embedding technique employed. Collusion attacks can be categorized into two main types. The first type is collusion type 1, where the attacker attempts to generate the unmarked video by approximating the used signature through calculating the average of a specific set of videos that have been marked with the same signature. In the case of

Table 5: Robustness results for anaglyph 3D image watermarking

Attack type	Attack value	Signature	NC	BER
Translation	From 5 until 20	S2	0.988	0.008
Rotation	90	S3	1	0
	45	S3	1	0
	10	S3	1	0
Scaling	Up (150%)	S3	1	0
	Up (200%)	S3	0.964	0.014
	Down (*0.8)	S3	0.898	0.056
	Down (*0.5)	S2	0.789	0.098
Salt & pepper noise	0.01	S2	0.862	0.078
Gaussian noise	0.01	S2	0.854	0.084
Poisson noise	-	S2	0.644	0.194
Cropping	10%	S3	0.988	0.008
	20%	S1	0.832	0.096
	25%	S1	0.814	0.112
Median filtering	-	S1	0.892	0.054
Gaussian filtering	-	S1	0.844	0.096
JPEG compression	90	S3	1	0
	70	S3	0.942	0.048
	50	S3	0.832	0.098
JPEG 2000	-	S1	0.826	0.104

the second type (collusion type 2), the attacker must be provided with multiple versions of marked videos, where the same video is marked using different signatures. The attacker's task is to identify the matching frames across these versions of marked videos. Then, they separate the different video scenes and find the unmarked frames by calculating the average of all adjacent frames. Finally, they combine all obtained frames to generate the unmarked video.
To counteract collusion attacks, there are two potential solutions that can be employed [39]. The first solution involves utilizing a mosaic image generated from the original video, while the second solution entails employing a sophisticated embedding scheme that significantly complicates signature extraction for potential attackers. The proposed approach is considered as a complex technique where the signature is embedded three times at different stages using three various domains and two different color spaces. This enables the attacker to learn about the embedding algorithm and guarantees the robustness of the proposed watermarking against collusion. In order to simulate collusion operations, we insert five various watermarks with a resolution of 64×64 in the original video. Then, the anti-collusion performance of the suggested technique is tested by averaging the marked frames of the five obtained videos (by varying average number of frames). Figure 11 illustrates the obtained NC values after applying collusion attack with different average number of frames for the 10 test videos and confirms the robustness of the proposed approach against the collusion attack.

Table 6 illustrates the measurements of BER and NC obtained following the application of the tested attacks. It shows that after collusion, detection succeeds from the first step thanks to the use of a complex embedding schema that makes signature extraction from marked videos hard. Concerning the compression standards, S1 is detected successfully thanks to the robustness of the DWT transformation to this attack. Finally, after frame-based attacks, S3 and S2 are detected. This can be explained by the repetition of the signature into all frames of the given video.

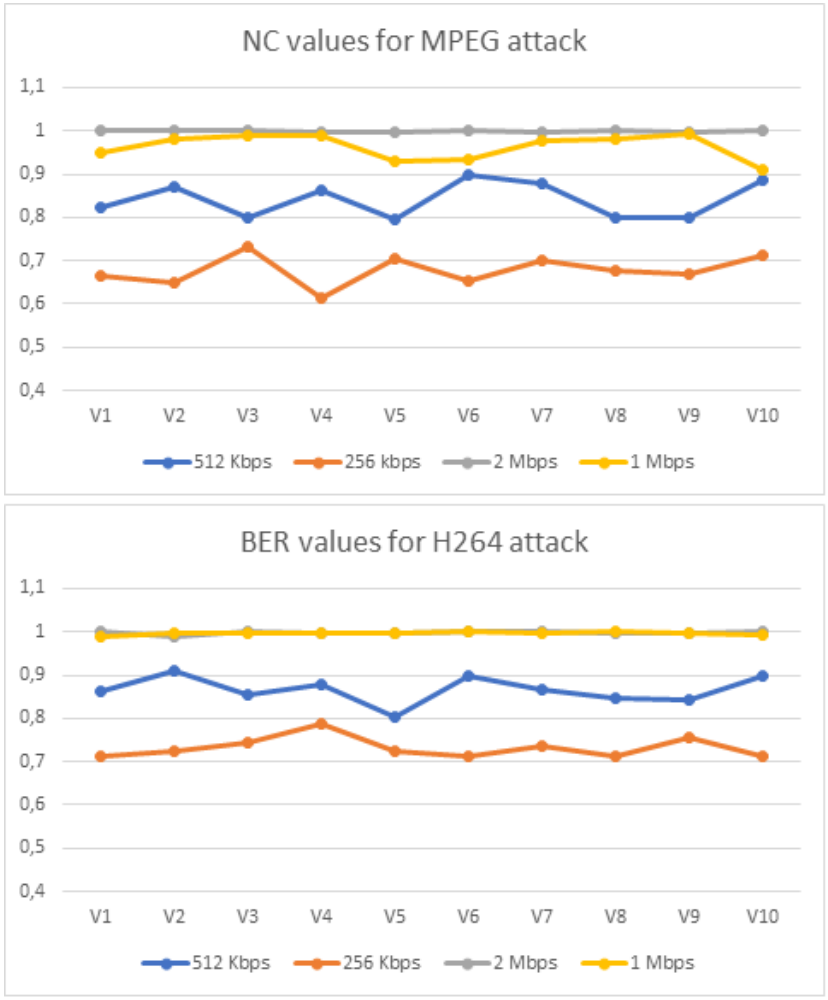

Fig. 10: NC and BER values for MPEG and H264 attacks.

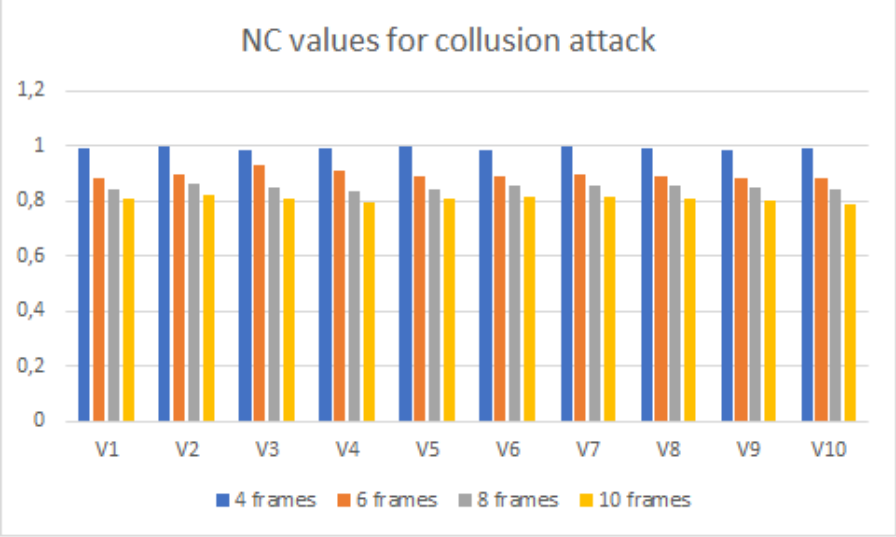

Fig. 11: NC values for collusion attack.

Table 6: Robustness results for anaglyph 3D video watermarking

Attack type	Attack value	Signature	NC	BER
Frame dropping	30%	S3	1	0
Frame swapping	-	S3	1	0
Frame change rate	15	S2	0.966	0.026
MPEG4	2 Mbps	S1	1	0
	1 Mbps	S1	0.948	0.064
	512 Kbps	S1	0.786	0.126
	256 Kbps	S1	0.665	0.182
H264	2 Mbps	S1	1	0
	1 Mbps	S1	1	0
	512 Kbps	S1	0.844	0.096
	256 Kbps	S1	0.776	0.124
Collusion (Parameter = Average number of frames)	4	S3	0.992	0.012
	6	S3	0.896	0.086
	8	S3	0.842	0.098
	10	S3	0.814	0.102

6 Comparative study

The first contribution of the proposed work is that it is the unique watermarking that embeds the signature simultaneously with 3D anaglyph generation from two stereopair images. This ensures avoiding any visual degradation caused by the generation process. Moreover, the suggested method enhances robustness against attacks thanks to the multi-embedding applied before, during and after the generation process.

The experimental tests presented in section 5 prove that the proposed approach for anaglyph 3D images and videos ensures favorable outcomes in terms of invisibility and robustness. However, this effectiveness should be proven by comparing it with existing techniques.
Since the suggested watermarking is dedicated to both image and video 3D anaglyph content, the results are compared with [20,21,22,23] for videos and with [12,15, 16,6] for image watermarking.The evaluation focuses on the invisibility and robustness of the compared methods against attacks.

6.1 Invisibility comparison

First, we note that the proposed approach minimizes the distortion of colors, the retinal rivalry and the ghosting effect. This was proven by the qualitative evaluation shown in the previous section. Concerning signature invisibility, we compare the mean PSNR of the proposed approach with the selected existing techniques for image and video watermarking. Figure 12 and figure 13 illustrate this comparison and show that the mean PSNR obtained for the proposed approach is close to 57 and 60 for images and video respectively. Despite the little decrease of the proposed approach invisibility compared with existing techniques, it is considered as a high visual quality. This little difference can be explained by the proposed multi-embedding of the signature before, during and after generation. Consequently, the signature capacity is more important and it is repeated in all frames. For the existing techniques, the signature is not repeated in all frames composing the video. That was why they provided a mean PSNR higher than the proposed approach. However, we note that the existing techniques didn't consider the generation deficiencies during the invisibility assessment.

6.2 Robustness comparison

Experimental results showed that the proposed approach is robust against different usual and malicious attacks. The proposed method's superior performance emerges due to its multi-signature embedding and to its hybrid domain insertion. However, in order to prove these re-

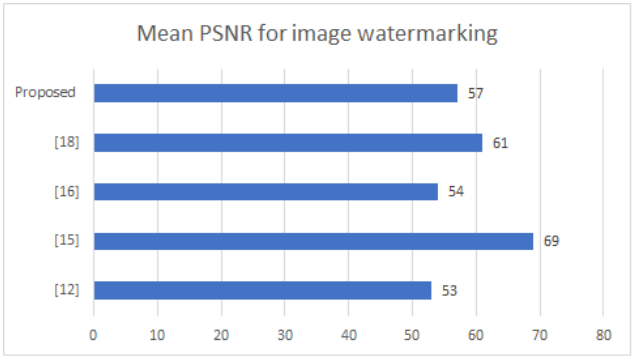

Fig. 12: Invisibility comparison for image watermarking.

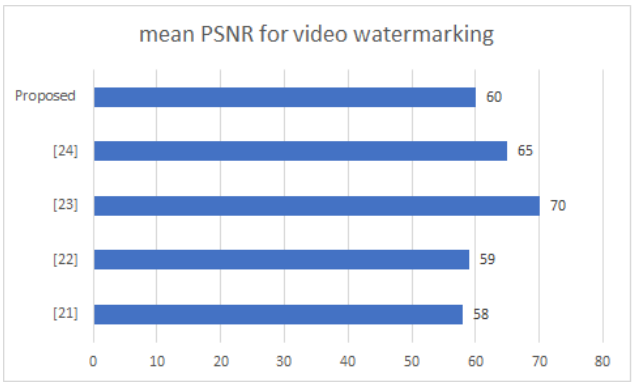

Fig. 13: Invisibility comparison for video watermarking.

sults, we compared the robustness of the proposed image and video watermarking with existing techniques performances.

Concerning image watermarking, table 8 summarizes the robustness comparison results. It confirms the efficiency of the suggested scheme which is robust to the most important manipulations done on image content, such as geometric attacks, filtering, noise, cropping, and JPEG compression. We note that the existing 3D anaglyph image watermarking is not robust against cropping. In figure 14, we present NC values obtained for all compared techniques for scaling, average filtering and rotation (50°). This figure shows that all techniques can resist these attacks. For cropping attack, we note that [12] and [15] are not robust to this attack. The proposed image watermarking approach presents the same performances of [6] where robustness against usual attacks and JPEG compression is achieved. However, the proposed approach outperforms [6] in cropping attack where detection can be achieved until a percentage of 70% with NC close to 0,7.

Concerning video watermarking, we note that only the proposed video watermarking is robust to the usual attacks and malicious attacks including collusion, MPEG

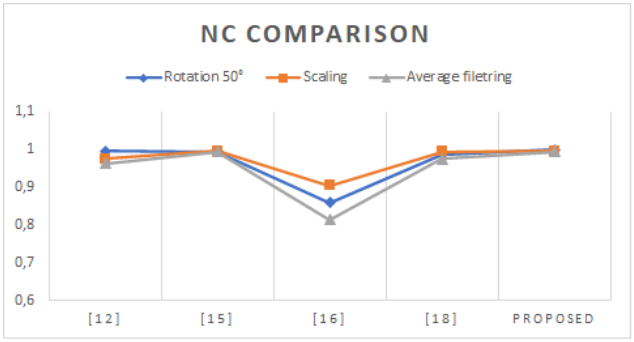

Fig. 14: NC comparison after scaling, rotation and average filtering.

and H264 compression. These performances are obtained thanks to the hybrid domain embedding and to the insertion of different signatures by different ways. Only the proposed approach and [23] are robust to H264 compression which is an important standard of coding these last years. For [20,21,22], they are not robust against this compression but they resist collusion attacks thanks to their embedding based on mosaic generation. The performances comparison between the proposed approach and the existing schemes is shown in table 7 where all characteristics of these techniques are detailed.

6.3 Capacity comparison

Concerning capacity, the proposed approach for image or video embeds three signatures : the first one is embedded into stereo pairs images before generation using DWT, the second one is embedded during generation step using LSB and the last one is embedded after generation using DCT based scheme. This multi-embedding allows obtaining a high capacity of the inserted signature. Table 7 compares the capacity of the signature between proposed and existing approach of anaglyph 3D image watermarking.

6.4 Execution timing & overall performances

The average embedding timing of the proposed image watermarking technique is 115.34 ms and the average extraction time is 152.21 ms. Our approach's timings are lower than [6] where embedding and extraction timings are 136.91 ms and 187.36 ms respectively. Concerning video watermarking, the execution timing depends on the total time of the host video. Furthermore, we noted that despite the advantages of the proposed approach, it presents only one drawback. In fact, the

Table 7: Capacity comparison

Technique	Content type	Signature capacity
[12]	Image	32×32
[15]	Image	32×32
[16]	Image	3232
[6]	Image	128×128
[20]	Video	160×50
[21]	Video	32×32
[22]	Video	32×32
[23]	Video	64×64
Proposed	Image + Video	64×64×3

proposed approach is applied on image and video before their transmission or storage for protecting them against attacks. Hence, it takes the stereo pairs images instead of the anaglyph image as input. If only anaglyph content is available, a reversing method should be applied to obtain stereo pairs.

Finally, a comprehensive comparison has been provided in Table 8, evaluating the proposed method against other approaches based on various criteria like embedding domain, technique, invisibility and robustness. In Table 8, it can be seen that the proposed technique outperforms all other competing methods.

7 Conclusion and future work

A robust, fast and imperceptible anaglyph 3D image and video watermarking scheme has been proposed in this paper. The suggested technique is the first anaglyph watermarking that embeds the signature simultaneously with the generation step in order to avoid generation deficiencies. To enhance robustness against most attacks, especially against malicious attacks, three signatures have been embedded before, during and after the generation process using different domains (DWT, spatial and DCT domains). In addition, the proposed technique is based on a complex embedding schema based on multi-embedding in a hybrid domain and using two different color spaces, which allows obtaining robustness against collusion because this makes the signature extraction very hard for the attacker.
Extensive qualitative and quantitative experiments were conducted on a specific anaglyph 3D video and image, affirming the resilience of the proposed approach against a range of tested attacks. These attacks include common manipulations such as geometric alterations, filtering, and noise, as well as temporal attacks like MPEG4 and H264 compression, and collusion. Furthermore, the visual quality has been confirmed by measuring the mean PSNR and SSIM where the obtained values are close to 58 dB and 0,8 respectively. This efficiency has been proven by comparing the suggested technique with existing anaglyph 3D image and video approaches in terms of invisibility and robustness.

As the proposed method is a first proposal that combines a generation and a watermarking process, it can be improved in order to maximize generation results and watermarking performances. In fact, watermarking step can be improved by using deep learning. In fact, deep learning based watermarking proved their efficiency compared to traditional techniques [40]. We can apply a CNN based watermarking either on the anaglyph image in the case of image watermarking or on the mosaic image generated from the host video. Moreover, the generation step can be improved by using a method which combines two generation classes in order to profit from the advantages of each class and minimize the deficiencies of generation process.

Author's contributions All authors contributed to the study conception and design, data collection and the experiments analysis.

Funding The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability The datasets analysed during the current study are available from the corresponding author upon reasonable request.

Declarations

Competing interests The authors declare that they have no competing interests.

References

1. Fan, B., Li, Z., Gao, J.: Dwimark: a multiscale robust deep watermarking framework for diffusion-weighted imaging images. Multimedia Systems pp. 1–16 (2021). DOI 10.1007/s00530-021-00835-0
2. Evsutin, O., Dzhanashia, K.: Watermarking schemes for digital images: Robustness overview. Signal Processing: Image Communication **100**, 116523 (2022). DOI 10.1016/j.image.2021.116523

Table 8: Comparison of anaglyph 3D image and video watermarking techniques

Ref	Media	Domain	Invisibility	Capacity	Robustness
[12]	image	DWT	++ 53	+	Filtering +noise + geometric attacks + histogram equalization + JPEG
[15]	image	PCA	+++ 69	+	Filtering +noise + geometric attacks + intensity adjustment + histogram equalization + JPEG
[16]	image	DWT + SVD	++ 54	+	Geometric attacks + noise + cropping + filtering
[6]	image	DST + MNF	+++ 61	++	Filtering +noise + geometric attacks histogram equalization + cropping + JPEG
[20]	video	DWT + spatial	+++ 58	++	Geometric attacks + noise + filtering + frame suppression + MPEG4 + collusion
[21]	video	DWT + spatial	+++ 59	+	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + collusion
[22]	video	DWT + spatial	+++ 70	+	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + collusion
[23]	video	DCT	+++ 65	++	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + H264 + collusion
Proposed	Image	DWT + spatial + DCT	+++ 57	+++	Geometric attacks + noise + cropping + filtering + JPEG + intensity adjustment + histogram equalization
Proposed	Video	DWT + spatial + DCT	+++ 60	+++	Geometric attacks + noise + cropping + frame-based attacks + filtering + MPEG4 + collusion +H264

3. Kerbiche, A., Ben Jabra, S., Zagrouba, E., Charvillat, V.: A robust video watermarking based on feature regions and crowdsourcing. Multimedia Tools and Applications **77**(20), 26769–26791 (2018). DOI 10.1007/s11042-018-5888-6
4. Bayoudh, I., Ben Jabra, S., Zagrouba, E.: Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications. Multimedia Tools and Applications **77**(11), 14361–14379 (2017). DOI 10.1007/s11042-017-5033-y
5. El-Shahed, R.A., Al-Berry, M.N., Ebied, H.M., Shedeed, H.A.: High capacity video hiding based on multi-resolution stationary wavelet transform and hybrid-matrix decomposition techniqueset transform and hybrid-matrix decomposition techniques. Bulletin of Electrical Engineering and Informatics **11**(4) (2022). DOI 10.11591/eei.v11i4.2922
6. Koley, S.: Bat optimized 3d anaglyph image watermarking based on maximum noise fraction in the digital shearlet domain. Multimedia Tools and Applications **81**(14), 19491–19523 (2022). DOI 10.1007/s11042-021-11861-5
7. Dhaou, D., Ben Jabra, S., Zagrouba, E.: A review on anaglyph 3d image and video watermarking. 3D Research **10**(2), 13 (2019). DOI 10.1007/s13319-019-0223-1
8. Patel, R., Parth, B.: Robust watermarking for anaglyph 3d images using dwt techniques. International Journal of Engineering and Technical Research (IJETR) **3**(6), 55–58 (2015)
9. Zadokar, S.R., Raskar, V.B., Shinde, S.V.: A digital watermarking for anaglyph 3d images. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 483–488 (2013). DOI 10.1109/ICACCI.2013.6637219
10. Sanjay R., Z., Ravindra B., R.: A robust dwt watermarking for 3d images. International Journal on Emerging Trends in Technology (IJETT) **2**(1), 210–214 (2015)
11. Prathap, I., Anitha, R.: Robust and blind watermarking scheme for three dimensional anaglyph images. Computers and Electrical Engineering **40**(1), 51–58 (2014). DOI 10.1016/j.compeleceng.2013.11.005
12. Devi, H.S., Singh, K.M.: A robust and optimized 3d red-cyan anaglyph blind image watermarking in the dwt domain. Contemporary Engineering Sciences **9**, 1575–1589 (2016). DOI 10.12988/ces.2016.69156
13. Munoz-Ramirez, D.O., Reyes-Reyes, R., Ponomaryov, V., Cruz-Ramos, C.: Invisible digital color watermarking technique in anaglyph 3d images. In: 12th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), pp. 1–6 (2015). DOI 10.1109/ICEEE.2015.7357955
14. Y, R., Krishna, D.R.: Digital watermarked anaglyph 3d images using frft. International Journal of Computer Trends and Technology (IJCTT) **41**(2), 77–80 (2016). DOI 10.14445/22312803/IJCTT-V41P113
15. Devi, H.S., Singh, K.M.: A novel, efficient, robust, and blind imperceptible 3d anaglyph image watermarking. Arabian Journal for Science and Engineering **42**(8), 3521–3533 (2017). DOI 10.1007/s13369-017-2531-1
16. Devi, H.S., Singh, K.M.: Red-cyan anaglyph image watermarking using dwt, hadamard transform and singular value decomposition for copyright protection. Journal of Information Security and Applications **50**, 102424 (2020). DOI https://doi.org/10.1016/j.jisa.2019.102424
17. Wang, C., Han, F., Zhuang, X.: Robust digital watermarking scheme of anaglyphic 3d for rgb color images. Int. J. Image Process.(IJIP) **9**(3), 156 (2015)

18. Waleed, J., Jun, H.D., Hameed, S., Hatem, H., Majeed, R.: Integral algorithm to embed imperceptible watermark into anaglyph 3d video. International Journal of Advancements in Computing Technology **5**(13), 163 (2013)
19. Salih, J.W., Abid, S.H., Hasan, T.M.: Imperceptible 3d video watermarking technique based on scene change detection. International Journal of Advanced Science and Technology **82**, 11–22 (2015). DOI 10.14257/ijast.2015.82.02
20. Dhaou, D., Ben Jabra, S., Zagrouba, E.: A multi-sprite based anaglyph 3d video watermarking approach robust against collusion. 3D Research **10**(2), 21 (2019). DOI 10.1007/s13319-019-0231-1
21. Dhaou., D., Ben Jabra., S., Zagrouba., E.: A robust anaglyph 3d video watermarking based on multi-sprite generation. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - SECRYPT,, pp. 260–267. INSTICC, SciTePress (2019). DOI 10.5220/0007930102600267
22. Dhaou, D., Ben Jabra, S., Zagrouba, E.: An invisible hybrid 3d video watermarking robust against malicious attacks. In: M.S. Obaidat (ed.) E-Business and Telecommunications, pp. 157–179. Springer International Publishing, Cham (2020). DOI 10.1007/978-3-030-52686-3_7
23. Jabra, S.B., Zagrouba, E.: Robust anaglyph 3d video watermarking based on cyan mosaic generation and dct insertion in krawtchouk moments. The Visual Computer pp. 1–15 (2021). DOI 10.1007/s00371-021-02191-6
24. Dhaou, D., Ben Jabra, S., Zagrouba, E.: An efficient group of pictures decomposition based watermarking for anaglyph 3d video. In: the 13th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2018, VISAPP), pp. 501–510 (2018). DOI 10.5220/0006619305010510
25. Dhaou, D., Ben Jabra, S., Zagrouba, E.: An efficient anaglyph 3d video watermarking approach based on hybrid insertion. In: International Conference on Computer Analysis of Images and Patterns, pp. 96–107. Springer (2019). DOI 10.1007/978-3-030-29891-3_9
26. Dubois, E.: A projection method to generate anaglyph stereo images. In: 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221), vol. 3, pp. 1661–1664. IEEE (2001). DOI 10.1109/ICASSP.2001.941256
27. McAllister, D.F., Zhou, Y., Sullivan, S.: Methods for computing color anaglyphs. In: Stereoscopic Displays and Applications XXI, vol. 7524, p. 75240S. International Society for Optics and Photonics (2010). DOI 10.1117/12.837163
28. Ideses, I., Yaroslavsky, L.: Three methods that improve the visual quality of colour anaglyphs. Journal of Optics A: Pure and Applied Optics **7**(12), 755 (2005). DOI 10.1088/1464-4258/7/12/008
29. Sanftmann, H., Weiskopf, D.: Anaglyph stereo without ghosting. In: Computer Graphics Forum, vol. 30, pp. 1251–1259. Wiley Online Library (2011). DOI 10.1111/j.1467-8659.2011.01984.x
30. Li, S., Ma, L., Ngan, K.N.: Anaglyph image generation by matching color appearance attributes. Signal Processing: Image Communication **28**(6), 597–607 (2013). DOI 10.1016/j.image.2013.03.004
31. McAllister, D.F., Zhou, Y., Sullivan, S.: Methods for computing color anaglyphs. In: Stereoscopic Displays and Applications XXI, vol. 7524, p. 75240S. International Society for Optics and Photonics (2010). DOI 10.1117/12.837163
32. Matsuura, F., Fujisawa, N.: Anaglyph stereo visualization by the use of a single image and depth information. Journal of visualization **11**(1), 79–86 (2008). DOI 10.1007/BF03181917
33. Diaz, E.R., Ponomaryov, V.: Reconstruction of 3d video from 2d real-life sequences. Revista Facultad de Ingeniería Universidad de Antioquia (56), 111–121 (2010)
34. Lu, Z., ur Réhman, S., Khan, M.S.L., Li, H.: Anaglyph 3d stereoscopic visualization of 2d video based on fundamental matrix. In: 2013 International Conference on Virtual Reality and Visualization, pp. 305–308. IEEE (2013). DOI 10.1109/ICVRV.2013.59
35. Jain, K., Raju, U.: A digital video watermarking algorithm based on lsb and dct. Journal of Information Security Research **6**(3) (2015)
36. Anaglyph video dataset. URL `https://www.youtube.com/playlist?list=PLuAqFR-aKaxh0ThTiZhJrVDHu1y058Dvj`
37. Zingarelli, M.R.U., Andrade, L.A.d., Goularte, R.: Reversing anaglyph videos into stereo pairs. In: Proceedings of the 17th Brazilian Symposium on Multimedia and the Web on Brazilian Symposium on Multimedia and the Web - Volume 1, p. 205–212. Brazilian Computer Society, Porto Alegre, BRA (2011)
38. Kunze, L.F., Goularte, R., de Sousa, E.P.M.: Sira - an efficient method for retrieving stereo images from anaglyphs. Signal Processing: Image Communication **85**, 115866 (2020). DOI https://doi.org/10.1016/j.image.2020.115866
39. Manaf, A.A., Boroujerdizade, A., Mousavi, S.M.: Collusion-resistant digital video watermarking for copyright protection application. International Journal of Applied Engineering Research **11**(5), 3484–3495 (2016)
40. Kaczyński, M., Piotrowski, Z.: High-quality video watermarking based on deep neural networks and adjustable subsquares properties algorithm. Sensors **22**(14), 5376 (2022). DOI https://doi.org/10.3390/s22145376