Circuits, Systems, and Signal Processing (2021) 40:2464–2493
https://doi.org/10.1007/s00034-020-01585-6

Robust and Secure Video Watermarking Based on Cellular Automata and Singular Value Decomposition for Copyright Protection

C. Priya[1] · C. Ramya[2]

Received: 12 July 2019 / Revised: 21 October 2020 / Accepted: 23 October 2020 /
Published online: 3 November 2020

Abstract

In recent years, watermarking techniques have been under deliberation for their wide variety of applications in various fields. An organization transmits its data through digital communication channels, where the probability of attack is more. To protect the data transmitted through the channel, a novel fuzzy-based digital video watermarking scheme based on Cellular Automata Transform and Singular Value Decomposition (SVD) for copyright protection is proposed. The proposed scheme adopts a mixture of both cellular automata and SVD, which provides copyright protection with high robustness and imperceptibility for multiple transform planes with high processing speed and data redundancy. Moreover, the confidentiality of the proposed scheme is improved with the help of SVD. The watermarked video is experimented with to prove the strength by extracting the watermark image after applying geometric transformation, noise addition, enhancement, and compression attacks. The quantitative performance analysis, which shows improved robustness and imperceptibility of the proposed method compared to the existing methods, is performed by calculating the peak signal-to-noise ratio, structural similarity index, bit error rate, and normalized cross-correlation.

Keywords Cellular automata · Imperceptibility · Robustness · Singular value decomposition · Watermark

✉ C. Priya
priyakarthikayeni@gmail.com

C. Ramya
crm.ece@psgtech.ac.in

[1] Department of ECE, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

[2] Department of ECE, PSG College of Technology, Coimbatore, Tamil Nadu, India

1 Introduction

Data security is essential in today's world of Internet and networking technology. Although the technology provides secure transmission, hackers have devised numerous ways of stealing important data, which are later on misused. Hence, securing the information of an organization is crucial. One of the methods by which data can be secured is to make certain data invisible to the hacker by concealing the message behind other data through a technique called cryptography or steganography.

Watermarking is the process of embedding data, which are called the watermark or label, into a multimedia object such that watermark can be detected or extracted to make an assertion about the object. The watermark object may be an image, audio, or video [4]. Data-hiding schemes that embed secondary data in digital media have attracted the attention of various organizations. Also, various techniques have been proposed for a variety of applications, including ownership protection, authentication, and access control. The ability to hide data is the most basic technique of all and is quite a conflicting requirement in many data-hiding applications [2]. Moreover, the watermark might contain additional information that may include the identity of the owner of a particular copy of the object.

In a spatial domain-based watermarking scheme [5], the embedding process is done in luminance and color components, but owing to the lack of concern in a temporal axis, the multiple frame conspiracy and optimization are difficult. In the least significant bit modification scheme [23], the watermark image is embedded in the least significant bit, which is simple and straightforward with high capacity speed and limited robustness. Digital video watermarking based on DCT is proposed in [10], where the watermark image is embedded on a selected block of cover video, which is perpetually significant to the human visual system, but is not robust against all types of attack. DWT–PCA-based watermarking [6, 9, 17] provides copyright protection in both the time and frequency domains with a higher compression ratio, but the pitfall is the high computational cost and time.

A robust and synthesized watermarking scheme [1] adapts the depth image-based rendering (DIBR) technique where the modifications of the depth are restricted based on the prior restrictions. This method avoids distortion, but is complex and takes more time to compute. Robust DT-CWT-based DIBR-3D video watermarking using a chrominance embedding scheme was proposed to embed the watermark image in both the chrominance channels of a YUV representation of the center view, which provides better robustness with its approximate shift invariance and directional selectivity [11] properties. In the paper [15], the watermark video is compressed and transmitted by introducing techniques like the MPEG-2 coding structure, which removes the temporal redundancy by using forward and statistical methods and also reduces the overall time of processing.

The rest of this article is organized as follows: Sect. 2 presents the proposed watermark embedding and encryption process, along with the decryption and watermark extraction process. Section 3 highlights the superiority of the proposed algorithm with the experimental results and qualitative comparative analysis. Finally, Sect. 4 draws the conclusion of the paper.

2 Proposed Methodology

This paper proposes a watermark embedding algorithm for the secure transmission of images. The proposed scheme uses cellular automata transform in two successive stages to encrypt and to embed the watermark image; initially, the encryption technique is performed for the watermark image using one-dimensional cellular automation (1D CA) transform. In the second stage, the encrypted image is embedded into the input video using three-dimensional (3D) CA transform and singular value decomposition (SVD), and then the output of both the stages are combined to obtain a watermarked video. With the help of Internet technology, the watermarked video is sent over a digital communication channel, where malevolent changes may affect the transmitted watermarked video. Hence, the proposed work attempts to provide imperceptibility and robustness against the various attacks. The following are the steps involved in watermark encryption, embedding, and extraction algorithm.

2.1 Watermark Encryption and Embedding Process

The proposed watermark encryption, embedding, extraction, and decryption algorithm is used to authenticate not only whether any modifications are performed in the watermarked video but also whether any confidential transfer of the watermark image is made. The design flow diagram of the proposed watermark encryption and embedding process is shown in Fig. 1. The watermark image embedding algorithm is divided into seven steps; the first three steps present the watermark image encryption process and the remaining steps provide the encrypted watermark image embedding process.

Input: Cover video $I(n,j,t)$ and watermark image $W(x,y)$.

Output: Watermarked video $W_{\mathrm{I}}(n,j,t)$.

Step 1: The watermark image represented by $W(x,y)$ of size $M \times N$ is encrypted and embedded into the cover video $I(n,j,t)$.

Step 2: The watermark array $W(x,y)$ is first scanned into the 1D sequence using a circular shift of the diagonal pixel, which is presented in binary form as $W\{0,1\}$. To increase the robustness of the watermarking algorithm, the watermark sequence is obtained by merging the image array and then by passing the sequence through a scrambler to embed and disseminate data in space.

Step 3: In this step, the watermark sequence is scrambled by the 1D CA transform and the scrambled data are generated according to integral gateway values used to generate the CA bases function [12–14, 24]. The coefficients obtained from the CA transform are stored in the position of the watermark image. In a 1D CA, the state of each cell is given by means of the Boolean values (0, 1). The CA evolution of the nth cell is expressed in the form of

$$a_{n,t+1} = F(a_{n-1,t}, a_{n,t}, a_{n+1,t}) \tag{1}$$

where the variable $a_{n,\mathrm{t}}$ represents the state of the nth cell at time t, $a_{n-1,\mathrm{t}}$, $a_{n+1,\mathrm{t}}$ are the two neighboring states and F is a Boolean function defining

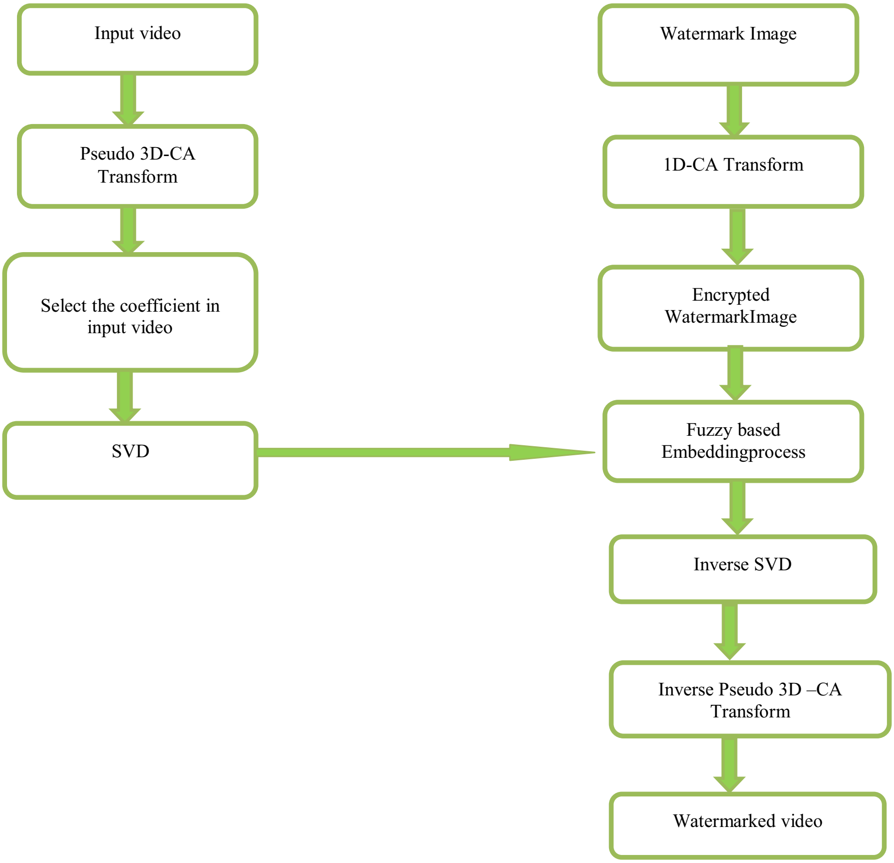

Fig. 1 Watermark encryption and embedding process

the CA rule. When n cells are evolved over N time steps, the transform base and bases function type 2 are given in Eqs. (2) and (3), respectively.

$$a = a_{n,t}, n, t = 0, 1, 2, \ldots N - 1 \tag{2}$$

$$A_{n,k} = 2a_{n,k}a_{k,n} - 1 \tag{3}$$

where $A_{n,k}$ is the CA bases function that can be expressed as a function of $a_{n,t}$, as shown in Eq. (2). The scrambled coefficients of the watermark sequence are obtained from the 1D CA transform with the help of Eqs. (4) and (5).

$$B_{n,k} = \frac{A_{n,k}}{\sum_{i=0}^{N-1} A_{n,k}^2} \tag{4}$$

$$w_k = \sum_{i=0}^{N-1} f_n B_{n,k} \tag{5}$$

where w_k denotes the coefficient of the watermark sequence,f_{n} represents the watermark sequence, and $B_{n,k}$ represents the inverse CA bases function obtained by Eq. (4). Here, Wolfram Rule 30 shows responsive dependence on the initial configuration; this diverges rapidly when there is a small change in the initial configuration. The gateway of the CA transform is as follows: Wolfram Rule: 30; cell number: 8; initial configuration: 00011110; boundary configuration: cyclic; and bases function type: 2. Hence, the encrypted watermark image $E(x,y)$ is obtained.

Step 4: The uncompressed cover video sequence is separated into a group of frames to embed the encrypted watermark image into it. Here, the encrypted watermark image is embedded using the 3D CA transform and SVD.

Step 5: The 3D CA transform bases function A_{njtklm} is derived from the two dimensional (2D) CA transform over a specified time. The 3D CA transform filters are the products of orthogonal 2D and 1D CA transform filters and are given as,

$$A_{njtklm} = A_{njkl} \times A^{'}_{tm} \tag{6}$$

where A' is the 1D bases function and A'' represents the 2D bases. To perform watermarking based on space and temporal, the video is viewed as a 3D signal with two dimensions in the space domain and one dimension in the time domain. In the 3D signal, the data of each pixel are represented by $I(n,j,t)$ at point (n,j) and the time instant t is used to calculate the coefficients of the transform A_{njtklm}.

$$B_{njtklm} = \frac{A_{njtklm}}{\sum_{n=0}^{N-1} \sum_{j=0}^{N-1} \sum_{t=0}^{N-1} A^2_{njtklm}} \tag{7}$$

$$C_{klm} = \sum_{k=0}^{N_k-1} \sum_{l=0}^{N_l-1} \sum_{m=0}^{N_m-1} I(n, j, t) B_{njtklm} \tag{8}$$

where A_{njtklm} represents the 3D CA bases function, N represents the filter size according to their directions, and $\mathrm{c}_{\mathrm{klm}}$ represents the transform coefficient values that are obtained from Eq. (8). The basic function of the CA transform is generated using a set of gateway values as follows: Wolfram Rule: 142; cell number: 8; initial configuration: 01,101,010; boundary configuration: cyclic; and bases function type: 2.

Step 6: The coefficients obtained from the 3D CA transform are divided into four blocks of low, two middle and high-frequency components. To make lower visibility for $E(x,y)$, is added to the higher frequency coefficients.

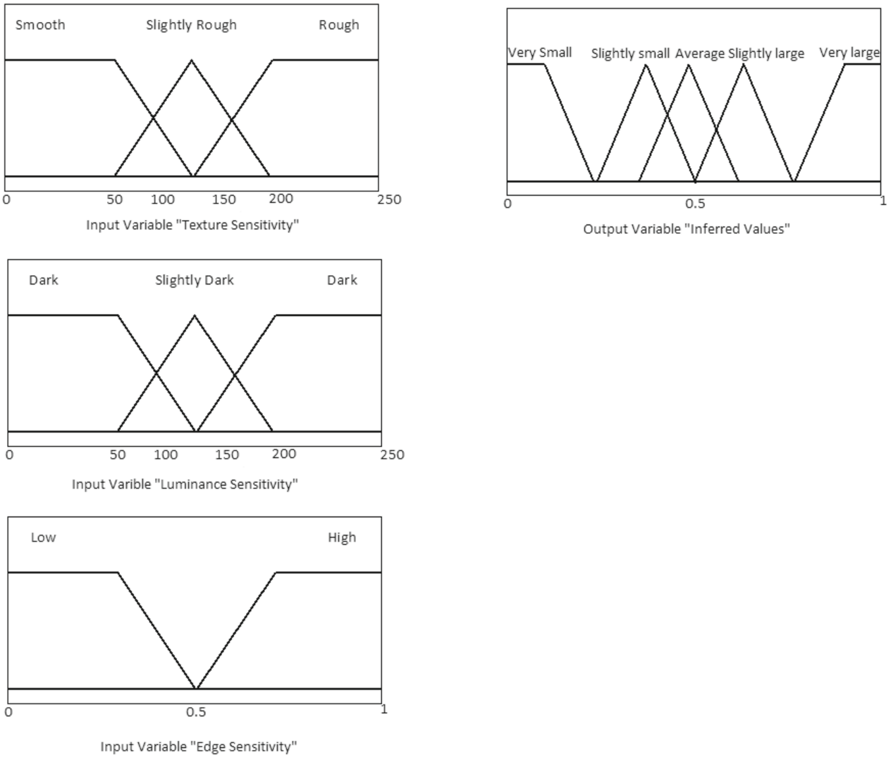

Fig. 2 Input and output membership functions for the fuzzy inference system

Step 7: Then, SVD is applied to the coefficients of the cover video obtained from 3D-CA, where F_c defines the SVD block processing as follows:

$$F_c = \sum_{c=1}^{r} U_c S_c V_c^T \tag{9}$$

where U_c and ${V_c}^T$ represent the eigenvectors of CA coefficients and $\mathrm{S_c}$ denotes the eigenvalues of the coefficients. Embedding parameter α is inferred from the fuzzy inference system (FIS) that enhances the imperceptibility of the watermarked video. In the FIS, the robust embedding of $E(x,y)$ is achieved based on the texture, luminance, and edge sensitivity of cover video frames to make the $W(x,y)$ imperceptible. Input and output membership functions are shown in Fig. 2.

In the embedding process, the coefficientw_k obtained from the 1D CA transform of the encrypted watermark image $E(x,y)$ is embedded into the coefficient $\mathrm{c_{klm}}$ obtained from the 3D CA for the cover video with the help of SVD and the FIS at high frequency. The coefficient of the cover video is updated using Eq. (10):

$$S_w(n, j) = S_c(n, j) \times (w_k + \alpha) \tag{10}$$

where $S_w(n,j)$ denotes the eigenvalue of watermarked video frames, $S_c(n,j)$ represents the eigenvalues of cover video frames, and w_k denotes the coefficient of the watermark image. F_w as the inverse SVD with the eigenvalue of the watermarked video sequences is obtained with Eq. (11), for those coefficients apply inverse 3D CA transform using Eq. (12):

$$F_w = CW_{klm} \tag{11}$$

$$W_I(n, j, t) = \sum_{k=0}^{N_k-1} \sum_{l=0}^{N_l-1} \sum_{m=0}^{N_m-1} CW_{klm} A_{njtklm} \tag{12}$$

where $W_I(n,j,t)$ represents the watermarked video and cw_{klm} represents the watermarked coefficients. Finally, the watermarked video sequences $W_I(n,j,t)$ are produced by the inverse 3D CA transform.

2.2 Watermark Extraction and Decryption Process

The watermark extracting process is the converse of the watermark embedding process. The watermark image can be extracted from the distorted or attacked watermarked video without using the watermark image. The watermark extracting and decryption process of the proposed method is shown in Fig. 3.

Step 1: The watermarked video sequence received is first separated into a group of frames to extract the encrypted watermark image from the frames. Here, the encrypted watermark image is extracted with the 3D CA transform and SVD.

Step 2: To extract $E(x,y)$, the 3D CA transform is applied to the watermarked video sequences. Hence, the coefficients of the watermarked video sequence are obtained with the CA gateway values for Wolfram Rule: 142 by using Eqs. (7) and (8).

Step 3: Then, SVD is applied to the coefficients taken from the 3D CA transform as F_{wi}, which defines the SVD block processing as follows:

$$F_{wi} = \sum_{wi=1}^{r} U_{wi} S_{wi} V_{wi}^T \tag{13}$$

where U_{wi} and $V_{{wi}^T}$ denote the eigenvectors of watermarked coefficients from the watermarked video sequences and S_{wi} represents the eigenvalue of the watermarked coefficient.

Step 4: In the extraction process, the coefficients of $W(x,y)$ are extracted from the eigenvalue of the watermarked coefficient with the help of the embedding parameter taken from the FIS using Eq. (14):

$$w_e(n, j) = (S_{wi}(n, j) - \alpha)/S_c(n, j) \tag{14}$$

where $w_e(n,j)$ denotes the coefficient of the extracted watermarked image. Hence, the encrypted watermark image is extracted from the watermarked

Fig. 3 Watermark extraction and decryption process

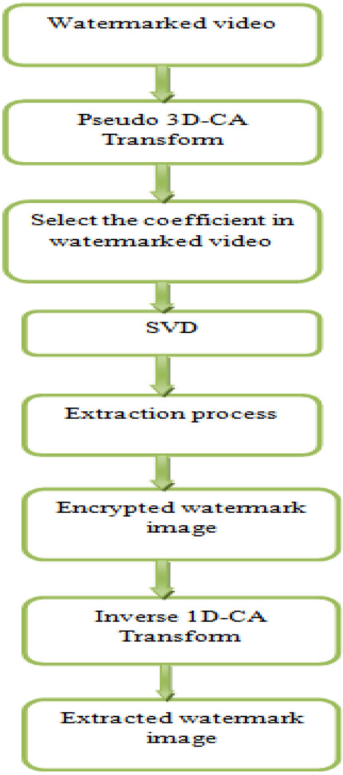
Watermarked video
Pseudo 3D-CA Transform
Select the coefficient in watermarked video
SVD
Extraction process
Encrypted watermark image
Inverse 1D-CA Transform
Extracted watermark image

image. Then, the encrypted watermark image is inversely scrambled by applying the 1D CA transform using Eqs. (3) and (15):

$$D(x,y)=\sum_{k=0}^{N_k-1} w_e A_{n,k} \tag{15}$$

where $D(x,y)$ represents the extracted watermark image. Finally, the watermark image is extracted from the watermarked video sequence.

3 Results and Discussion

To validate the authenticity of the watermark image for the proposed watermark embedding and extraction algorithm, the experiment has been carried out on a variety of videos and images (nearly 35 videos and 150 images were used), including different benchmark datasets [7, 8, 21, 22]. For this, selected grayscale images of size 256 × 256, including real-time images, medical images, synthetic chessboard images, and other images, are collected from the Internet and used as watermark images to demonstrate the performance of the proposed method. Besides the other videos, the

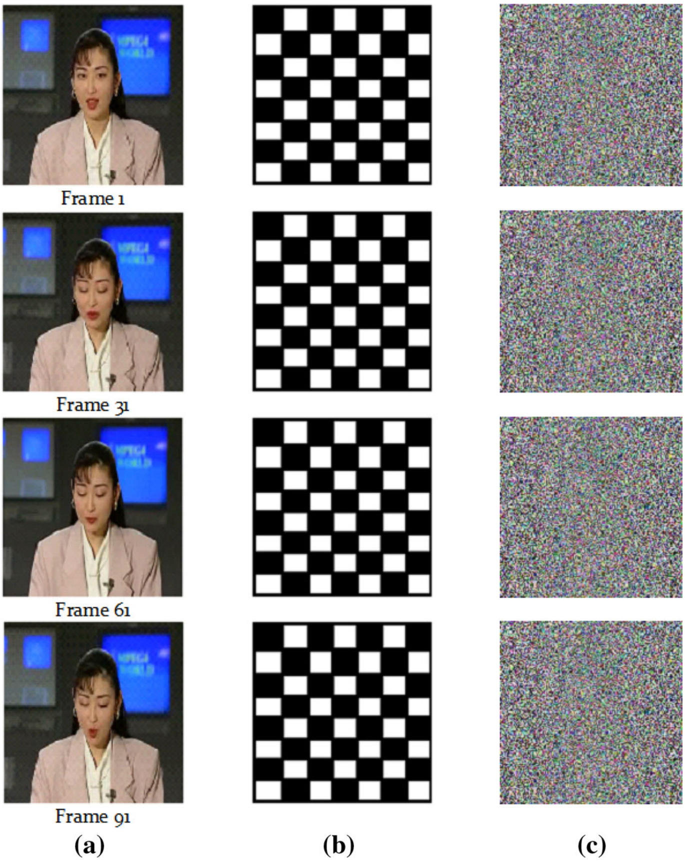

Fig. 4 Watermark embedding process: **a** cover video frames; **b** watermark image; **c** encrypted watermark image

selected videos of Akiyo and medical videos in AVI format, of size 360 × 240 and frame rate 30 fps, are used as cover videos to show the characteristics of the proposed method in this section. The output of the encrypted watermark for every first frame per second of the Akiyo cover video of frames 1, 31, 61, and 91 for the synthetic chessboard watermark image is shown in Fig. 4.

The selected synthetic chessboard watermark image of size 256 × 256 is considered to demonstrate the performance of the proposed method as shown in Fig. 4b. The watermark image is encrypted using the 1D CA transform with CA gateway values using 8-bit 1D CA, initial configuration: 00011110, and Wolfram Rule 30, as shown in Fig. 4c. The embedding coefficients are selected using the 3D CA transform with CA gateway values for transform using 8-bit 1D CA, initial configuration: 01101010, and Wolfram Rule 142.

Then, the encrypted watermark image is embedded in the cover video using SVD and the FIS, with the embedding parameter $\alpha = 0.65$, as shown in Fig. 5a. Figure 5b represents the extracted scrambled image from the watermarked video. After apply-

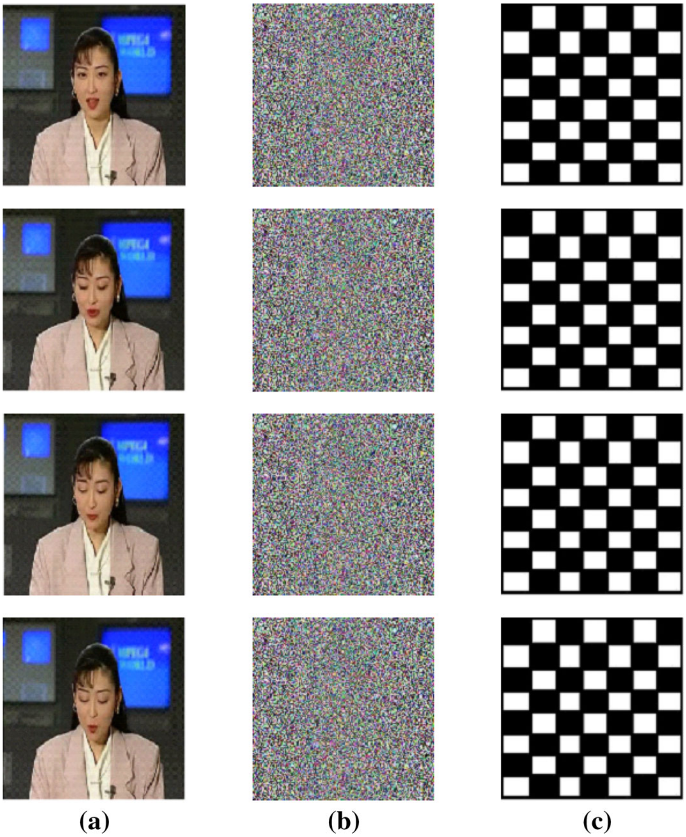

Fig. 5 Watermark extracting process: **a** watermarked video frames; **b** extracted encrypted watermark image; **c** decrypted watermark image

ing the inverse 1D CA transform, the decrypted scrambled data are shown in Fig. 5c. The embedding and extraction outputs of the proposed method for the same cover video with different watermark images are shown in Figs. 6 and 8 and Figs. 7 and 9, respectively. The experimental results show that the proposed work: (a) provides the encrypted watermarked image that cannot be visually identified, (b) eliminates the statistical correlation between the watermarked image and the encrypted watermarked image, (c) provides no change in image during encryption and after the decryption process, and (d) is robust to a wide range of attacks, such as median filtering, brightness and contrast variation, resizing attack, Gaussian noise, speckle noise, salt and pepper noise, JPEG compression, rotation, cropping, and image blurring. To verify the effectiveness, the proposed method is examined with the following parameters: (i) elapsed time; (ii) robustness; (iii) mean squared error (MSE); (iv) peak signal-to-noise ratio (PSNR); and (v) structural similarity index (SSIM).

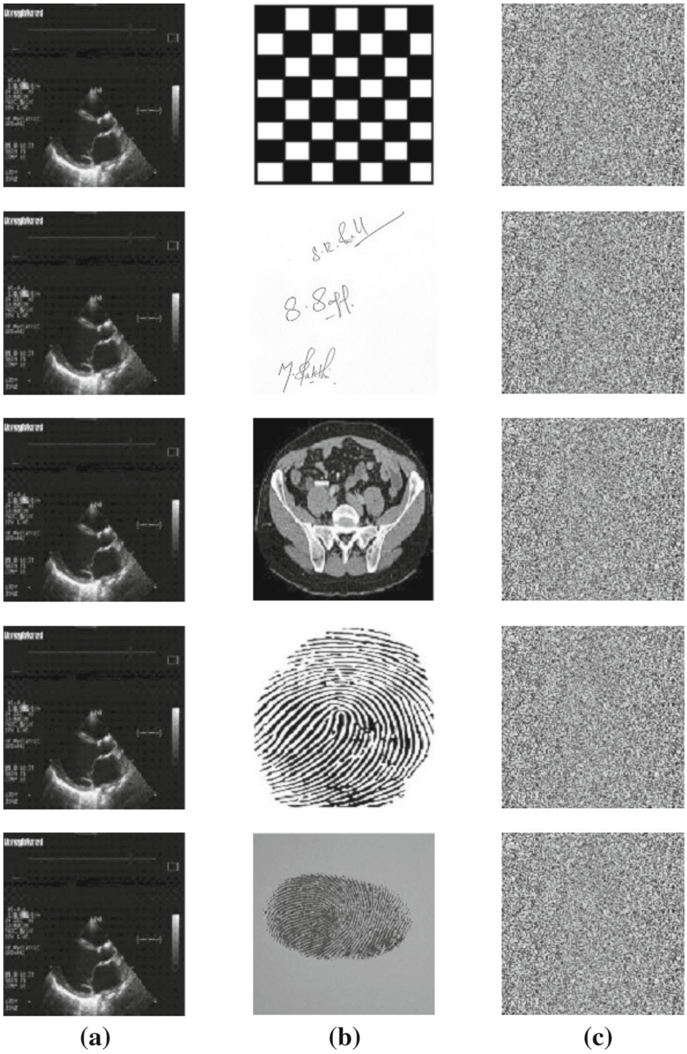

Fig. 6 Watermark embedding process: **a** cover video (frame 1); **b** watermark image; **c** encrypted watermark image

3.1 Evaluation Parameters

3.1.1 Elapsed Time

The elapsed time is an important metric used to evaluate the performance of the proposed watermarking and encryption algorithm. The elapsed time refers to the time required to complete a process that includes fuzzy-based embedding and extracting processes using CA transform and SVD, as shown in Table 1.

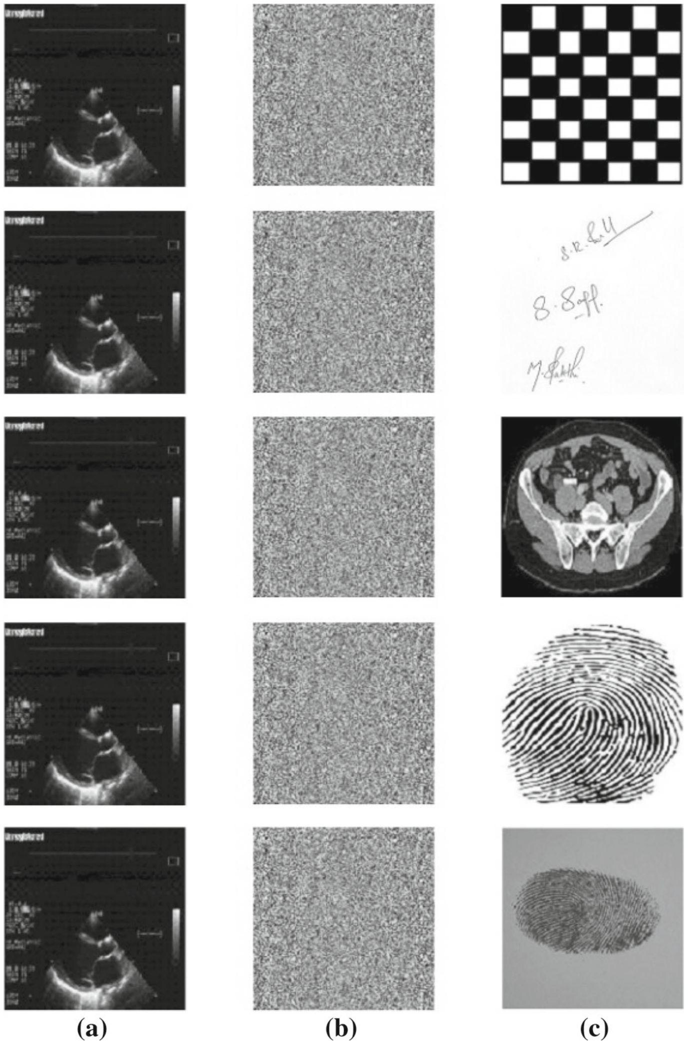

Fig. 7 Watermark extracting process: **a** watermarked video frame; **b** extracted encrypted watermark image; **c** decrypted watermark image

3.1.2 Robustness Analysis

The bit error rate (BER) and normalized cross-correlation (NCC) values between the watermark image and the extracted watermark image with the following two attacks, geometric and non-geometric, are compared to establish the robustness benchmark property of the proposed method [20]. Robustness and quality measurements of the proposed scheme without attack are listed in Table 1 and those with attacks are listed in Tables 2, 3, 4, and 5. The correlation between the watermark image and the extracted watermarked image is calculated as follows:

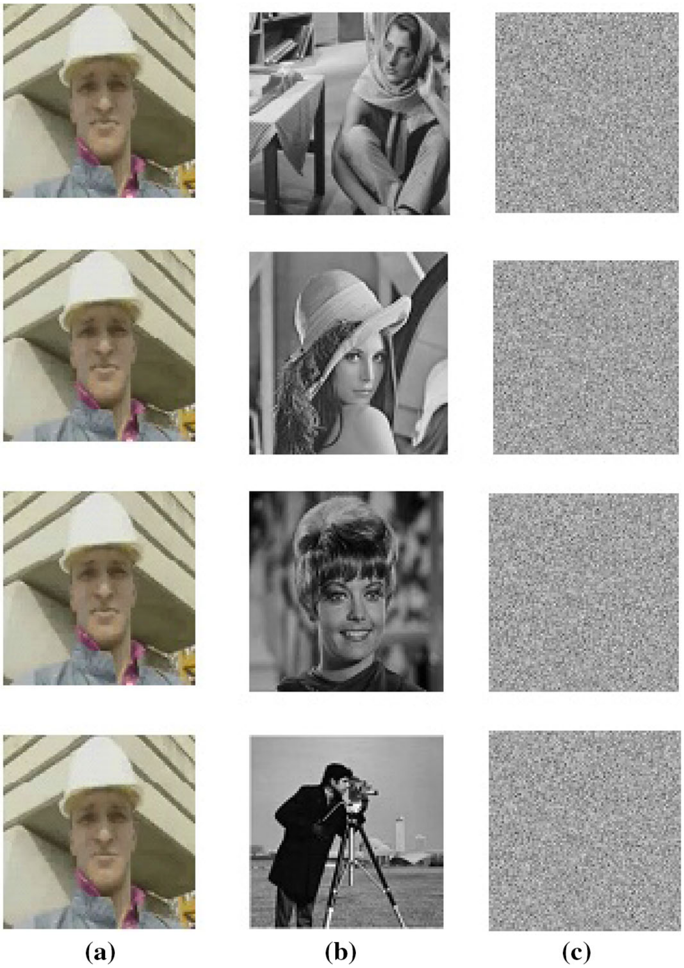

Fig. 8 Watermark embedding process: **a** cover video frames (frame 3); **b** watermark image; **c** encrypted watermark image

$$\text{BER} = \frac{\text{Number of error bits}}{\text{total transmitted bits}} \tag{16}$$

$$NCC(W_i, W_{i1}) = \frac{\sum_{i=1}^{N} \{w_i(x, y)][w_{i1}(x, y)}{\sqrt{\sum_{i=1}^{N} (w_{i1}(x, y))^2}\sqrt{\sum_{i=1}^{N} (w_{i1}(x, y))^2}} \tag{17}$$

where w_i denotes the mean value of the original watermark image at coordinate (*x*,*y*), w_{i1} depicts the mean value for the extracted watermark image at the coordinate (*x*,*y*), and *N* represents the number of pixels.

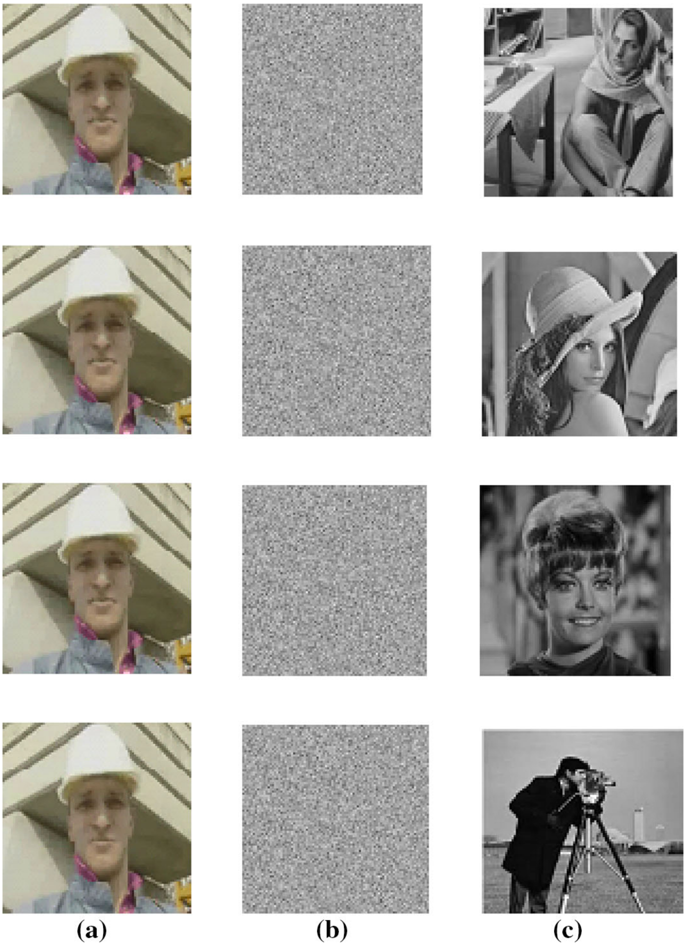

Fig. 9 Watermark extracting process: **a** watermarked video frames; **b** extracted encrypted watermark image; **c** decrypted watermark image

3.1.3 Mean Squared Error

The MSE is an important metric used to measure the average value of the energy lost in the embedding technique. The term MSE is calculated in decibels, which defines the error function of the watermark image pixel $W(x, y)$ and the extracted watermark image pixel value $D(x, y)$, as shown in Table 1. Mathematically, it is calculated as

$$MSE = \frac{1}{(M \times N)} \sum_{x=1}^{M} \sum_{y=1}^{N} \{W(x, Y) - D(x, y)]^2 \tag{18}$$

where M and N are the size of the images, $W(x,y)$ represents the original watermark image, and $D(x,y)$ denotes the extracted watermark image.

Table 1 Robustness and quality measurements of the proposed scheme without attack

Watermark images	Elapsed time (in s)	MSE	PSNR (in dB)	BER	NCC	SSIM
Synthetic chessboard image	6.0235	0.1360	56.795	0	1	1
Digital signature	6.0235	0.1489	56.401	0	1	1
Medical image	6.0235	0.1431	56.579	0	1	1
Fingerprint	6.0235	0.1436	56.598	0	1	1
Real-time image	6.0235	0.1422	56.601	0	1	1

Table 2 Robustness and quality measurements for the proposed method against compression and geometric transformation attacks

Attacks	Synthetic chessboard image				Real-time image			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
JPEG compression (factor = 20)	56.264	0.9926	0.0067	0.9931	56.018	0.9979	0.0032	0.9926
JPEG compression (factor = 40)	56.487	0.9965	0.0049	0.9978	56.129	0.9998	0.0002	0.9982
JPEG compression (factor = 60)	56.598	1	0	1	56.327	1	0	1
JPEG compression (factor = 70)	56.601	1	0	1	56.523	1	0	1
Rotation (−45°)	55.452	0.9865	0.0142	0.9871	55.395	0.9855	0.0150	0.9865
Rotation (−5°)	55.956	0.9926	0.0071	0.9984	55.891	0.9950	0.0050	0.9973
Rotation (5°)	55.951	0.9931	0.0069	0.9989	55.895	0.9948	0.0049	0.9980
Rotation (22.5°)	55.789	0.9917	0.0083	0.9968	55.631	0.9925	0.0075	0.9972
Rotation (45°)	55.452	0.9865	0.0142	0.9872	55.397	0.9852	0.0157	0.9862
Cropping (64 × 64)	56.261	1	0	1	56.387	1	0	1
Cropping (128 × 128)	56.124	0.9988	0.0012	0.9998	55.987	0.9968	0.0032	0.9986
Image scaling (factor = 2)	56.569	0.9964	0.0024	0.9998	56.487	0.9987	0.0012	0.9967
Image scaling (factor = 4)	55.968	0.9905	0.0098	0.9945	55.987	0.9934	0.0074	0.9918
Image scaling (factor = 8)	55.587	0.9884	0.0112	0.9874	55.681	0.9881	0.0127	0.9875
Image scaling (factor = 16)	55.125	0.9865	0.0142	0.9821	55.324	0.9857	0.0143	0.9834

3.1.4 PSNR Analysis

The PSNR is employed to measure the quality of the proposed method. In the effective invisible watermarking technique, the watermark is invisible from the HVS with the standard PSNR [18]. The PSNR value is represented as,

$$\mathrm{PSNR} = 10\mathrm{Log}_{10}\{\mathrm{Max}^2/\mathrm{MSE}\} \tag{19}$$

Table 3 Robustness and quality measurements for the proposed method against compression and geometric transformation attacks

Attacks	Digital signature				Medical image				Fingerprint			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
JPEG compression (factor = 20)	56.107	0.9851	0.0073	0.9851	56.274	0.9896	0.0022	0.9926	56.089	0.9854	0.0059	0.9839
JPEG compression (factor = 40)	56.343	0.9965	0.0038	0.9965	56.470	0.9985	0.0010	0.9989	56.291	0.9966	0.0021	0.9967
JPEG compression (factor = 60)	56.581	1	0	1	56.642	1	0	1	56.532	1	0	1
JPEG compression (factor = 70)	56.815	1	0	1	56.911	1	0	1	56.809	1	0	1
Rotation (−45°)	55.445	0.9823	0.0210	0.9869	55.521	0.9843	0.0120	0.9863	55.398	0.9811	0.0199	0.9860
Rotation (−5°)	55.656	0.9929	0.0091	0.9966	55.856	0.9947	0.0045	0.9964	55.556	0.9923	0.0086	0.9958
Rotation (5°)	55.749	0.9931	0.0085	0.9985	55.895	0.9939	0.0042	0.9981	55.695	0.9925	0.0078	0.9976
Rotation (22.5°)	55.681	0.9930	0.0068	0.9959	55.712	0.9923	0.0051	0.9954	55.526	0.9928	0.0071	0.9947
Rotation (45°)	55.315	0.9824	0.0209	0.9866	55.486	0.9848	0.0137	0.9861	55.352	0.9846	0.0192	0.9865
Cropping (64 × 64)	56.318	1	0	1	56.975	1	0	1	56.018	1	0	1
Cropping (128 × 128)	56.189	0.9978	0.0035	0.9978	55.758	0.9986	0.0023	0.9985	56.098	0.9976	0.0031	0.9972

Table 3 continued

Attacks	Digital signature				Medical image				Fingerprint			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
Image scaling (factor = 2)	56.451	0.9958	0.0026	0.9965	56.687	0.9985	0.0018	0.9978	56.584	0.9947	0.0021	0.9981
Image scaling (factor = 4)	55.983	0.9932	0.0079	0.9946	56.087	0.9956	0.0064	0.9951	55.897	0.9931	0.0075	0.9976
Image scaling (factor = 8)	55.476	0.9883	0.0123	0.9862	55.581	0.9898	0.0103	0.9873	55.654	0.9864	0.0118	0.9926
Image scaling (factor = 16)	55.232	0.9858	0.0156	0.9821	55.419	0.9887	0.0134	0.9824	55.348	0.9849	0.151	0.9865

Table 4 Robustness and quality measurements for proposed method against the addition of noises and enhancement attacks

Attacks	Synthetic chessboard image				Real-time image			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
Gaussian noise (var = 0.2)	55.923	0.9974	0.0014	0.9978	55.571	0.9965	0.0032	0.9987
Gaussian noise (var = 0.3)	55.864	0.9926	0.0062	0.9865	55.321	0.9899	0.0135	0.9958
Gaussian noise (var = 0.4)	55.682	0.9867	0.0124	0.9832	55.239	0.9851	0.0169	0.9903
Gaussian noise (var = 0.5)	55.489	0.9801	0.0199	0.9786	55.097	0.9812	0.0170	0.9872
Speckle noise (var = 0.2)	55.956	0.9986	0.0024	0.9989	55.998	0.9978	0.0026	0.9981
Speckle noise (var = 0.3)	55.785	0.9914	0.0093	0.9911	55.598	0.9936	0.0064	0.9929
Speckle noise (var = 0.4)	55.698	0.9859	0.0148	0.9876	55.389	0.9910	0.0090	0.9899
Speckle noise (var = 0.5)	55.481	0.9823	0.0174	0.9834	55.178	0.9856	0.0151	0.9818
Salt and pepper noise (var = 0.2)	56.321	0.9983	0.0017	0.9989	56.201	0.9978	0.0023	0.9984
Salt and pepper noise (var = 0.3)	55.978	0.9925	0.0079	0.9938	55.861	0.9926	0.0065	0.9921
Salt and pepper noise (var = 0.4)	55.569	0.9878	0.0139	0.9878	55.798	0.9889	0.0123	0.9869
Salt and pepper noise (var = 0.5)	55.331	0.9835	0.0178	0.9826	55.632	0.9861	0.0139	0.9865
Median filtering (2 × 2)	56.601	0.9986	0.0008	0.9979	56.591	0.9991	0.0006	0.9986
Median filtering (2 × 3)	56.489	0.9972	0.0010	0.9965	56.532	0.9972	0.0011	0.9971
Median filtering (3 × 3)	56.362	0.9951	0.0012	0.9934	56.470	0.9959	0.0015	0.9954
Median filtering (4 × 4)	56.187	0.9932	0.0021	0.9912	56.201	0.9933	0.0019	0.9947
Brightness (increased by 5%)	55.986	0.9984	0.0015	0.9902	55.678	0.9987	0.0013	0.9986
Brightness (increased by 15%)	55.684	0.9956	0.0017	0.9989	55.439	0.9968	0.0029	0.9972
Brightness (increased by 25%)	55.539	0.9862	0.0021	0.9872	55.214	0.9943	0.0030	0.9868
Brightness (decreased by 5%)	55.967	0.9987	0.0013	0.9924	55.668	0.9989	0.0011	0.9968
Brightness (decreased by 15%)	55.627	0.9951	0.0019	0.9981	55.487	0.9971	0.0015	0.9923
Brightness (decreased by 25%)	55.532	0.9860	0.0023	0.9965	55.203	0.9950	0.0020	0.9859
Contrast (increased by 5%)	55.968	0.9974	0.0023	0.9923	55.597	0.9975	0.0023	0.9984
Contrast (increased by 15%)	55.853	0.9891	0.0122	0.9901	55.384	0.9907	0.0094	0.9965
Contrast (increased by 25%)	55.671	0.9875	0.0129	0.9886	55.267	0.9851	0.0162	0.9868
Image blurring	55.789	0.9926	0.0073	0.9965	55.869	0.9868	0.0140	0.9926

where MSE represents the mean squared error and Max denotes the maximum value obtained from the two images. The PSNR finds the similarity between the watermark image and the extracted watermark image without attack as shown in Table 1, and with various attacks as shown in Tables 2, 3, 4, and 5. There is no visual difference between the cover video and the watermarked video, and thus the proposed method shows a high degree of imperceptibility, which is shown in Figs. 6, 7, 8, and 9.

Table 5 Robustness and quality measurements for the proposed method against the addition of noises and enhancement attacks

Attacks	Digital signature				Medical image				Fingerprint			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
Gaussian noise (Var = 0.2)	55.989	0.9952	0.0021	0.9943	56.957	0.9968	0.0019	0.9971	56.857	0.9953	0.0023	0.9952
Gaussian noise (Var = 0.3)	55.879	0.9851	0.0053	0.9876	55.848	0.9953	0.0056	0.9983	55.736	0.9949	0.0061	0.9895
Gaussian noise (Var = 0.4)	55.768	0.9844	0.0115	0.9843	55.539	0.9951	0.0105	0.9923	55.559	0.9943	0.0120	0.9863
Gaussian noise (Var = 0.5)	55.345	0.9798	0.0173	0.9806	55.298	0.9949	0.0126	0.9886	55.312	0.9932	0.0168	0.9821
Speckle noise (Var = 0.2)	55.941	0.9963	0.0032	0.9942	56.282	0.9998	0.0025	0.9983	55.982	0.9986	0.0039	0.9979
Speckle noise (Var = 0.3)	55.685	0.9905	0.0083	0.9902	55.958	0.9982	0.0056	0.9965	55.785	0.9912	0.0074	0.9923
Speckle noise (Var = 0.4)	55.489	0.9874	0.0123	0.9881	55.732	0.9895	0.0092	0.9892	55.522	0.9858	0.0119	0.9879
Speckle noise (Var = 0.5)	55.281	0.9833	0.0154	0.9842	55.416	0.9858	0.0128	0.9858	55.356	0.9848	0.0149	0.9823
Salt and pepper noise (Var = 0.2)	55.921	0.9932	0.0021	0.9954	56.519	0.9985	0.0018	0.9978	56.901	0.9965	0.0023	0.9932
Salt and pepper noise (Var = 0.3)	55.878	0.9905	0.0089	0.9914	55.824	0.9974	0.0061	0.9952	55.821	0.9914	0.0076	0.9919
Salt and pepper noise (Var = 0.4)	55.639	0.9857	0.0129	0.9876	55.681	0.9893	0.0113	0.9897	55.594	0.9896	0.0121	0.9889

Table 5 continued

Attacks	Digital signature				Medical image				Fingerprint			
	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM	PSNR	NCC	BER	SSIM
Salt and pepper noise (Var $=$ 0.5)	55.312	0.9818	0.0138	0.9841	55.254	0.9854	0.0124	0.9854	55.262	0.9843	0.0149	0.9831
Median filtering(2×2)	56.651	0.9979	0.0011	0.9965	56.911	0.9982	0.0009	0.9986	56.897	0.9972	0.0017	0.9979
Median filtering(2×3)	56.439	0.9964	0.0019	0.9954	56.827	0.9979	0.0013	0.9972	56.724	0.9967	0.0021	0.9962
Median filtering(3×3)	56.258	0.9947	0.0026	0.9942	56.685	0.9956	0.0020	0.9945	56.689	0.9936	0.0034	0.9934
Median filtering(4×4)	56.089	0.9939	0.0039	0.9912	56.225	0.9942	0.0023	0.9923	56.482	0.9929	0.0039	0.9924
Brightness increased by 5%	55.826	0.9974	0.0015	0.9956	55.962	0.9982	0.0012	0.9996	55.986	0.9979	0.0018	0.9982
Brightness increased by 15%	55.674	0.9927	0.0024	0.9935	55.765	0.9958	0.0029	0.9982	55.753	0.9931	0.0029	0.9965
Brightness increased by 25%	55.581	0.9821	0.0039	0.9889	55.698	0.9931	0.0033	0.9898	55.521	0.9829	0.0041	0.9819
Brightness decreased by 5%	55.928	0.9987	0.0017	0.9914	55.989	0.9989	0.0014	0.9989	55.458	0.9982	0.0021	0.9972
Brightness decreased by 15%	55.767	0.9954	0.0025	0.9903	55.657	0.9976	0.0021	0.9976	55.269	0.9964	0.0036	0.9958
Brightness decreased by 25%	55.568	0.9873	0.0041	0.9895	55.468	0.9925	0.0036	0.9893	55.112	0.9841	0.0049	0.9865
Contrast increased by 5%	55.618	0.9982	0.0023	0.9954	55.871	0.9985	0.0017	0.9982	55.854	0.9979	0.0028	0.9943
Contrast increased by 15%	55.553	0.9918	0.0102	0.9932	55.798	0.9976	0.0084	0.9961	55.658	0.9925	0.0112	0.9923
Contrast increased by 25%	55.303	0.9885	0.0149	0.9881	55.654	0.9838	0.0152	0.9895	55.471	0.9873	0.0131	0.9878
Image blurring	55.784	0.9937	0.0072	0.9972	55.857	0.9891	0.0130	0.9969	55.954	0.9952	0.0067	0.9981

3.1.5 Structural Similarity

The SSIM index is a method used to predict the perceived quality of digital images based on an initial uncompressed image or a distortion-free image as a reference. The SSIM values for the proposed method without attack are shown in Table 1 and those with attacks are shown in Tables 2, 3, 4, and 5. The SSIM of the proposed method preserves the structural quality of the image.

$$SSIM(x, y) = \frac{(2\mu_x, \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2, \mu_y^2 + c_1)(2\sigma_{xy} + c_2)} \tag{20}$$

where μ_x is the average of the watermark image, μ_y is the average of the extracted watermark image, ${\sigma_x}^2$ is the variance of the watermark image, ${\sigma_y}^2$ is the variance of the extracted watermark image, and σ_{xy} is the covariance of the watermark and extracted watermark image.

3.2 Robustness Test for Images

Robustness represents the confrontation for the deformation or elimination of the watermark due to various types of attacks, such as premeditated or unpremeditated attacks. The proposed method exhibits good robustness against different types of attacks, such as image compression, geometric transformation attacks (rotation, scaling, and cropping), the addition of noises (Gaussian, speckle, and salt and pepper), and common signal-processing operations (median filtering, image blurring, brightness, and contrast attacks) [3, 16, 19].

3.2.1 Performance Under JPEG compression

The watermarked video is compressed with different quality factors, ranging from 20 to 70. The quality of the watermarked video is decreased by decreasing the quality factor. The extracted watermark images with NCC and BER values from the compressed watermarked video are depicted in Tables 2 and 3, and those with quality factor 60 are shown in Fig. 10. Also, the NCC values of the extracted watermarked images versus different quality factors are plotted in Fig. 11, which indicates the robustness of the proposed scheme against the JPEG compression attack, which is quite high.

3.2.2 Performance Under Geometric Transformation Attacks

When the value of a watermarked video is opposed too much by applying a small rotation, the encrypted watermarked image can be affected. The robustness of the proposed method is examined from 5° to 45° and from -5° to -45°, and the effectiveness of the proposed method is represented by its quantitative values in Tables 2 and 3, which show that the watermark image is effectively extracted by the proposed method for the rotation attack. The robustness against the rotation attack is tested at angles of 45° and -45°, as shown in Fig. 12. Figure 13 represents the SSIM between the watermark image and the extracted watermark image after applying a rotation attack.

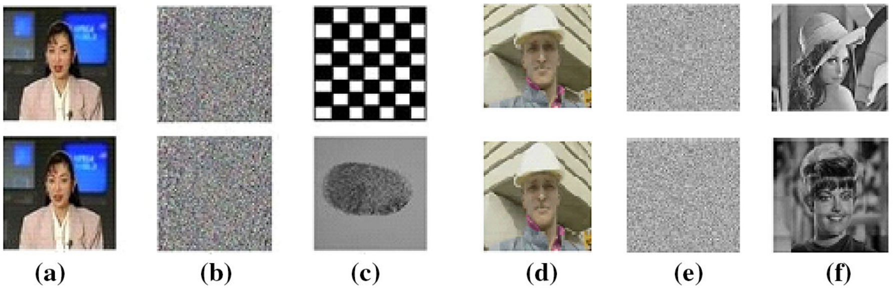

Fig. 10 **a** and **d** JPEG compression ($Q = 60$) attack of watermarked video; **b** and **e** extracted encrypted watermark images; **c** and **f** decrypted watermark images

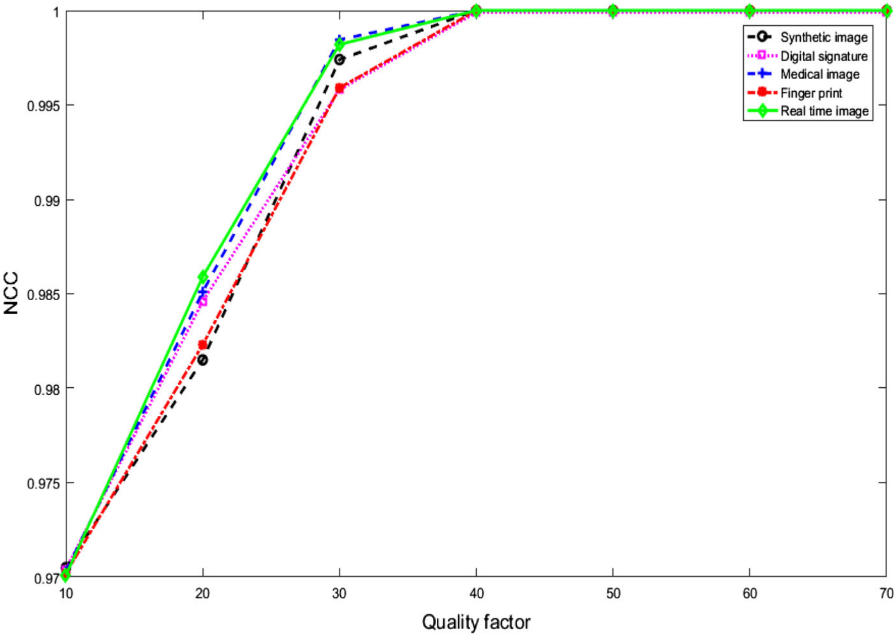

Fig. 11 Quality factor versus NCC

For a cropping attack, up to 50% of the watermarked video is cropped and tested. The extracted watermark image is shown in Fig. 12. The watermark image is effectively extracted by the proposed method for a cropping attack and is illustrated with quantitative values in Tables 2 and 3.

For a scaling attack, the size of the watermarked video sequences is reduced by the different factors and then returned to the original size. The watermarked video is scaled by a factor of 2, as shown in Fig. 12; the scaled image loses a lot of data, but the extracted watermark is still recognizable. The robustness and SSIM values of the extracted watermarks acquired by the proposed scheme for various watermark images are listed in Tables 2 and 3, which show that the proposed method provides better

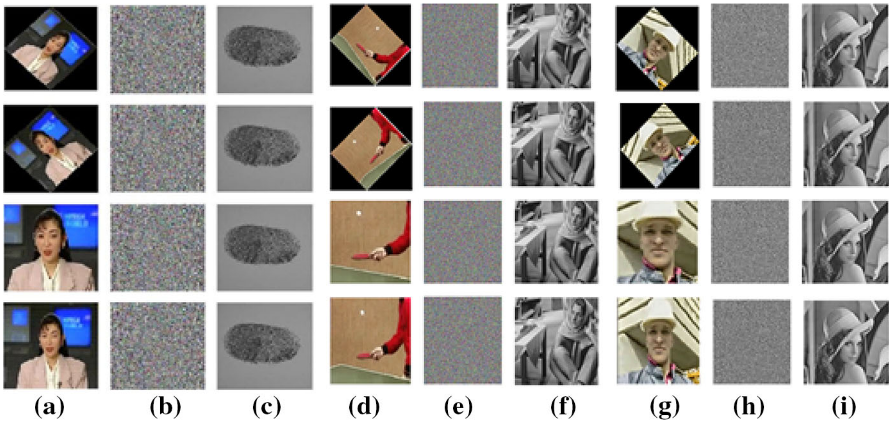

Fig. 12 **a**, **d**, and **g** Rotation attack of a watermarked video with −45° and 45° rotation angles, cropped with 128 × 128 and a scaling attack of factor 2; **b**, **e**, and **h** extracted encrypted watermark image **c**, **f**, and **i** decrypted watermark images

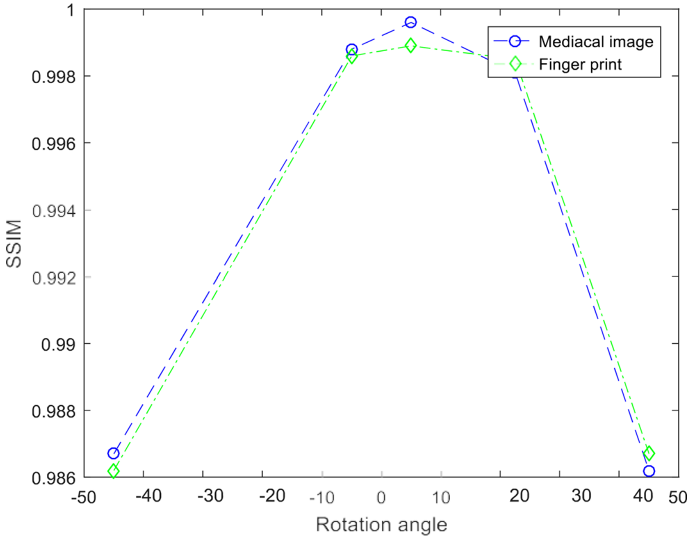

Fig. 13 Different rotation angles versus SSIM values

robustness against the scaling attack. The SSIM values for test watermark images with scaling factors 2, 4, 8, and 16 are plotted in Fig. 14.

3.2.3 Performance Under Addition of Noises

To evaluate the proposed method, noise is added to the watermarked video for the different variance and the watermark image thus extracted is analyzed as follows. Gaussian noise is one of the statistical noise processing operations and is used to prove the robustness of the proposed method. By the addition of noise to the watermarked

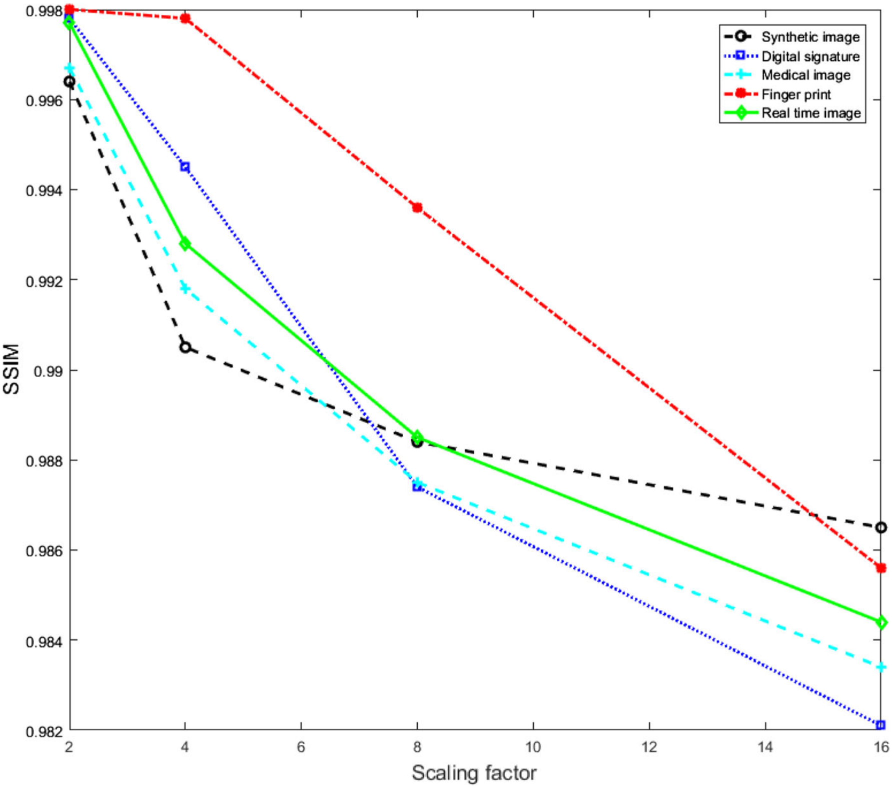

Fig. 14 Scaling factor versus SSIM values for various watermark images

video with variance from 0.1 to 0.5, the quantitative values for the extracted watermark are presented in Tables 4 and 5. The results of Fig. 15 show that the extracted watermark image is highly correlated with the original watermark image, and its NCC values for different watermark images with variances are shown in Fig. 16.

Speckle noise is a multiplicative noise that exists inherently like a granular noise. The variance of the single pixel and that of the local area are equal and centered on that pixel. It can be understood easily that the image quality of the extracted watermark is improved with the decrement of the noise variant. The proposed method is tested against speckle noise under different noise variances from 0.1 to 0.5 and is depicted in Tables 4 and 5.

Salt and pepper noise is caused by pixel error at the time of data transmission. In salt and pepper noise, tainted pixel values are set to zero, a maximum value, or to single bits flipped over. This pixel value alteration gives an image like salt and pepper emergence, where the noise density is calculated by the modification of the percentage of pixels. The modified watermarked videos by speckle noise and salt and pepper noise of noise density 0.5 and 0.3, with the extracted encrypted watermark image and decrypted watermark image, are shown in Fig. 15. Robustness and quality measurement values of the extracted watermark images with different noise densities

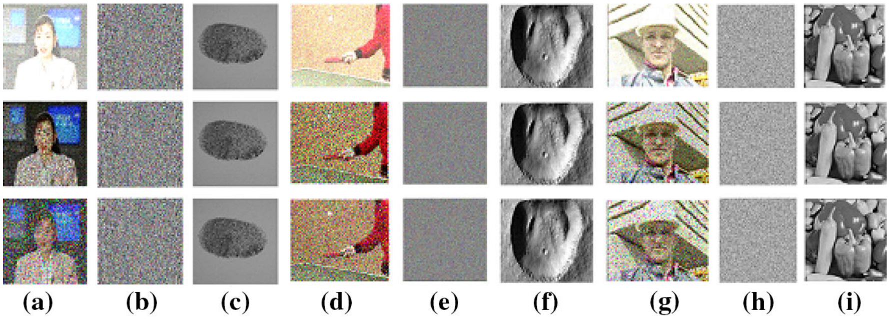

Fig. 15 **a** Watermarked video attacked by Gaussian noise, speckle noise, and salt and pepper noise with variance 0.5; **d** and **g** watermarked videos attacked by Gaussian noise, speckle noise, and salt and pepper noise with variance 0.3; **b**, **e**, and **h** extracted encrypted watermark images; **c**, **f**, and**i** decrypted watermark images

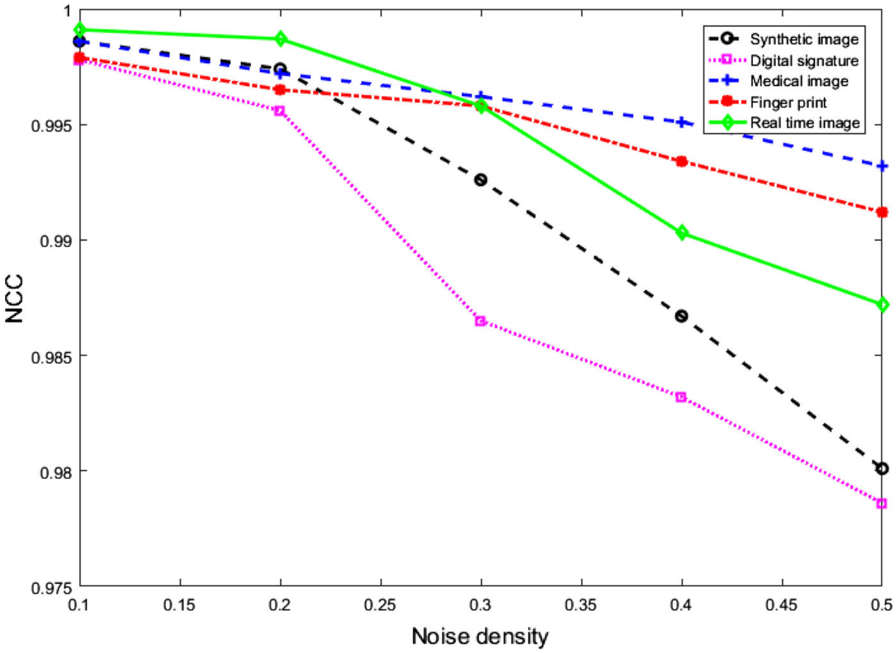

Fig. 16 Noise density versus NCC of Gaussian noise

are given in Tables 4 and 5. The NCC values of the digital signature watermark images are plotted against different noise densities for a different method, as shown in Fig. 17.

3.2.4 Performance Under Enhancement Attacks

In image enhancement applications, a median filter modifies the center pixel value of the window with the middle value of the sorted pixel values. The proposed method is

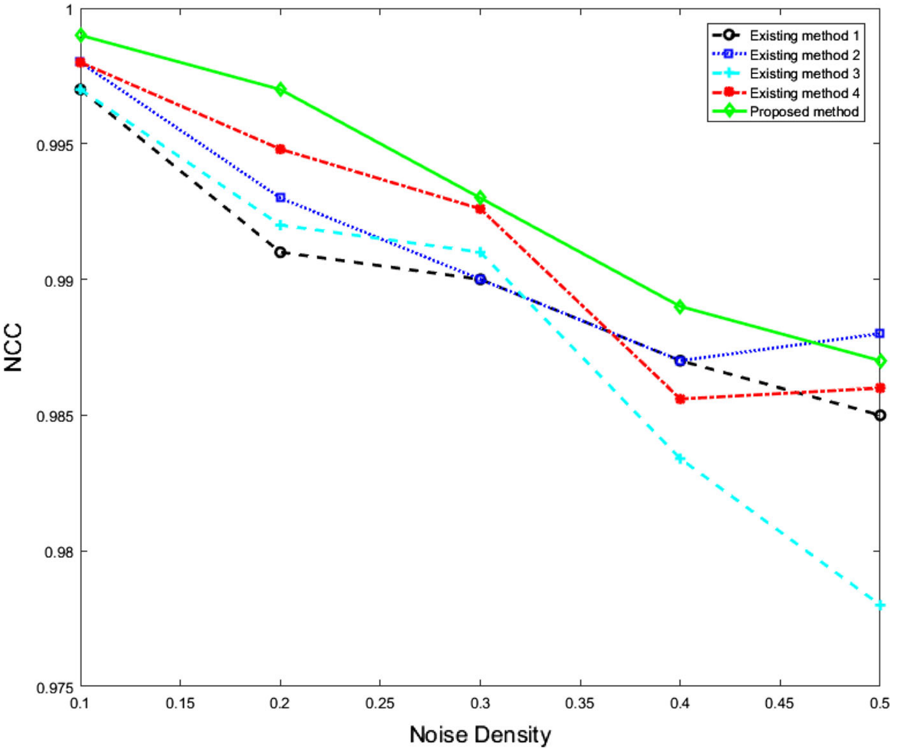

Fig. 17 Comparison of NCC verses noise density for various methods

examined in opposition to median filtering attacks with different window sizes of 2 × 2, 3 × 3, 2 × 3, and 4 × 4. The extracted watermark images and their corresponding median filtering modified images are shown in Fig. 18. The BER and NCC values of the extracted watermark images prove that the robustness and the PSNR values show the quality of extraction against the median filtering attack, as tabulated in Tables 4 and 5.

Brightness and contrast attacks are the common attacks on multimedia. The brightness and contrast of the watermarked video are increased and decreased from 5 to 25%, respectively. The brightness and contrast of the image are increased by 5%, as shown in Fig. 18. The performance metrics are presented in Tables 4 and 5 and show the robustness of the proposed method and also confirm the steadiness of the method. For a motion blur attack, a motion of 70 pixels with an angle of 100° in the counterclockwise direction is considered. The proposed scheme is highly robust against these attacks and is shown clearly in Fig. 18 and the NCC, PSNR, and SSIM values are given in Table 3.

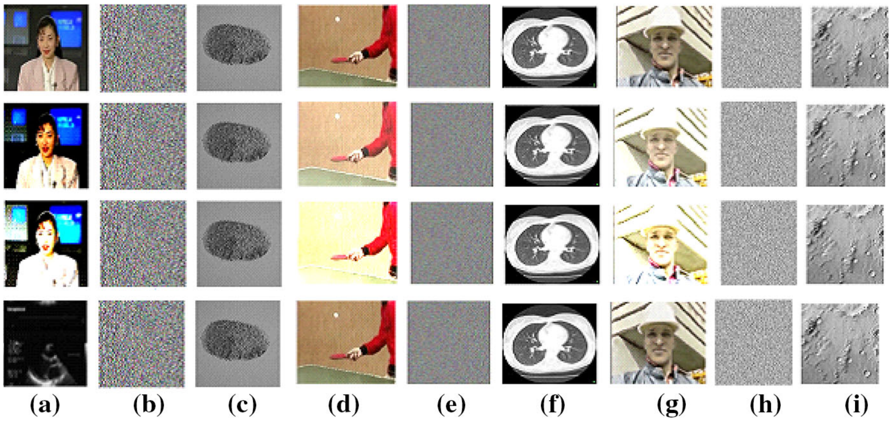

Fig. 18 **a**, **d**, and **g** Watermarked videos against median filtering (2 × 2), brightness and contrast increased by 5%, and blurring; **b**, **e**, and **h** extracted encrypted watermark images; **c**, **f**, and **i** decrypted watermark images

3.3 Comparative Analysis

The proposed scheme is compared with the existing watermarking methods, and the evaluation parameters are tabulated in Table 6. The experimental results of the PSNR, NCC, and graphical analysis for SSIM with and without attack are shown in Fig. 19, which conclude the eminence of the proposed scheme. Robustness and quality measurement values of the extracted watermark against the various attacks are illustrated for the synthetic chessboard watermark image in Table 6.

4 Conclusion

This paper has proposed a fuzzy-based digital video watermarking algorithm. The CA and SVD algorithm with fuzzy-based embedding improved the quality and robustness of the extracted watermark image and guaranteed high authenticity against the various attacks. Here, pixel scrambling for the watermark image is achieved by the 1D CA transform, which provides security, and the FIS is used to enhance the data-hiding capacity. The 3D CA transform ensures high robustness and confidentiality for multiple transform planes. Hence, SVD enhances the imperceptibility and improves the robustness of the watermarked image by resistance against various types of attacks due to non-fixed orthogonal bases. Moreover, the technique provides resistance against various attacks, such as JPEG compression, rotation, cropping, image scaling, Gaussian noise, speckle noise, salt and pepper noise, median filtering, brightness, contrast, and image blurring. The proposed method improves the quality and robustness of the extracted watermark image, which is exposed by the quality metrics; for example, the PSNR value of the extracted watermark image is in the range of 54–56 dB. However, the NCC value obtained from the extracted watermark image is maintained above 99.5%; the SSIM value of the proposed method also clearly shows that it preserves the

Table 6 Comparison of the proposed method with existing methods against various attacks

Attacks	Existing method 1 [6]		Existing method 2 [14]		Existing method 3 [3]		Existing method 4 [16]		Proposed method	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
Without attack	47.24	0.99	55.67	0.99	49.76	0.96	49.67	1	56.58	1
JPEG compression (Q = 50)	46.54	0.98	55.60	0.99	49.87	0.93	47.72	1	56.68	1
Rotation (45º)	47.13	0.97	55.33	0.98	48.76	0.92	23.89	0.84	55.45	0.99
Cropping (128 × 128)	47.02	0.99	55.57	0.99	46.65	0.87	47.64	0.88	56.26	1
Image scaling (factor = 2)	46.36	0.98	54.26	0.99	52.87	0.97	48.86	0.98	56.57	0.99
Gaussian noise (Var = 0.5)	46.26	0.99	55.12	0.98	49.07	0.91	34.85	0.94	55.49	0.98
Speckle noise (Var = 0.5)	46.36	0.97	54.99	0.98	43.23	0.97	48.63	0.97	55.48	0.98
Salt and pepper noise (Var = 0.5)	45.79	0.99	55.22	0.98	48.43	0.94	32.91	0.91	55.33	0.99
Median filtering (2 × 2)	46.99	0.96	55.78	0.98	48.31	0.90	52.97	0.98	56.60	0.99
Brightness (increased by 5%)	47.04	0.99	55.52	0.93	48.76	0.97	49.79	0.95	55.99	0.99
Contrast (increased by 5%)	47.27	0.99	55.43	0.99	49.87	0.98	48.78	0.99	55.97	0.99
Image blurring	45.04	0.98	55.36	0.99	47.52	0.91	37.68	0.76	55.79	0.99

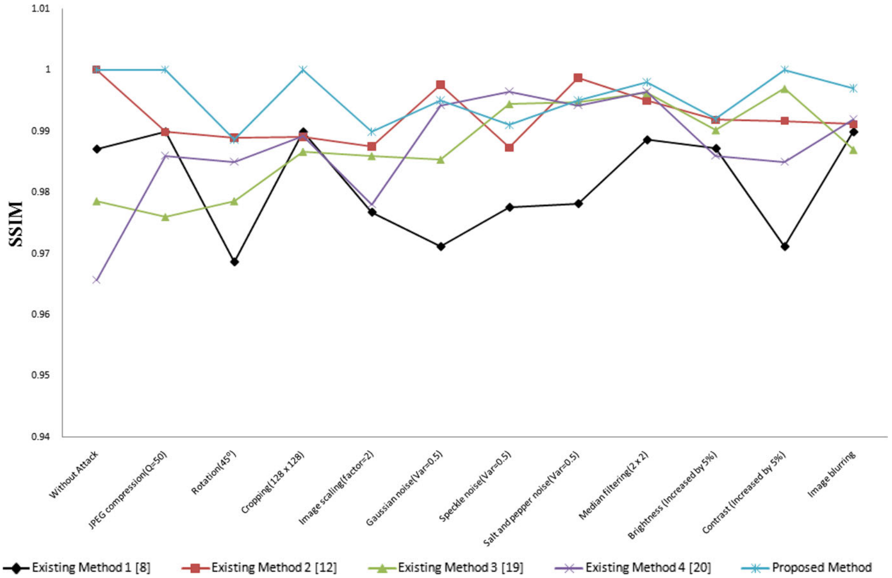

Fig. 19 Comparative analysis of SSIM of the proposed method with existing methods

fine details of the extracted watermark image. Thus, the proposed method provides better robustness and security for the transmitted watermark image, which is useful for copyright protection.

Availability of data and Materials The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.

References

1. Md. Asikuzzaman, Md.J. Alam, A. Lambert, M.R. Picering, Robust DT CWT-based DIBR 3D Video wWatermarking using Chrominance Embedding. IEEE Trans. Multi. **18**(9), 1733–1748 (2016)
2. Md. Asikuzzaman, R.M. Pickering, An Overview of Digital Video Watermarking. IEEE Trans. Circuits Systems Video Tech.. **28**(9), 1–23 (2017)
3. V. Ashok Kumar, C. Dharmaraj, Ch. Srinivasa Rao, A Hybrid Digital Watermarking Approach using wavelets and LSB. Int. J. Electrical Comp. Eng. (IJECE)**7**, 2483–2495 (2017).
4. D. Bhowmik, C. Abhayaratne, Quality Scalability Aware Watermarking for Visual Content. IEEE Trans. Image Process. **25**(11), 5158–5172 (2016)
5. S.Dong, J.Li, S.Liu, Frequency Domain Digital Watermark Algorithm Implemented in Spatial Domain Based on Correlation Coefficient and Quadratic DCT Transform, IEEE International Conference on Progress in Informatics and Comput. (2016), pp.596–600.
6. S.K. Habiba, D. Niranjanbabu, Advance Digital Video Watermarking based on DWT-PCA for copyright protection.Int. J. Res. Appli. **4**(10), 73–78 (2014)
7. ImageProcessingplace.com:Imagedatabase,https://www.imageprocessingplace.com/root_files_V3/image_databases.html.Accessed,24 January 2019.
8. Jet Propulsion Laboratoy: photojournal, https://photojournal.jpl.nasa.gov/new. Accessed, 25 January 2019.
9. S.Kadu, Ch.Naveen, V.R.Satpute, A.G.Keskar: Discrete Wavelet Transform Based Video Watermarking technique, International Conference on Microelectronis, Computing and Comm. (2016), pp.25–30.

10. A.Kunhu, K. Nisi, S.Sabnam, A.M.Saeed AL-Mansoori, Index Mapping based Hybird DWT-DCT Watermarking Technique for Copyright Protection of video files, International Conference on Green Engineering and Tech. (2016), pp.1–8.
11. X. Liu, F. Li, J. Du, R.M. Pickering, A robust and synthesized-unseen watermarking for the DRM of DIBR-based 3D video. Neurocomput. **222**, 155–169 (2016)
12. X.W.Li, S.J.Cho, S.T.Kim, A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. Optik – International Journal for Light and Electron Optics 125 (13), 2983–2990 (2014).
13. X.W. Li, I.K. Lee, Robust Copyright Protection using Multiple Ownership Watermarks. Optical Soc. Am. **23**(3), 3035–3046 (2015)
14. X.W. Li, S.T. Kim, Q.H. Wang, Designing Three-Dimensional Cellular Automata Based Video Authentication With an Optical Integral Imaging Generated Memory-Distributed Watermark. IEEE J. Selected Topics Signal Process.. **11**(7), 1200–1213 (2017)
15. Z.Ma, J.Huang, M.Jiang, X.Niu, A Video Watermarking DRM Method Based on H.264 Compressed Domain with Low Bit-Rate Increasement. Chin. J. Electronics 25(4), 641–647 (2016).
16. L.Narkedamilly, V.Prasad Evani, S.K.Samayamantula, Discrete Multiwavelet-based Video Watermarking Scheme using SURF. ETRI J.**37**, 595–605 (2015).
17. S.Ponni, S.Dhinakaran, P.SabariAshwanth, P.Dhamodharan: Chaotic Map Based Video Watermarking Using DWT and SVD, International Conference on Inventive Communication and Computation and Tech. pp. 45–49, (2017).
18. C. Ramya, S. Subha Rani, Rain Removal in Image Sequence Using Sparse Coding, Communications in Computer and Information Science. Springer, Heidelberg (2012), pp.361–370.
19. C. Ramya, S. Subha Rani, A Sparse based rain removal algorithm for image sequences. Int. J. Robotics Automation**29**, 1–7 (2014).
20. C. Ramya, S. Subha Rani, Video denoising without motion estimation using K means clustering. J.Sci. Industrial Res.**70**, 251–255 (2011).
21. Standford 40 Actions:A dataset for understanding human actions in still images, https://Vision.stanford.edu/Datasets/40actions.htms. Accessed, 25 January 2019.
22. The USC-SIPI Image Database: Image Database, https://sipi.usc.edu/database/. Accessed, 24 January 2019.
23. J.Upadhyay, B.Mishra, P.Patel, A Modified Approach of Video Watermarking Using DWT-BP Based LSB Algorithm, in International Conference on Information, Communication, Instrumentation and Controls, pp.1–6 (2017).
24. Y.Wang, Y.Zhao, Q.Zhou, Z.Lin, Image Encryption Using Partitioned Cellular Automata. Neurocomp. **275**(c), 1318–1332 (2018).