Multimedia Tools and Applications (2021) 80:20449–20476
https://doi.org/10.1007/s11042-021-10730-5

A secure method in digital video watermarking with transform domain algorithms

Mohammad Reza Keyvanpour[1] · Neda Khanbani[2] · Mahsa Boreiry[2]

Received: 13 September 2020 / Revised: 25 January 2021 / Accepted: 16 February 2021 /
Published online: 6 March 2021

Abstract
One of the problems in the digital world is the secure transmission of information through insecure communication channels which has been selected as the main concept discussed in this research. This article, by thoroughly analyzing the types of attacks in video watermarking, learns the basics used in the proposed method and offers a solution to deal with the most important categories. Therefore, it presents a secure solution against collusion attacks by introducing a three-dimensional discrete cosine transform algorithm. According to the evaluations, it can be claimed that the proposed solution is resistant to collusion attacks, which is the most important attack in the field of digital watermarking. Another strength of the proposed algorithm compared to other methods is its higher capacity in watermarking. The proposed algorithm, using its special blocking method, has the ability to cover all types of video, both dynamic and static. Various tests have been applied to the selected dataset to analyze the security and the performance of the proposed algorithm. The results show that if the proposed algorithm is used in watermarking, in addition to high accuracy, it can have an acceptable resistance to attacks.

Keywords Security · Discrete cosine transform · Watermark · Digital video Watermarking · Collusion attacks

✉ Mohammad Reza Keyvanpour
keyvanpour@alzahra.ac.ir

Neda Khanbani
neda.khanbani@yahoo.com

Mahsa Boreiry
mahsa.boreiri@yahoo.com

[1] Department of Computer Engineering, Alzahra University, Tehran, Iran

[2] Data mining Lab, Department of computer Engineering, Alzahra University, Tehran, Iran

1 Introduction

High-speed computer networks, the Internet, and web pages have revolutionized the distribution of digital data. Explosion of digital multimedia products results in rigid demand on security and authenticity of private digital contents [44]. Therefore, it is predicted that more music, movies and images will be transferred on the Internet day by day and the download sales of multimedia will exceed their traditional sales [37]. Watermarking technology has excellent applications in various aspects of social development, such as privacy protection, military, communication, identity identification, media file archiving, etc. Encryption methods alone can not prevent the unauthorized use of digital products, the main problem of these methods is that after the transfer and delivery of data, no monitoring is done on the content and the legal recipient data can be easily reproduced and distributed. In addition, the real owner will not be able to trace those responsible for the illegal duplication of their data. With regard to these issues, the need to choose an appropriate method for permanent protection of multimedia content during the transfer and after the delivery of information is of high importance and digital watermarking methods are discussed [2, 40].

Watermark is a piece digital data that is inserted into multimedia objects; watermark is extracted and visible when we want to prove a claim about that object. [7]. Depending on the content of the host, digital watermarking is divided into three categories: image watermarking (image as a mapping of two-dimensional space), video watermarking, and audio watermarking (one-dimensional media over time) [2]. Video watermarking faces more challenges than image watermarking. Video data is inherently more diffused between their frames. Imbalance between moving and stationary areas, and limitations due to the instantaneous nature of video during playback, causes coded video sequences to withstand attacks such as lossy compression, frame change, parsing. Moreover, statistical analysis and digital-to-analog and analog-to-digital conversions are more sensitive [30]. The complete process of video watermarking can be explained in four stages: attachment or embedding of the watermark, sending or distributing the watermark through the channel, extraction or detection of the watermark and decision making [22].

One of the challenges that video watermarking faces is attacks. The main question of this article is how to use a conversion domain algorithms to present a watermarking method with higher security and more resistance to all kinds of attacks, especially collusion attacks which are among the most important types of attacks in the field of video watermarking [5, 9]. One of the practical purposes of this article is to prevent illegal copying of new films that are being shown on the cinema screens. It is possible to identify the guilty cinema by embedding a separate watermark for each cinema, in case of any problems and the distribution of the film.

One of the most important types of attacks in the field of video watermarking is collusion attacks. In this paper, a method resistant to the aforementioned attacks will be developed using conversion domain algorithms. The proposed method allows us to customize each copy for the recipient. This requires that we have a unique watermark for each copy, for example a customer ID or customer name. The customer ID is inserted as a watermark in the video, which can be used to track the user's non-compliance with the rules [31].

In general, performance metrics for having strong watermarking can be expressed as follows: stability, intangibility, capacity, and security. Relative achievement of any of the above criteria can be considered as one of the main goals of providing a useful algorithm in the field of watermarking. Among these, the main purpose of this article is to focus on the fourth criterion, i.e. having the ability to provide the required security in the application, which has a close conceptual relationship with the first criterion, namely stability.

In this research, we present a secure method for digital video watermarking using conversion domain algorithms called SCDW_CD. The innovations are as follows:

- Proposed preprocessing algorithm BED_CP: In this section, the advantage of three innovations hasbeen taken. Case 1) The first case is to calculate the minimum and maximum block length in this method, so that the security of the watermarking is maintained and it will be more resistant to attacks. Case 2) The proposed blocking algorithm does not depend on the type of input video and changes the number of blocks extracted by changing the alpha value. In this algorithm, not only dynamic videos are still blocked with the quality of the past, but also the scope of video coverage is increased and static videos are included in the scope. Case 3) The block end detector in the proposed algorithm performs the detection operation based on comparing the pixels of each block with the pixel values of the first frame in the block. The advantage of this method is that it ignores small changes but recognizes the path as a block by moving the main object in the video away from its original state.
- Proposed watermarking embedding algorithm WE_EP: In the section of marking the selected pixels in each frame, we use the human visual system (HSV) and select the host pixels from the edge pixels.

In this article, first, the related work is presented in Section 2. Then, in Section 3, the proposed method will be presented in detail. Section 4 presents the experimental results. Finally, in Section 5, we present the general conclusion.

2 Related works

In general, watermarking methods can be divided based on the range of embedding into spatial methods (pixel domain approach), spectral methods (conversion domain approach), and compression methods (compact domain approach). This article focuses on methods based on spatial embedding [7].

Domain space technologies are technologies that embed watermarks by directly changing the pixels of the host image. Some common algorithms of domain space technologies include low-bit (LSB) and forty-bit bit conversion and texture block encoding, and so on. The most important form of domain space technology is optimism. It is very difficult for domain space watermarks to survive attacks such as loss, compression, and low-pass filtering, and the information that can be embedded in domain space is very limited [18]. In recent years, these technologies have been largely abandoned. Low computer simplicity and complexity are the advantages of pixel-based methods. Therefore, most of these methods are used in real-time applications. Watermark optimization using spatial analysis methods alone is very difficult [45]. The LSB method is the most advanced method for embedding watermarking in this field. Although somewhat resistant to shear attacks, adding a little noise, loss, or compression is sufficient to break the watermark [21, 22, 34].

Compared to domain space watermarking, frequency domain watermarking is stronger and more compatible with general image compression methods and standards. Therefore, frequency domain watermarking has received more attention.In this category of methods, frequency transformations are applied to the data host when embedding the watermark, and then embedded in the host data by changing the watermark coefficients. Image frequency

transformations include discrete Fourier transform (DFT) and discrete cosine transform (DCT) [23, 31].

One of the major challenges in cryptographic methods is how to increase the security rate of the implemented system. The main proposed solution in this field is the use of cryptographic techniques [38] which has used the turbulence method and especially turbulence mapping that can be returned to the original state. In this regard, he introduced two famous recursive and Arnold mappings and examined how to change the methods of image watermarking, both blind and conscious, if the Ashobgon cryptographic key is used.

Different from other block selection rules devised by subjective evaluation means, in [29] selection rule aims to retain the image quality as much as possible from the source. Furthermore, information entropy is utilized to achieve the purpose of adaptive embedding. In the experiment, the proposed watermarking scheme is tested under several attacks, such as noise attack, JPEG compression, blurring, sharping, and etc. Finally, the proposed watermarking scheme is compared with other existing schemes, and the experimental results demonstrate the robustness, imperceptibility and superior of the proposed watermarking scheme.

Many scholars have proposed some algorithms for video watermarking based on the difference between video and images. Agilandeeswari, L et al. [13] presented a video watermarking algorithm based on bidirectional associative memory network. The algorithm input the watermark information and the random sequence into the network to obtain the weight matrix, so as to encrypt the watermark information. The simulation results demonstrated that the scheme had good robustness and imperceptibility. Aree A. Mohammed and Nyaz A. Ali [2] raised a video watermarking technique based on efficient video coding. Simulation experiments were carried out using videos with different resolutions (1 k, 2 k, 4 k).

The tolerance degree of watermarking methods to perturbations, which can occur in any of the steps of the watermarking process, is discussed in [45]. This paper proposes the use of self-similarity in the fractal concepts of images in order to search for the safe locations needed to embed the watermark. Based on the results of tests performed in the implementation phase, this method has an acceptable accuracy in the face of geometric attacks, especially compression operations.

The first efficient watermarking project was introduced by Koch et al. In their method, for DCT calculations, the image is first divided into square blocks in size 8*8 [22]. In conversion methods, the host signals are converted in different amplitudes and the watermark is embedded in the selected coefficients. Common methodologies are DCT cosine conversion coefficients and DWT wavelet transform coefficients [13].

DCT cosmic transformation and Fourier DFT discrete transformation and DWT wavelet discrete transformation are the three main methods for data conversion. In conversion domain methods, the cursor is embedded distributively throughout the original data domain. The Chinese authors then presented an algorithm based on embedding an image watermark three times in a row in three different frequency bands called Low, Medium, and High. The result showed that the watermark embedded with this method is resistant to low-pass, mid-pass and high-pass filters and is not completely destroyed [45].

The best advantage of these methods is that they can use alternating domain properties to fix the limitations of pixel-based methods to support a number of additional capabilities. Generally, the main problem with domain methods is that they require complex calculations [45].

3 The proposed algorithm of the secure video digital watermarking using conversion domain algorithm (SVDW_CD)

The proposed SCDW_CD algorithm receives the raw video, the watermark, and the key from the input and produces the watermarked video as output. From the beginning, the focus has been on the use of cinema, so for example, the produced film file can be considered as input. The QR code specific to each cinema is used as a receiver. When the film is delivered to the cinema, a special QR code is generated and embedded in the host. In case of any problem, this watermark is extracted from the host data and is known as the faulty cinema. In addition to these two inputs, a key is used to select the host blocks.

Therefore, the watermarking phase can be divided into two sub-phases of preprocessing and embedding the watermark. The watermarking will be used as input to both phases, but the switch will be used as input in the preprocessing phase. In the preprocessing stage, after selecting the host blocks, these blocks will be sent as input to the cache embedding phase in the host and the key will not play a role in the second phase. The proposed watermarking algorithm diagram is shown in Fig. (1). In the following, we will describe the steps of the proposed SVDW_CD algorithm. In all the diagrams used, the steps in the two-line boxes are the proposed algorithms, and the single-line boxes are the algorithms used.

3.1 Preprocessing using the proposed algorithm BED_CP[1]

In the preprocessing phase, raw video, keys, and watermarking are used as input to select the host blocks. The preprocessing stage diagram is shown in Fig. (2). First, we receive the raw video as input and extract its frames and number them. This phase is done in two stages, which are described below.

3.1.1 Calculate and determine default values

In this step, the fixed values of the video type and the maximum and minimum block length are calculated. These values are used for video blocking in the next step. This function extracts the fixed values required to select the host blocks (video type and minimum and maximum block length) as output by receiving the frames extracted in the previous step and watermarking. This step itself, as shown in Fig. (3), consists of the following three steps, which are described below:

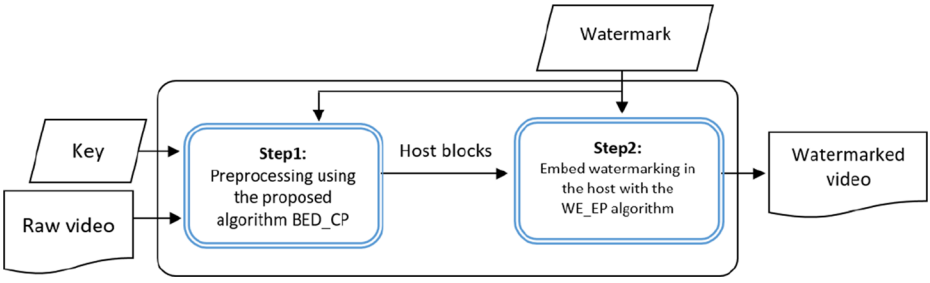


Fig. 1 Video watermarking diagram in the proposed SCDW_CD algorithm

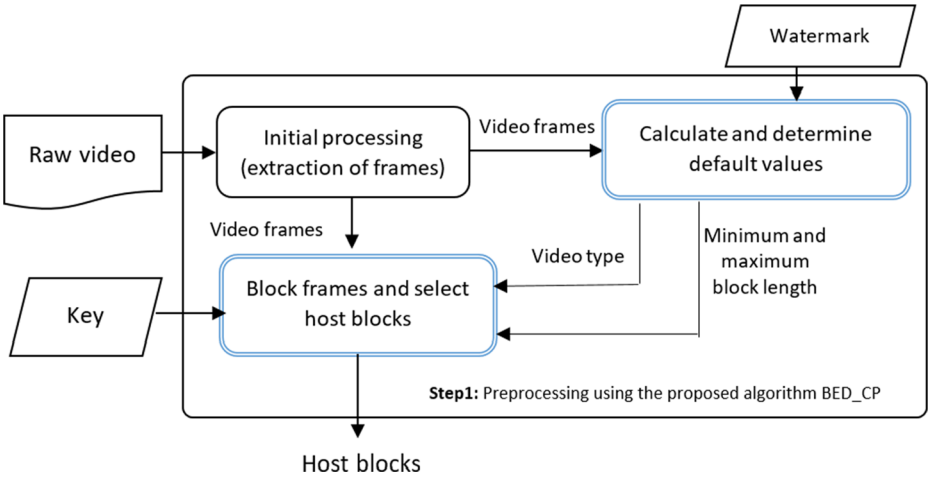


Fig. 2 Preprocessing phase diagram of the proposed algorithm BED_DP

- ***Calculate the minimum and maximum block length***

Small and large blocks are equally dangerous in our work. At this stage, we try to calculate this interval. Block sizes based on frequency-based algorithms use 8×8 blocks to hide a pixel. Therefore, the default watermark size is 1/8 video frame size [11, 24].

Maximum and minimum block length values are calculated according to Eqs. (1) to (4) [11, 17]. Assuming that each frame of the block must contain at least one pixel of the watermark, the maximum length of the block is equal to the number of the watermark pixels.

$$MaxBlockLength = \frac{I_{0x}}{8} \times \frac{I_{0y}}{8} = w_x \times w_y \tag{1}$$

In the above relation, I_{0x} and I_{0y} represent the width and length of the first host video frame, respectively, and w_x and w_y represent the width and length of the watermark, respectively.

The minimum amount of block length, by taking into account the condition of non-adjacency of the host frame blocks (due to the principle of similarity of adjacent pixels in each frame and more balanced distribution of cached pixels) was calculated based on Eq. (4).

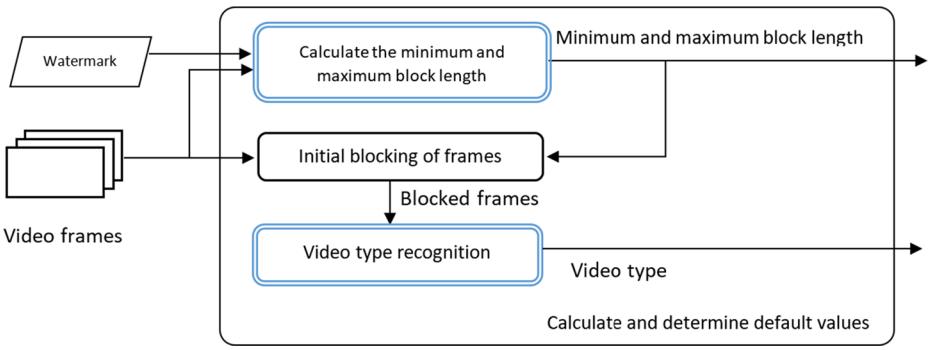


Fig. 3 Diagram of the calculation step and determination of default values

$$\forall x, y \in Even \rightarrow FrameCapacity = \frac{\left(\frac{x}{8}\right)}{2} \times \frac{\left(\frac{y}{8}\right)}{2} \tag{2}$$

$$\forall x, y \in Odd \rightarrow FrameCapacity = \left(\frac{\left(\frac{x}{8}\right)+1}{2}\right) \times \left(\frac{\left(\frac{y}{8}\right)+1}{2}\right) \tag{3}$$

$$MinBlockLength = \frac{w_x \times w_y}{FrameCapacity} \tag{4}$$

- ***Initial blocking of frames***

As mentioned earlier, in this study, the input videos are divided into two categories: fixed and variable videos. If the scene change in the input video is done slowly, the input video type will be fixed, otherwise it will be variable. To identify the type of video, assuming that dynamic scenes exists, the video frames were blocked according to formula (5) [15].

$$MAD_t = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |I_{t+1}(x,y) - I_t(x,y)| \tag{5}$$

Where the values M and N represent the pixels and the frame number respectively. If the calculated value of MAD_tcalculated is greater than the fixed value $\propto$ intended to change the scene, the frame $I_t$is considered as the final frame of the previous block and the frame I_{t+1} is the initial frame of the next block [7, 8, 14].

This step is considered the preprocessing step and is used to calculate default values such as minimum and maximum block length and video type. The blocks generated in this step are used in the next step to identify the type of video.

- ***video type recognition***

The type of input video is one of the most important and fixed parameters during the program and some decisions are made automatically based on this parameter. This step is considered as the preprocessing phase to calculate the required values. The video type recognition algorithm is shown in Fig. (4).

3.1.2 Framing blocks and selecting host blocks

In this step, first the video is converted to video blocks with variable length based on the end-of-block detection function and then based on the video type (fixed or dynamic) and the minimum and maximum values of the block length calculated in the previous step, and the input key selects host blocks as the output. The watermark is embedded in all the selected blocks. During extraction, if the extraction of the watermark from a block is difficult, the remaining blocks are used as a host alternative. The diagram of this step is illustrated in Fig. (5). In the following, each of the 2 stages of this phase will be examined:

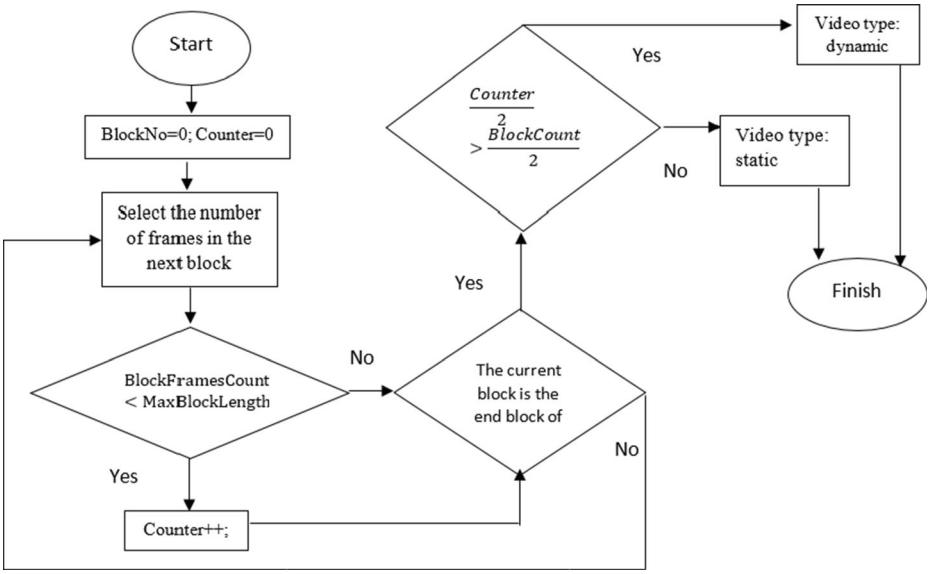


Fig. 4 Flowchart of video type recognition algorithm

- ***Block end detector***

The proposed blocking algorithm in [3, 43] determines the recognition of the end of the block based on the scene change. In the proposed algorithm, depending on the type of host video, if the host video scenes are quiet and without any scene change, the block end detection function performs the detection operation based on comparing the pixels of each block with the pixel values of the first frame in the block. The advantage of this algorithm is that it ignores small changes but recognizes this path as a block by moving the main object in the video away from its original state. In the proposed algorithm, the block end recognition is calculated based on formula (6). If the calculated value is greater than the constant value of α, frame t is considered as the end frame of the block and frame $t+1$ is considered as the starting frame of the next block.

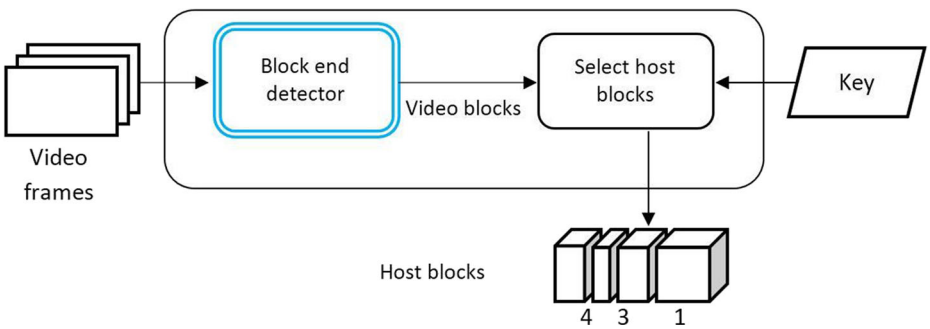


Fig. 5 Blocking frames and selecting host blocks

$$MAD_t = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |I_{t+1}(x,y) - I_0(x,y)| \tag{6}$$

- ***Select host blocks***

As mentioned earlier, the invisibility of the watermark is one of its important features and there is always a compromise between the volume of the watermark embedded in the host and its invisibility. Due to this issue, if the number of block frames extracted in the previous step is small, the share of each frame in the watermark becomes a large number and, of course, affects the invisibility of the watermark. To prevent this from happening, at this stage the blocks whose length is less than the minimum value of the block length are considered as noise and are removed, and among the remaining blocks, the host blocks by making use of the key are selected according to formula (7) [4, 39].

$$BlockIsHost \rightarrow \frac{block\ no}{key} = 0 \tag{7}$$

3.2 Embedding the watermark in the host with algorithmWE_EP[2]

In this step, the watermark is embedded in the selected blocks in the previous step. The main processing step is done in three phases: selection of host pixels, watermarking and connection of frames. The host pixel selection section in each block has two inputs: the host blocks (selected **from the &quot**;Select host blocks" step) and the watermark, which is a binary image and a QR code containing the recipient ID.. The output of this step is marked blocks. These blocks are used as input to the 3D-DCT watermarking phase [27, 42]. In this step, the watermarking is done on each frame according to the host pixels, the watermarked frames are connected in the next step and finally it produces the watermarked video as output. To better understand this step, its diagram is illustrated in Fig. (6). In the following, all these three steps will be described in more detail.

3.2.1 Selecting the host pixels in each block

Once the host blocks have been identified, it is time to select the host pixels in each frame. We use the HVS human vision system to select the host pixels from all the frame pixels. In this step, all the host blocks are taken as input and marked using the host pixel watermark for each frame in the block. The output of this step are blocks containing marked frames. The diagram of this step is shown in Fig. (7). The details of each of the two sub-steps of this step are described below.

- ***Marking the selected pixels in each frame of the block***

In this step, the host pixels are selected from all the pixels in each frame. We use the human visual system (HVS) to select the host pixels. In this study, we select the host pixels from the

[2] Watermark Embedding with using Edge Pixels

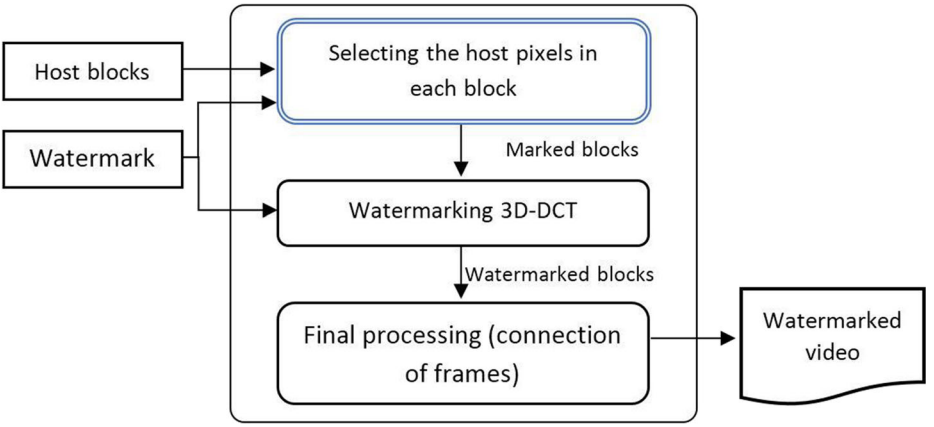


Fig. 6 Embedding a watermark in a host with the WE_EP algorithm

edge pixels. And because the viewer is more focused on the person talking and to prevent the image quality from deteriorating, we remove the facial pixels from the host pixel set. From the set of the remaining pixels, the ones with the highest intensity are selected as hosts. In the following, we will describe and review each step of this algorithm.

Calculating the share of each frame of the watermark In the proposed algorithm for embedding the watermark, one frame will not be used as the host, but the whole block will be our host and the watermark will be spread throughout the block. Due to the variability of block length, based on the number of frames in the current block and the number of watermark pixels, the share of each frame of the watermark is calculated according to Eq. (8):

$$EF = {}^{NP}/_{NF} \tag{8}$$

In Eq. 8, EF means the share of each watermark frame, NP, the number of watermark pixels, and NF, the number of current block frames.

Detection of animated pixels To make the watermark more secure and to prevent some attacks based on guessing the true value of the pixel, fixed pixels will be chosen as the host and animated pixels will be used as the host. Moving pixels in each frame can be obtained by using

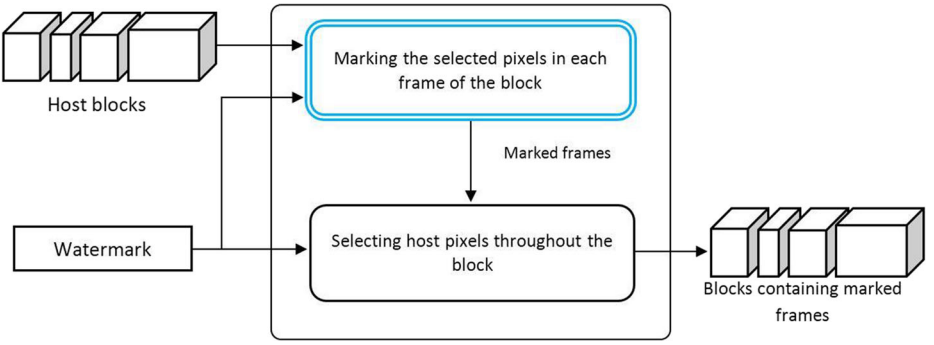


Fig. 7 Selecting the host pixels in each block

the corresponding difference between the pixels in the current frame and the previous frame [1].

Elimination of facial pixels Due to the advanced features of the human visual system (HVS), in moving scenes, the viewer focuses more on moving objects in the scene, and if a moving object is talking, the viewer focuses on the person, especially on a person's face. For this reason, in the proposed algorithm, in order to maintain the invisibility feature of the cantilever, at this stage the facial pixels are removed from the host pixel set.

Detection of sharp pixels Image pixels can be divided into two general categories: sharp pixels and smooth pixels. Sharp pixels are pixels that have a large difference in brightness with neighboring pixels. Sharp pixels represent the edges of objects in the image and its noise, and in general the details of the image are shown using sharp pixels. As mentioned earlier, due to the human visual system and the phenomenon of coating, the choice of sharp pixels as the host helps to increase the invisibility of the watermark. The output of this step is the marked frames.

- ***Selecting host pixels throughout the block***

Among all the edge pixels, we need host pixels for the number of current frames of the watermark. To select these pixels from the set of pixels in the frame, we use the brightest pixels with the maximum intensity for watermarking. By arranging the bright pixels of the image based on the maximum difference, the required number of pixels per frame is selected.

3.2.2 Watermarking 3D-DCT

After using the selected pixels in the previous part, the watermark is embedded in the host blocks by a three-dimensional discrete cosine algorithm. The variable X is a 3D signal of size m in n at t, whichis assigned to a set of consecutive video frames. The variable Y is also 3D DCT, X with size m in n in t. Since 3D DCT is a separate function, the above expressions can be evaluated by converting 1D DCT along each of the three X dimensions [35]. The Y matrix can be calculated using Eq. (9):

$$Y_{kij} = \alpha_k \alpha_i \alpha_j \sum_{t=0}^{N_f-1} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X_{tmn} \cos\frac{\pi(2t+1)k}{2N_f} \cdot \cos\frac{\pi(2m+1)i}{2M} \cdot \cos\frac{\pi(2n+1)j}{2N}$$

$$\alpha_k = \begin{cases} \frac{1}{\sqrt{T}}, & k = 0 \\ \frac{2}{\sqrt{T}}, & else \end{cases}, \quad \alpha_i = \begin{cases} \frac{1}{\sqrt{M}}, & i = 0 \\ \frac{2}{\sqrt{M}}, & else \end{cases}, \quad \alpha_j = \begin{cases} \frac{1}{\sqrt{N}}, & j = 0 \\ \frac{2}{\sqrt{N}}, & else \end{cases} \tag{9}$$

3.2.3 Watermarking extraction

To extract the watermark, first the frames are extracted and all forms are blocked using the scene change detection algorithm, then the host blocks are detected using the key and a block is selected as the host block for watermark extraction. In this step, as in the watermarking step, the share of each frame of the watermark is calculated and after

identifying the edge and host pixels, their value is compared with the initial value. If the pixel value is more than the initial value, the watermark pixel value is equal to one and otherwise equal to zero. This operation is performed up to the last frame of the block and all cache pixels are extracted.

The extraction process for the 8 * 8 block can be described using Eq. 10 [25, 32]:

$$\begin{aligned} \Delta I_{DCT} &= I_{DCT_W}(i,j) - I_{DCT_{Original}}(i,j), \\ W_P(s) &= \begin{cases} 1 & ak \quad \Delta I_{DCT} > 0 \\ 0 & ak \quad \Delta I_{DCT} \leq 0 \end{cases} \end{aligned} \tag{10}$$

$\Delta I_{DCT}$is the difference between the coefficientI_{DCT_W}, the selected DCT and the coefficient $I_{DCT_{Original}}$, the original DCT with coordinates i and j.$W_P(s)$, s is the first bit of the watermark. To reverse the watermark, the reverse shift function must be performed.

After extracting the values of zero to pixels with white color and the values of one to pixels with black color, the watermark image is reconstructed. To ensure the accuracy of the extracted watermark, we consider another block as the host and perform this operation on it. If the two extracted watermarks do not match, we detect an attack on the host data and perform this operation on all blocks for more security. Other blocks are used as backup blocks. In addition to the QR code features, we can mention the Reed-Solomon error correction feature, which has a different ability to fix errors at different levels. In general, these barcodes are 7 to 30% correctable and often do not have problems when decrypting. In addition, they are resistant to rotational attacks. This category of attacks does not cause problems in extracting the content of this code [6, 16, 26].

4 Experimental results

The implementation of the proposed SCDW_CD algorithm has been done in the phase of embedding and extracting the watermark, the attack phase of statistical averaging and extracting the watermark in the net-based platform and the Visual Studio 2015 environment. All implementation steps are done in Visual Studio 2015 using C # language. Finally, in order to analyze and display the extracted values in the diagram, MATLAB software has been used.

4.1 Evaluation criteria

There are different criteria for comparing the similarity and quality of images. According to the quality evaluation criteria in [10, 19, 26, 36], in this study, in order to compare the performance results, we examine the obtained values with MSE, NC and PSNR criteria.

- Criteria for checking the similarity of two PSNR images

One of the evaluation criteria used to evaluate the quality of extraction operations is the PSNR criterion, which is defined as a criterion for evaluating and comparing the degree of similarity in the quality of the original image and the image that has been changed [26, 36]. The PSNR criterion is introduced in Eq. (11) and its value is appropriate if it is approximately in the range of 30–50 db and it can be claimed that the changes applied by the human visual system are not recognisable.

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{I_H \times I_w} \sum_{x=0}^{I_H-1} \sum_{y=0}^{I_w-1} [f(x,y) - g(x,y)]^2} \tag{11}$$

In relation (11) I_H and I_w are the length and width of the image, respectively, and $f(x, y)$ and $g(x, y)$ are the values that are in place (i, j) in the original and modified image matrix.

- Criteria for evaluating the quality of extracted NC watermark

In order to evaluate the quality of the extracted watermark image, the NC criterion can be used [10, 26, 33]. Which is calculated according to Eq. (12).

$$\mathrm{NC} = \frac{\sum_{i=0}^{I_H-1} \sum_{j=0}^{I_w-1} W_{ij} W'_{ij}}{\sum_{i=0}^{I_H-1} \sum_{j=0}^{I_w-1} (W_{ij})^2} \tag{12}$$

Where W_ij is the pixel value of the main watermark in the coordinates i, j, and 〚W‘〛_ij is the pixel value of the watermark extracted in those coordinates. The closer the NC value is to 1, the better the quality of the extracted image.

4.2 DataSets

In terms of scene change, videos are divided into three general categories namely static videos, semi-static videos, and dynamic videos. Static videos are a category in which the scene changes slowly. In semi-static videos, a part of the image has slow changes and the other part has sudden changes, and dynamic videos are sudden scene changes. In order to fully cover the videos, one video from each category was selected as a sample and experiments were performed on each of the sample videos.

In addition, the selection of the dataset is to compare the proposed SCDW_CD algorithm with the proposed algorithms in [10, 19, 26, 36]. The selected dataset consists of 3 raw videos in Y4M format with a resolution of 352 × 288, which is shown in Fig. (8).

4.3 The selected watermark

As mentioned earlier, in this experiment we will use the QR code generated for each recipient of the work as the identifier. This code is a binary image and is watermarked by being converted to zero and one and changing the host data coefficients. Also, due to the error

Foreman (dynamic video) **News (semi-static video)** **Akiyo(static video)**

Fig. 8 Dataset used in the experiment

correction capability in this code, we can be more hopeful of recovering the extracted watermark after multiple attacks.For this experiment, the website address of Al-Zahra University (https://www.alzahra.ac.ir/) has been used as the QR code address. The size of the watermark is considered to be 44×36 according to the resolution of the host data image (1/8 of the host data size). The watermark used in this experiment is shown in Fig. (9).

4.4 Extracting default values

As mentioned in the previous section, fixed values of the video type and the maximum and minimum block lengths are calculated before the start of the watermarking step. These values are used to block video in the next step. The results are shown in Table (1).

4.5 First test: The quality of the blocking function

First, the proposed algorithm in the blocking stage is checked and the quality of this algorithm is compared with the previous algorithm [26] and its acceptability is evaluated. The test method in this section is in accordance with the test methods used in the research [26], which is among the most widely used articles in this field.

In the blocking step, according to the fixed values obtained in the previous step, the extracted frames of each video are blocked using the proposed scene recognition algorithm and the host blocks are selected using the watermark key. When blocking, the maximum value of the block length is always considered. If the block length reaches the maximum value, regardless of the calculated circuit, the end-of-block recognition function declares the end of the block.

In the noise block removal step, using the default values calculated in the previous step, blocks with a block length less than the allowable value are considered as noise and are removed from the host block set. Finally, using the key, the host blocks are selected and ready for watermarking. The values obtained are shown in Table (2).

The host blocks are renumbered after removing the noise blocks and the new number of each block is mapped on it. The host blocks are selected based on the new number assigned to

Fig. 9 Watermark (QR Code, size 36×44)

Table 1 Default values calculated for extracting host blocks

video	Number of frames	Minimum block length	Maximum block length	Number of blocks	Video type
Akiyo	150	4	1584	1	Static
News	150	4	1584	3	Semi-static
Foreman	150	4	1584	5	Dynamic

them. After selecting the desired block with its initial number, it is sent to the next step as the host block (in this implementation, the key value is considered equal to 3).

As shown in Table (2), in the proposed algorithm, by changing the alpha value, a desired number of blocks can be extracted from the host video, which of course varies according to the changes in the scene in the host video and its type. However, in the previous blocking algorithm, only one block is extracted from static videos and only the number of noise blocks increases by changing the alpha value.

- ***Discussion***

Figure (10) shows a comparison of the extracted blocks in the proposed SCDW_CD algorithm and the previous algorithm. As shown in Fig. 10, in the previous algorithm, by reducing or increasing the alpha value in static videos such as Akyio, we still see a block in the extracted blocks, but in the case of dynamic videos, this algorithm is efficient and by increasing or decreasing the alpha value, the number of host blocks will change. In the proposed SCDW_CD algorithm, in both static and dynamic videos, increasing or decreasing the alpha value allows you to change the number of host blocks. Like the previous algorithm, as can be seen, by increasing or decreasing the alpha value, the number of host blocks in the two dynamic videos of News and Foreman remained constant and did not play. In our proposed SCDW_CD algorithm, we claim that the blocking algorithm does not depend on the type of input video and changes the number of blocks extracted by changing the alpha value. In fact, due to the automatic detection of the video type in the preprocessing stage, in later stages, decisions will be easily made with this input parameter. In this algorithm, not only dynamic videos are still blocked with the quality of the past, but also the coverage area of videos is increased and static videos are also included in the domain. This can be considered as an improvement for blocking. Coverage of all types of video is a positive feature of the proposed algorithm.

Table 2 Selection of host blocks

video	Alpha value	Number of blocks extracted	Number of blocks deleted	Number of host blocks	Key	Host blocks
Akiyo	39	11	0	11	3	3,6,9
News	100	11	2	9	3	3,7,10
Foreman	400	11	4	7	3	3,10

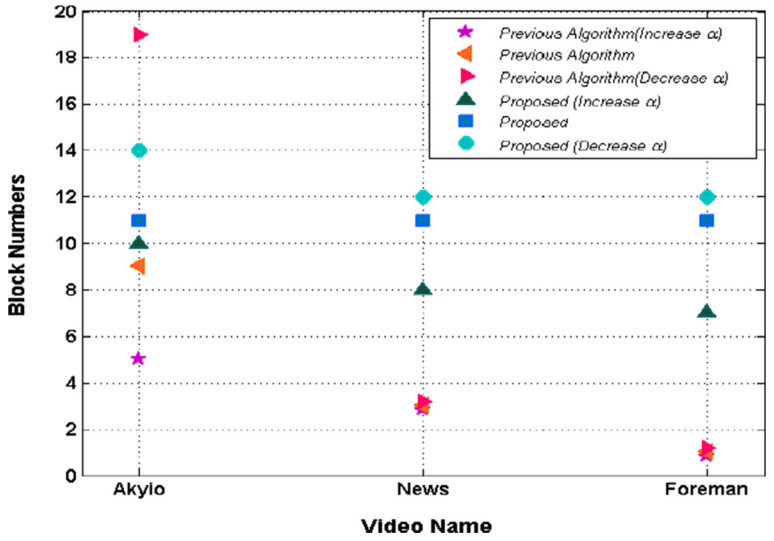


Fig. 10 Comparison of extracted blocks in the proposed SVDW_CD algorithm and previous algorithms [26]

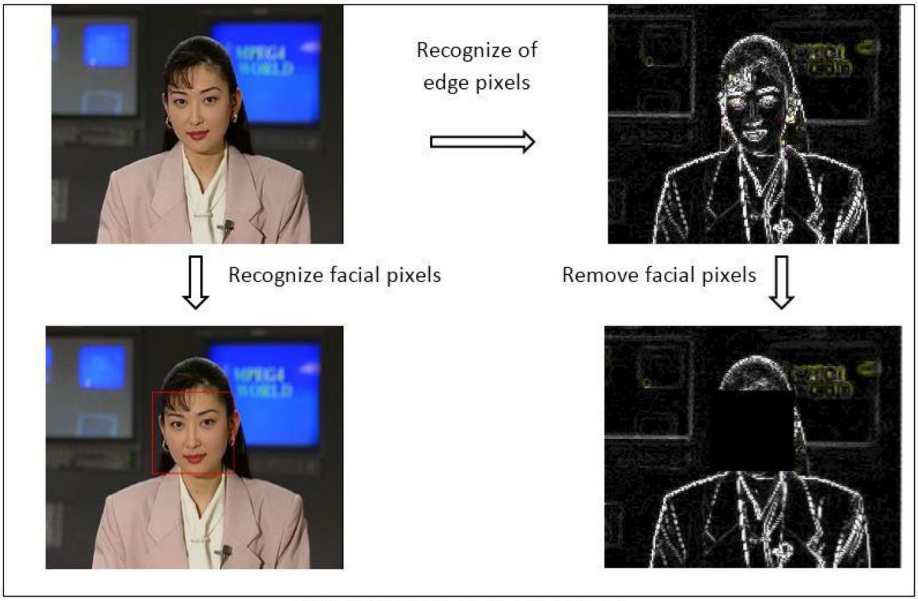
4.6 Second test: Watermarked video quality

In this step, the details of embedding the watermark are examined and finally the quality of the watermarked videos is evaluated using the mentioned criteria (PSNR criterion). In order to embed a watermark, first the host pixels in each frame are selected and finally, the watermarking operation is performed. In order to better represent these steps, we will express them in the form of expression and examine each step.

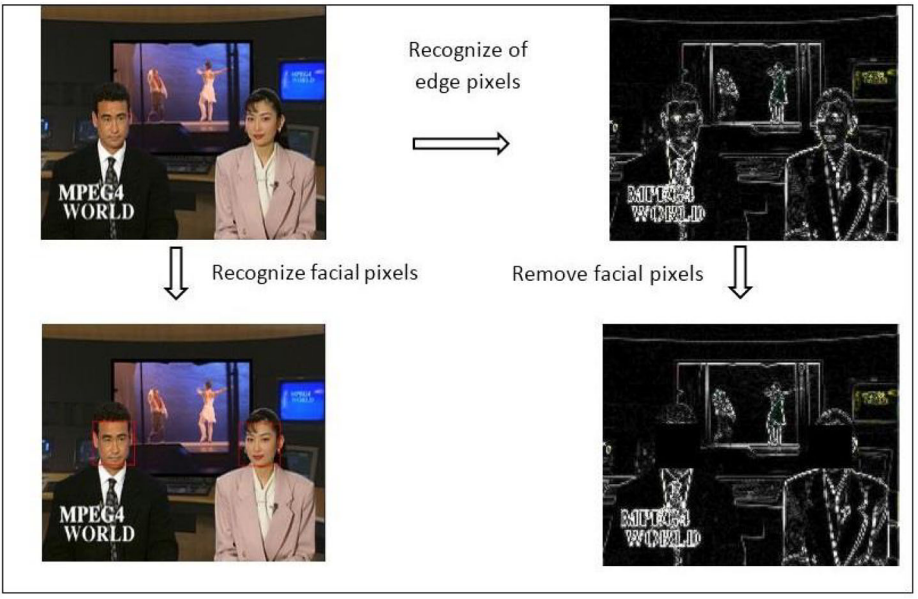
When embedding watermark in host data, first the share of each frame of the watermark is specified, then the host pixels in each frame are selected (the edge pixels with maximum intensity were used to select the host pixels). In this step, the edge pixels are selected first, and after removing the fixed and face pixels from the host set, the pixels with the maximum intensity per frame (the number of frames per share of the watermark) are selected as the host.In order to better represent the algorithm and the results of its execution, the selected pixels in each video are shown in Fig. (11).

As shown in the figure, in order to maintain the image quality of the frames, the host pixels have been intelligently selected by considering the human visual system (texture sensitivity, coverage phenomenon and sensitivity to the amount of light) to Increase the quality of the watermarked video as much as possible. Also, splitting the watermark between the frames and assigning a part of the watermark to each frame increases the capacity of the frame and this feature can also be considered as a positive feature in the quality of the watermarked video.

Finally, image quality measurement criteria (PSNR) were used to evaluate the quality of the coded video. The PSNR value for each video is calculated and the results are shown in Table (3). In addition, Fig. (12) compares the PSNR framed watermarks in the proposed method and the methods presented in the articles [19, 20, 28, 41], which are new or widely used methods.



a) Select host pixels in Akyio video

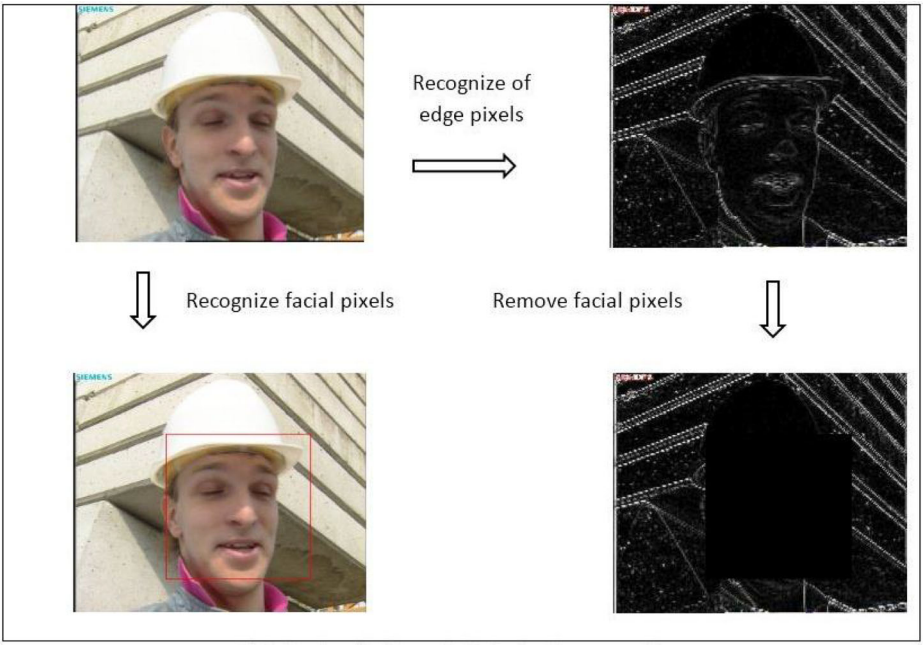


b) Select the host pixels in the News video

Fig. 11 Selecting host pixels in video (**a**) Akyio (**b**) News (**c**) Foreman

- ***Discussion***

What is clear from Table 3 is that all PSNR values calculated for watermarked videos are in the range of 30 to 50, as mentioned earlier; in this case the watermark will not be visible to the



c) Selecting the host pixels in the Foreman video

Fig. 11 (continued)

human eye. As a result, it is a suitable amount. In each of the videos reviewed, this value is different. It has the lowest value in the Foreman video and the highest value in the News video.

As can be seen from Fig. (12), although the values are not at their best and given the fact that the focus in this study is more on the security of the watermark, not the quality of the watermarked image, and there is always a compromise between image quality and watermark security, it can be concluded that the quality of watermarking in the proposed method is acceptable.

4.7 Third test: Attacks

The watermark embedded in the host may suffer from many intentional and unintentional attacks. These attacks include noise attacks, filter attacks, and rotation attacks. In addition,

Table 3 PSNR watermarked frame

PSNR	Foreman	News	Akyio
SCDW_CD	40.6	42.1	41.4
Himeur et al. [19]	57.206	57.564	57.165
Li et al. [28]	46.59	47.12	46.86
Xiang-yang et al. [41]	48.32	48.78	48.11
Hua et al. [20]	49.15	49.95	49.82

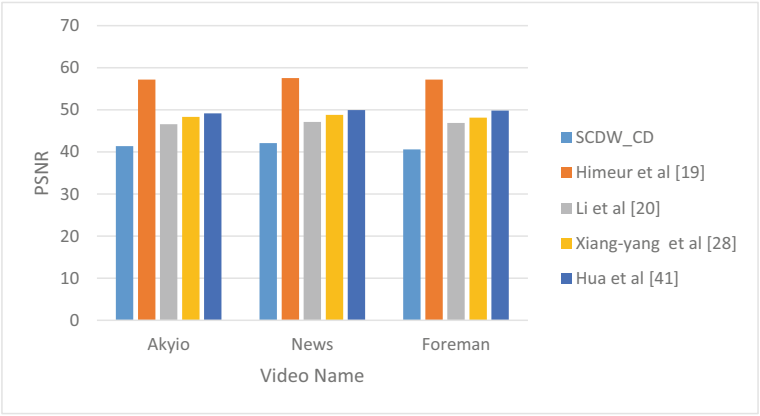


Fig. 12 Comparison of PSNR watermarked frames in the proposed SVDW_CD method and the methods presented in the articles [19, 20, 28, 41]

there are special attacks on video watermarks, such as frame averaging, frame swapping and so on. The performance of resisting different attacks of the watermark scheme **is** given below.

4.7.1 Image processing attacks and rotation attacks

Image processing attacks include noise attacks and filter attacks. The host may be affected more or less by noise during the transmission process. Table 4 describes the performance of the method after the host is attacked by different types of noise, filtering and rotation.

- ***Discussion***

As can be seen from the table, when only one of the three components (R, G, B) in the watermarked video frames was exposed to various attacks, the average NC value of the extracted watermark is above 0.6827. This shows that when a certain component of watermarked video frames suffers different attacks, the algorithm has good robustness and can meet the requirements of secure and high-quality transmission of watermark pictures.

Through the data in the Table 4, as we can see, watermarked frames can maintain good invisibility under various attacks. This shows that this watermarking algorithm is very effective for maintaining the imperceptibility of the watermark, which is very important for the confidential transmission of the watermark information.

4.7.2 Video attacks

For video watermarking, there are special attacks, including frame dropping, frame swapping and frame averaging. Due to the presence of a large amount of data redundancy between video frames, the difference between two adjacent frames is very small. Therefore, the receiver may not be able to perceive it when the watermarked video suffers these attacks. The performance under these attacks is particularly important for a video watermarking technique.

Table 4 Extracted watermark and NC value under various attacks

Row	Attack	Extracted watermark			Watermark frames
		Akyio	News	Foreman	
1	Gaussian noise(0.01)	NC=0.720	NC=0.680	NC=0.647	PSNR=20.300 SSIM=0.397
2	Gaussian noise(0.05)	NC=0.710	NC=0.704	NC=0.689	PSNR=19.445 SSIM=0.401
3	Gaussian noise (0.1)	NC=0.707	NC=0.710	NC=0.720	PSNR=17.479 SSIM=0.390
4	Salt & pepper noise (0.01)	NC=0.717	NC=0.650	NC=0.687	PSNR=26.053 SSIM=0.801
5	Salt & pepper noise (0.05)	NC=0.711	NC=0.649	NC=0.690	PSNR=19.076 SSIM=0.390
6	Salt & pepper noise (0.1)	NC=0.700	NC=0.723	NC=0.702	PSNR=14.132 SSIM=0.207
7	Poisson noise	NC=0.728	NC=0.719	NC=0.710	PSNR=30.484 SSIM=0.886
8	Median filter (2*2)	NC=0.783	NC=0.735	NC=0.637	PSNR=26.083 SSIM=0.835
9	Median filter (3*3)	NC=0.839	NC=0.820	NC=0.801	PSNR=31.977 SSIM=0.990
10	Histogram equalization	NC=0.694	NC=0.739	NC=0.735	PSNR=9.5674 SSIM=0.613
11	Rotation (5 degree)	NC=0.787	NC=0.804	NC=0.788	PSNR=57.810 SSIM=0.996
12	Rotation (20 degree)	NC=0.692	NC=0.689	NC=0.645	PSNR=60.261 SSIM=0.999
13	Rotation (45 degree)	NC=0.680	NC=0.653	NC=0.698	PSNR=58.898 SSIM=0.996
14	Rotation (75 degree)	NC=0.689	NC=0.730	NC=0.721	PSNR=57.095 SSIM=0.995
15	Rotation (90 degree)	NC=0.701	NC=0.702	NC=0.675	PSNR=58.167 SSIM=0.997
16	Rotation (135 degree)	NC=0.679	NC=0.698	NC=0.703	PSNR=59.303 SSIM=0.997
17	Rotation (180 degree)	NC=0.689	NC=0.843	NC=0.793	PSNR=57.038 SSIM=0.999

Frame swapping Frame swapping is to exchange two frames in a similar scene of the video. In this paper, the watermark was embedded in the specific video frames, so a small range of frame swapping attacks will not affect the extraction of watermark. In

Table 5 Performance under different video attacks

Attack	Extracted watermarked			Watermarked frames
	Akyio	News	Foreman	
Frame dropping	NC=1.000	NC=1.000	NC=0.989	PSNR=57.05 dB SSIM=0.999
Frame swapping	NC=1.000	NC=0.987	NC=1.000	PSNR=57.03 dB SSIM=0.999
Frame averaging	NC=0.618	NC=0.935	NC=0.873	PSNR=44.62 dB SSIM=0.999

order to verify this hypothesis, we also conducted a simulation experiment. In the experiment, we took a random swapping of two adjacent frames in different video scenes. The results showed that a small-scale frame exchange did not affect the extraction of watermark without any other attacks. And if there is a large range of frame swapping. It is bound to cause the receiver's attention. Consequently, if this happens, the approach of frame-by-frame extraction can be taken.

Frame dropping Frame dropping is also a video attack that attackers may adopt. Unlike frame swapping attacks, there are three possible scenarios for frame dropping. In the first case, if the frame without watermark is lost, there will be no impact on the receiver's extraction. The watermark can be properly extracted. And the rest can be non-motion frames dropping or watermarked non-motion frames dropping. In both cases, the receiver can only use the same method of handling frame swapping to extract watermark. In general, when the receiver receives the video and fails to extract the watermark according to the algorithm, it is necessary to consider whether the watermark has been attacked by these two attacks.

Frame averaging The frame averaging attack is to replace one frame with the average pixels of two frames adjacent to it. In the simulation experiment, we directly attack the watermarked frames using frame averaging.

Table 5 demonstrates the performance of the proposed watermarking technique under different video attacks.

- ***Discussion***

As can be seen from Table 5, after the frame dropping and frame swapping attack, the extracted watermark can be extracted without loss since the NC is 1.000. The host can maintain its high quality. The high values of PSNR and SSIM indicate that the host can maintain its high quality. In other words, the watermark is invisible after these two attacks. Frame averaging attack does have some effects on the host and the extracted watermark, but we could still use the watermark. And the PSNR of watermarked frames means that attackers could not get the information of watermark. Therefore, we can conclude that the proposed algorithm is efficient and the watermarking security is still maintained under these attacks.

4.8 Fourth test: The quality of the extracted watermarked

The main purpose of the research was to provide a security model against attacks, especially collusion attacks, so that the product can be provided to consumers with more confidence, and in case of any problems, the watermark can be extracted and the culprit identified. To evaluate

Fig. 13 Image of averaging three consecutive frames in Akyio video

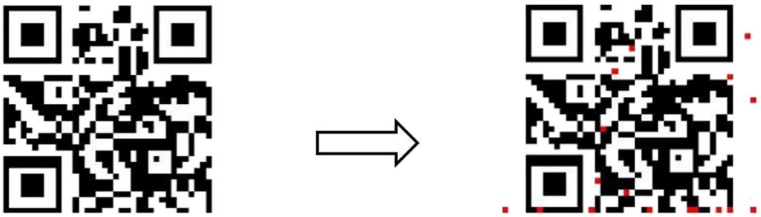


Fig. 14. Watermark extracted after averaging attack.

the quality of the watermark, the results are compared with three algorithms [10, 19, 25, 26], which are the most widely used and newest methods in this field.

Statistical averaging attacks are one of the most notable attacks in video watermarking. It is clear that averaging multiple frames eliminates the watermark dynamic pixels in the host data. In this experiment we use the previous two frames and the next selected frame to replace the current frame shown in formula (13).

$$f_k(i,j) = \frac{1}{3}\left[f_{k-1}(i,j) + f_k(i,j) + f_{k+1}(i,j)\right] \tag{13}$$

Where k is between 2 and n-1 (n is the number of frames extracted from the video).

Figure (13) shows the image obtained by averaging three consecutive frames in Akyio video.

- ***Discussion***

In this experiment, due to the presence of watermark in different blocks, the damaged parts can be repaired while extracting the watermark from all the blocks, and also due to the use of error correction technology, Reed- Solomon, in the QR code, it can be concluded that the extracted watermark error is up to 30% correctable and we will not have any problems during decoding. The results of watermark extraction after this attack are shown in Fig. (14).

Table 6 Results of watermark extraction after averaging attack

Video name	Number of frames	NC%	BE%	Error number of pixels
Akyio	2	99.37	99.63	6
	3	98.2	98.93	17
	5	95.6	97.40	42
	10	91.04	94.6	86
News	2	96.96	98.18	29
	3	95.81	97.48	40
	5	94.03	96.41	57
	10	84.62	90.74	147
Foreman	2	98.43	99.06	15
	3	96.54	97.93	33
	5	93.82	96.29	59
	10	87.65	92.57	118

As it can be seen in Fig. 14, the different pixels in the extracted watermark are shown in red, 17 pixels out of 1586 pixels in this attack are incorrect. In other words, there is a 1.07% error in the extracted watermark.

The attack was implemented on Akyio, News, and Foreman videos, and in each run, a different number of frames were selected. The results are shown in Table (6).

The diagrams in Fig. 15 include the results obtained from the proposed algorithm compared to the results of the previous research. What is clear is the better performance of the proposed algorithm.

In the algorithms [19, 25], with increasing the number of frames in the averaging stage, the quality of the extracted watermark decreases significantly, but in the proposed algorithm, although increasing the number of averaging frames in the next steps has somewhat reduced the quality of the watermark, we still see an acceptable performance in this algorithm. Among these algorithms, the algorithm presented in [25] has a higher quality drop than the proposed algorithm and algorithm [19].

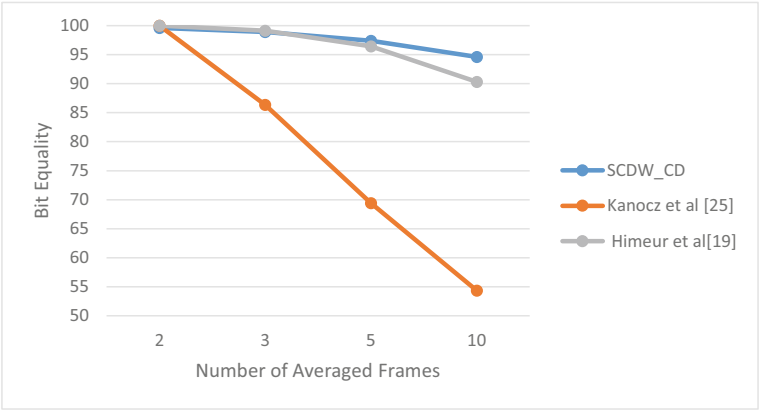
As can be seen in Fig. (15), the percentage of the extracted watermark accuracy is better than the previous method, and with increasing the number of frames in the averaging stage, we face a better relative decrease.

In [19, 25] methods, the whole watermark is embedded in the first frame and by averaging the frames in each step, the probability of losing the hidden value in the host pixel increases. However, in the proposed method, the watermark is divided into the number of block frames and a limited number of watermark pixels are embedded in each frame. Although the number of pixels at risk of disappearing increases with the increase of frames in the averaging phase, it is still not an attack on the entire cached pixels. In fact, in the proposed method, the attack is performed only on a percentage of the watermark pixels.

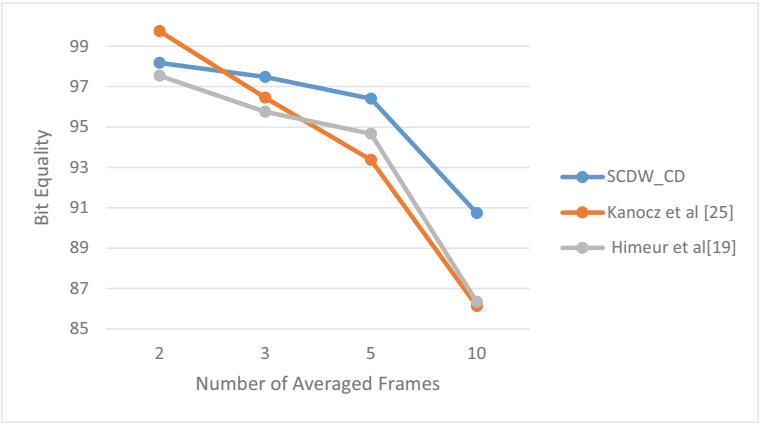
In addition, by considering the selection of moving edge pixels as host pixels in the averaging phase, the probability of losing the hidden value is greatly reduced. In the averaging phase, fixed pixels find a value equal to their true value, and the higher the number of frames in this phase, the more likely it is that the hidden value will be lost and the host pixel value will change to its original value. Due to this difference in the watermarking steps, in the diagrams of Fig. 15, a decrease in quality and a lower slope drop than the other two algorithms can be seen.

In Fig. 16, we examine the quality of the watermark using the NC criterion of the watermark extracted in the proposed SCDW_CD method and the previous methods.

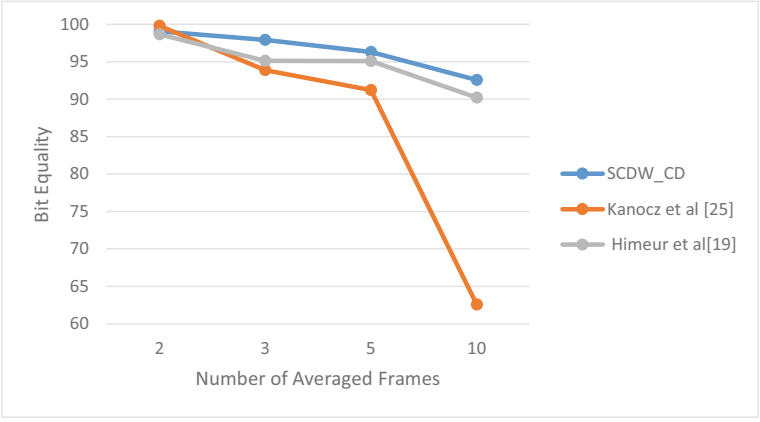
As can be seen from the values obtained in the NC criterion, here Fig. (16) shows the better performance of the proposed algorithm in resisting the averaging attacks of the frames. With the increase in the number of frames in the averaging stage, the quality of the extracted watermark has also decreased. But this reduction did not eliminate the ability to detect the watermark, and in the worst case, the error rate was still less than 30. According to the selected type of watermark (QR code) and the ability to correct the error of this code up to 30%, it can be concluded that even in the worst case, the extracted watermark is recognizable. Moreover, changes in the proposed graph have occurred with a low slope, and the slope of the graph in the proposed algorithm is less than other algorithms, and this indicates the quality of the proposed algorithm. Another advantage of the proposed SCDW_CD algorithm is the increase in the capacity of each frame. Whereas, in other algorithms such as algorithm [10, 19, 26], as the number of frames increases, the quality of the watermark decreases drastically. When the number of frames is fewer, such as 5 or fewer, the distance between the algorithms is less and they have a relatively equal slope, but when we increase this value to 6, 7 and finally 10



(a) Akyio video



(b) News video



(c) Foreman Video

Fig. 15 Comparison of the percentage of the extracted watermark accuracy after the attack of averaging the frames in the proposed method and the methods presented in the articles [19, 25]

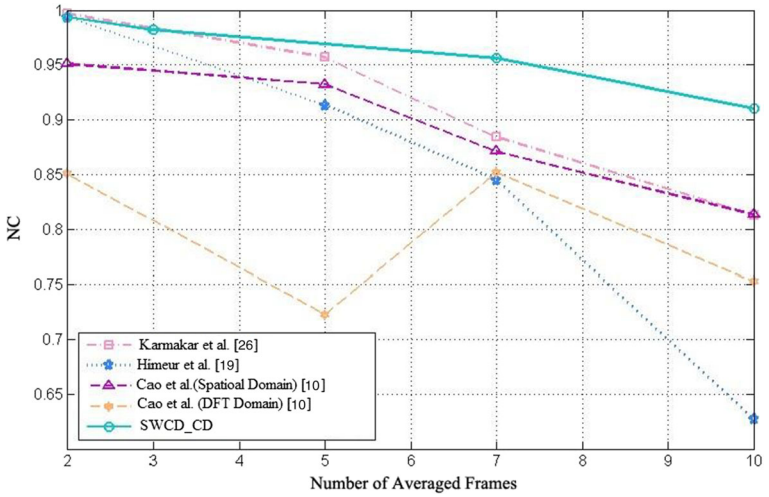


Fig. 16 Comparison of NC watermark extracted in the proposed SCDW_CD method and previous methods

frames, the quality decreases sharply, so that the slope of the graphs decreases sharply. Among these, the pattern [19] is strongly influenced by mediation attacks.

5 Conclusion

Applying cryptographic techniques is one way to protect digital data. To have a good and successful watermarking project, the three main needs of capacity, intangibility and stability must be considered. Given the impossibility of achieving all of these features completely, the main priority of the proposed model is to provide acceptable safety and stability. However, in order to achieve the goal set, three other features, namely less complexity, relative non-observability of the watermark and more capacity, have been considered.

With regard to selecting the field of work to present the desired algorithm, as a result of much research and in order to take full advantage of both existing fields of work, the proposed method in the field of conversion was presented. Among the algorithms of conversion domain due to the optimal compression of discrete cosine conversion methods which are very close to KL (optimal compression) compression and considering the property that three-dimensional conversion is an achievement an alternative to motion compensation (a technique used today for video coding standards), discrete three-dimensional cosine conversion has been used.

The calculation of the minimum and maximum block length in the proposed SCDW_CD method is such that the watermark security is maintained and will be more resistant to attacks. Furthermore, the proposed blocking algorithm does not depend on the type of input video and changes the number of blocks extracted by changing the alpha value. In this algorithm, not only dynamic videos are still blocked with the quality of the past, but also the scope of video coverage is increased and static videos are included in the scope. The block end detector in the proposed algorithm performs the detection operation based on comparing the pixels of each block with the pixel values of the first frame in the block. The advantage of this method is that

it ignores small changes but recognizes this path as a block by moving the main object in the video away from its original state.

In a part of the research, we have categorized and evaluated the types of existing attacks in order to learn the basic principles used in the proposed method and provide a solution for the most important categories by thoroughly analyzing the existing attacks. According to the evaluations, it can be claimed that the proposed solution is resistant to collusion attacks, which is the most important attack in the field of digital watermarking. Other strengths of the proposed algorithm include a higher capacity for watermarking.

In the continuation of this research, it is possible to take action to make the watermark more resilient. Besides, one of the most important measures for future development is to consider more attacks.

Availability of data and material Not applicable.

Code availability Not applicable

Declarations

Conflicts of interest/competing interests Not applicable.

References

1. Abdelwahab KM, Abd El-atty SM, El-Shafai W et al (2020) Efficient SVD-based audio watermarking technique in FRT domain. Multimed Tools Appl 79:5617–5648
2. Agarwal N, Singh AK, Singh PK (2019) Survey of robust and imperceptible watermarking. Multimed Tools Appl 78:8603–8633. https://doi.org/10.1007/s11042-018-7128-5
3. Ahmadi SBB, Zhang G, Wei S (2020) Robust and hybrid SVD-based image watermarking schemes. Multimed Tools Appl 79:1075–1117. https://doi.org/10.1007/s11042-019-08197-6
4. Al-Maweri NaAS, Sabri AQM, Mansoor AM et al (2017) Metadata hiding for UAV video based on digital watermarking in DWT transform. Multimed Tools Appl 76:16239–16261. https://doi.org/10.1007/s11042-016-3906-0
5. Bahrami Z, Akhlaghian Tab F (2018) A new robust video watermarking algorithm based on SURF features and block classification. Multimed Tools Appl 77:327–345. https://doi.org/10.1007/s11042-016-4226-0
6. Bahrami Z, Akhlaghian Tab F (2018) A new robust video watermarking algorithm based on SURF features and block classification. Multimed Tools Appl 77:327–345. https://doi.org/10.1007/s11042-016-4226-0
7. Bayoudh I, Ben Jabra S, Zagrouba E (2018) Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications. Multimed Tools Appl 77:14361–14379. https://doi.org/10.1007/s11042-017-5033-y
8. 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 77:19659–19678. https://doi.org/10.1007/s11042-017-5340-3
9. Cao Z, Wang L (2019) A secure video watermarking technique based on hyperchaotic Lorentz system. Multimed Tools Appl 78:26089–26109. https://doi.org/10.1007/s11042-019-07809-5
10. Cao Z, Wang L (2019) A secure video watermarking technique based on hyperchaotic Lorentz system. Multimed Tools Appl 78:26089–26109. https://doi.org/10.1007/s11042-019-07809-5
11. Chopra A, Gupta S, Dhall S (2020) Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks. Multimed Tools Appl 79:501–554. https://doi.org/10.1007/s11042-019-08087-x
12. Das S, Banerjee M, Chaudhuri A (2018) An improved video key-frame extraction algorithm leads to video watermarking. Int j inf tecnol 10:21–34. https://doi.org/10.1007/s41870-017-0054-3
13. Dhaou D, Jabra BS, Zagrouba EA (2019) Review on Anaglyph 3D Image and Video Watermarking. 3D Res **10**:13. https://doi.org/10.1007/s13319-019-0223-1

14. Dhaou D, Ben Jabra S, Zagrouba E (2019) A review on anaglyph 3D image and video watermarking. 3D. Res 10:13. https://doi.org/10.1007/s13319-019-0223-1
15. Favorskaya MN (2020) Watermarking models of video sequences. In: Favorskaya M, Jain L (eds) Computer vision in control systems—6. Intelligent systems reference library, vol 182. Springer, Cham
16. Gupta G, Gupta VK, Chandra M (2018) An efficient video watermarking based security model. Microsyst Technol 24:2539–2548. https://doi.org/10.1007/s00542-017-3689-x
17. He J, Ying Q, Qian Z, Feng G, Zhang X (2020) Semi-structured data protection scheme based on robust watermarking. J Image Video Proc 2020:12. https://doi.org/10.1186/s13640-020-00500-y
18. Himeur Y, Boukabou A (2018) A robust and secure key-frames based video watermarking system using chaotic encryption. Multimed Tools Appl 77:8603–8627. https://doi.org/10.1007/s11042-017-4754-2
19. Himeur Y, Boukabou A (2018) A robust and secure key-frames based video watermarking system using chaotic encryption. Multimed Tools Appl 77:8603–8627
20. Hua Z, Zhou Y (2016) Image encryption using 2D logistic-adjustedSine map. Inf Sci 339:237–253
21. Jafari Barani M, Ayubi P, Yousefi Valandar M, Yosefnezhad Irani B (2020) A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform. Multimed Tools Appl 79:2127–2159. https://doi.org/10.1007/s11042-019-08225-5
22. Jain R, Trivedi MC, Tiwari S (2018) digital audio watermarking: a survey. In: Bhatia S, Mishra K, Tiwari S, Singh V (eds) advances in computer and computational sciences. Advances in intelligent systems and computing, vol 554. Springer, Singapore. https://doi.org/10.1007/978-981-10-3773-3_42
23. Jakhmola R, Rani R (2019) Enhanced digital video watermarking technique using 2-level DWT. In: Pati B, Panigrahi C, Misra S, Pujari A, Bakshi S (eds) Progress in advanced computing and intelligent engineering. Advances in intelligent systems and computing, vol 713. Springer, Singapore
24. Kadu S, Cheggoju N, Satpute VR (2018) Noise-resilient compressed domain video watermarking system for in-car camera security. Multimedia Systems 24:583–595. https://doi.org/10.1007/s00530-017-0584-3
25. Kanocz T, Tokar T, Levicky D. (2009) Robust frame by frame video watermarking resistant against collusion attacks, IEEE, in Radioelektronika, RADIOELEKTRONIKA'09. 19th international conference, 99-102
26. Karmakar A, Phadikar A, Phadikar BS (2016) A blind video watermarking scheme resistant to rotation and collusion attacks. J King Saud Univ-Comput Inform Sci 28(2):199–210
27. Kumar S, Singh BK, Yadav M (2020) A recent survey on multimedia and database watermarking. Multimed Tools Appl 79:20149–20197. https://doi.org/10.1007/s11042-020-08881-y
28. Li Z, Chen XW, Ma J (2015) Adaptively imperceptible video watermarking based on the local motion entropy. Multimed Tools Appl 74(8):2781–2802
29. Luo AW, Gong LH, Zhou NR, Zou WP (2020) Adaptive and blind watermarking scheme based on optimal SVD blocks selection. Multimed Tools Appl 79:243–261. https://doi.org/10.1007/s11042-019-08074-2
30. Maloo S, Lakshmi N, Pareek NK (2018) Study of Digital Watermarking Techniques for Against Security Attacks. In: Satapathy S, Joshi A (eds) Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1. ICTIS 2017. Smart innovation, systems and technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-319-63673-3_61
31. Mohammed AA, Ali NA (2018) Robust video watermarking scheme using high efficiency video coding attack. Multimed Tools Appl 77:2791–2806. https://doi.org/10.1007/s11042-017-4427-1
32. Mohammed AA, Ali NA (2018) Robust video watermarking scheme using high efficiency video coding attack. Multimed Tools Appl 77:2791–2806. https://doi.org/10.1007/s11042-017-4427-1
33. Shoitan R, Moussa MM, Elshoura SM (2020) A robust video watermarking scheme based on Laplacian pyramid, SVD, and DWT with improved robustness towards geometric attacks via SURF. Multimed Tools Appl 79:26837–26860. https://doi.org/10.1007/s11042-020-09258-x
34. Singh KM (2018) A robust rotation resilient video watermarking scheme based on the SIFT. Multimed Tools Appl 77:16419–16444. https://doi.org/10.1007/s11042-017-5213-9
35. Singh KM (2018) Correction to: a robust rotation resilient video watermarking scheme based on the SIFT. Multimed Tools Appl 77:16445. https://doi.org/10.1007/s11042-017-5345-y
36. Singh TR, Singh KM, Roy S (2013) Video watermarking scheme based on visual cryptography and scene change detection. AEU-Int J Electron Commun 67(8):645–651
37. Singh OP, Singh AK, Srivastava G, Kumar N (2020) Image watermarking using soft computing techniques: a comprehensive survey. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-09606-x
38. Tian C, Wen RH, Zou WP, Gong LH (2020) Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain. Multimed Tools Appl 79:7515–7541. https://doi.org/10.1007/s11042-019-08530-z
39. Tian L, Dai H, Li C (2020) A semi-fragile video watermarking algorithm based on chromatic residual DCT. Multimed Tools Appl 79:1759–1779. https://doi.org/10.1007/s11042-019-08256-y

40. Wu JY, Huang WL, Xia-Hou WM, Zou WP, Gong LH (2020) Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition. Multimed Tools Appl 79: 22727–22747. https://doi.org/10.1007/s11042-020-08987-3
41. Xiang-yang W, Yu-nan L, Shuo L, Hong-ying Y, Pan-pan N, Yan Z (2015) A new robust digital watermarking using local polar harmonic transform. Comput Electr Eng 46:403–418
42. Yang R, Au MH, Lai J, Xu Q, Yu Z (2019) Collusion Resistant Watermarking Schemes for Cryptographic Functionalities. In: Galbraith S, Moriai S (eds) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019. Lecture notes in computer science, vol 11921. Springer, Cham
43. Yoo G, Kim H (2017) Real-time video watermarking techniques robust against re-encoding. J Real-Time Image Proc 13:467–477. https://doi.org/10.1007/s11554-015-0557-8
44. Zhou NR, Hou WMX, Wen RH, Zou WP (2018) Imperceptible digital watermarking scheme in multiple transform domains. Multimed Tools Appl 77:30251–30267. https://doi.org/10.1007/s11042-018-6128-9
45. Zhou NR, Luo AW, Zou WP (2019) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimed Tools Appl 78:2507–2523. https://doi.org/10.1007/s11042-018-6322-9