Artificial Intelligence Review
https://doi.org/10.1007/s10462-020-09877-8

A new chaotic complex map for robust video watermarking

Peyman Ayubi[1] · Milad Jafari Barani[2] · Milad Yousefi Valandar[2] · Behzad Yosefnezhad Irani[2] · Reza Sedagheh Maskan Sadigh[2]

Abstract
In this paper, using a new two-dimensional complex map, a secure video watermarking system is presented. Standard analyzes have been performed to analyze a dynamical system to prove the existence of chaos in the proposed map and the results indicate a chaotic behavior in this complex chaotic map. In addition, an efficient algorithm based on IWT, DWT, and CT transforms with the participation of single value decomposition for the embedding and extraction process is introduced. The simulation results showed that the proposed algorithm has good visual quality based on criteria such as PSNR and SSIM. Geometric and non-geometric attacks were also performed on the video obtained by watermarking, and the results showed that the proposed algorithm in many attacks with a value of 1.00 for the NC criterion can be a very robust algorithm against attacks. A correlation-based process for detecting the rotational attack is also presented which makes the rotational geometric attack successfully pass. The comparison of simulation results with other similar algorithms shows that the proposed method performs better than any of these methods in terms of visual quality analysis and attack resistance and can be used as an efficient robust algorithm in applied processes.

Keywords Blind and robust video watermarking · Chaotic complex map · IWT · DWT · CT · SVD

1 Introduction

Nowadays, growth of multimedia data encompasses all aspects of human life, especially in recent decades, the digital world has become a lifestyle. Digital data is now more widely available, due to the growth and development of computers, copying and manipulating the data is very easy for anyone. Given this point of view, the digital content producers is critical of creating a mechanism for protecting digital media. Traditional method of protecting multimedia data, such as encryption, is not effective in maintaining digital content, since it can only protect digital content until decoded, and after

✉ Peyman Ayubi
p.ayubi@iaurmia.ac.ir

[1] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

[2] Young Researchers and Elite Club, Urmia Branch, Islamic Azad University, Urmia, Iran

Published online: 30 July 2020

decoding any unauthorized copying and publication of the original content could be done (Caragata et al. 2016; Barani et al. 2015b; Loganathan and Kaliyaperumal 2016).

Hence, Digital Watermarking was introduced as an art of hiding information and a constructive way to protect inherent features as well as protecting the copyright of multimedia data such as image, video, and audio (Lin et al. 2017; Makbol et al. 2017; Stütz et al. 2014). Digital watermarking can be a good way to maintain the integrity of digital content in network-based communications such as the Internet, mobile, and cloud. Digital video is known as an important and effective media in today's communications world, including its applications in the dissemination of news, videos and cable network broadcasts of video programs. Protecting the ownership rights as well as the authenticity of the content of the video is the most important discussion in the world of video interchange, which the use of watermarking techniques in the field of digital video can create a safe platform to protect the copyright of video data (Inceoglu 2015; Boisvert et al. 2015). In general, the most important features of a watermarking algorithm are robustness, imperceptibility, and data payload. By balancing these three features, the watermarking algorithm can be considered as an efficient and effective way for use in watermarking applications (Selvam et al. 2017; Su and Chen 2017; Sun et al. 2009).

The use of dynamical systems and chaos theory in cryptographic systems has increased dramatically in the last two decades (Kocarev and Lian 2011). Chaotic systems, because of their sensitivity to the initial conditions and control parameters, are the best option for satisfying the confusion and diffusion features in cryptography. The slightest change in initial conditions and control parameters results in large changes in the production of chaotic sequences (Strogatz 2014). This feature is used as a secret key in cryptosystems. In cryptographic systems, chaotic iterated maps are used as pseudo-random numbers generators (Akhshani et al. 2014; Ayubi et al. 2020; Barani et al. 2020a). These PRNGs have been used in a variety of applications of image and video encryption (Valandar et al. 2019a; Irani et al. 2019), image and video watermarking (Valandar et al. 2020; Barani et al. 2015a, 2019, 2020b; Farri and Ayubi 2018), steganography (Valandar et al. 2015, 2017, 2019b), and hash functions (Akhshani et al. 2009).

Classical chaotic maps such as logistics, tent, sine have a small key space due to limitations on the initial conditions variables and control parameters and are not a good option for secure cryptography. For this reason, researchers in the field of dynamical systems and chaos are trying to create new chaotic maps that have a larger key-space and guarantee cryptographic security. For this reason, this paper proposes a 2D chaotic complex map for the security of a video watermarking.

In this paper, the concept of security and randomness of complex map are used which are very sensitive to the initial conditions and have different parameters as the key. In the proposed method, the complex map keys are set to the initial values and then a transform applied on frame. Proposed algorithm selects LL sub band of each channel, then a position in the LL sub bands selected by proposed map to create 4×4 block. SVD is applied to this block, and then one bits of watermark embedded inside the U matrix of SVD. Finally, the inverse of SVD applied on selected block. After embedding process finished, the inverse of selected transform applied on the channels of frame. The last values of the proposed map are used as the keys for the next frame. The extracting process is similar to the embedding process, except that after the logo is extracted, an error correction step is performed by calculating the correlation on the watermark. This paper also suggested a new method for rotation attacks to solve chaotic behaviors in rotation attack and extract watermark correctly after these type of attack.

The remain parts of this paper is organized as follows: Sect. 3 proposed a new 2-D chaotic complex map. Section 5 presents proposed video watermarking algorithm. Performance evaluation and experimental results of the proposed method are presented in Sect. 6. The comparison of proposed method with similar algorithms is shown in Sect. 7. Finally, Sect. 8 concludes this paper.

2 Related works

Watermarking schemes can be categorized in several aspects, one of which is the resistance to image processing attacks. In terms of resistance to image processing attacks, Watermarking can be categorized into three broad categories: 1. Robust watermarking (Moosazadeh and Ekbatanifard 2017; Liu et al. 2017; Chen and Zhao 2017a; Zhang et al. 2012; Sun et al. 2018), 2. Fragile watermarking (Renza and Lemus 2018; Yu et al. 2015) and 3. Semi-fragile watermarking (Al-Otum 2014; Li et al. 2016). In addition to this categorization, watermarking techniques can divided in 2 main group based on watermark embedding domain: spatial domain (Bayoudh et al. 2017; Batool et al. 2014) and frequency domain. The spatial domain is known as the low computational complexity and implementation simplicity (Su et al. 2013). In order to cope with the weaknesses in the spatial domain methods, transform domain based techniques have been developed to initially transform the domain of the image and map it to another values with different frequency transforms, and then use the generated coefficients for the insertion of the watermark. This field is growing and developing according to the type of transforms day by day (Ansari and Pant 2017; Khalilian and Bajic 2013; Soliman et al. 2016). The transforms used in frequency domain watermarking methods are the DFT, DCT, DWT, Contourlet transform (CT),Curvelet, Ridgelet, Shearlet , etc.

Generally, video watermarking have widely diversity, and we will reviews some of these methods. It's important to note that in fact video watermarking is a simple extension of image watermarking. A dynamical method for video watermarking in the wavelet transform domain is proposed by El'Arbi et al. (2011). Belhaj et al. (2010) presented a QIM-based video watermarking technique, which this technique robust against attacks such as noise addition, trans coding, and geometric attacks. Xu et al. (2010) provided a new low-complexity method for video watermarking, which uses CAVLC in the H.264/AVC video format. In Youssef et al. (2014), an adaptive fuzzy model for video watermarking is proposed that is based on the wavelet transform and is a combination of the human vision system and the Video Motion Sub Region. Himeur and Boukabou (2017) introduced a new watermarking method using chaotic map based cryptography for video. This technique is robust against attacks and is based on key frames, which is securely embeds the watermark in the wavelet transform and SVD domain.

Wu et al. (2011) have proposed evolutionary optimization technique for video watermarking in the H.264/AVC compression format. A video watermarking based on one-dimensional Fourier transform and Radon transformYan have been proposed by Liu and Zhao (2010), which is resistant to H.264 compression and RST attack. Dutta and Gupta (2016) proposed a new robust and blind high-efficiency video coding (HEVC) method.

Yassin et al. (2014) proposed a method for video watermarking, based on QIM and in the wavelet transform domain. The method presented in this paper is based on the principal coefficient analysis (PCA) for blind video watermarking. The visual cryptography in Singh et al. (2013) is used for video watermarking, which the watermark is inserted in the DWT transform

coefficients. The color video watermarking method based on combination insertion methods is proposed in Agilandeeswari and Ganesan (2016a). This method is based on Bit Plane Slicing and various transforms such as CT, DWT and SVD. In the contourlet domain transform, Chen and Zhao (2017b) presented a new method for video watermarking, which is resistant to geometric attacks as well as compression. This method is also applicable in both the video and image domain. In general, the proposed method in this paper uses the CT transform to resistance against the compression effects and the PCA to resist against geometric attacks.

Chaos as the science of dynamical systems has recently attracted much attention in areas such as encryption and authentication (Chang et al. 2011; Keyvanpour and Merrikh-Bayat 2011; Behnia et al. 2012). Chaotic maps can be used in cryptography algorithms because of inherent features of chaos and can be used to secure the insertion and extraction processes in the watermarking algorithms (Behnia et al. 2010, 2014; Panahi et al. 2013; Hadi and Ayubi 2012).

3 Proposed 2D chaotic complex map

The univariate family of quadratic polynomials is generally expressed by the following equation:

$$f(Z, \alpha_2, \alpha_1, \alpha_0) = \alpha_2 Z^2 + \alpha_1 Z + \alpha_0 \quad Where \quad \alpha_2 \neq 0 \tag{1}$$

The monic and centered form is the simplest form of a nonlinear function that has one input parameter. In the iterative functional system (IFS) fields, the monic form of quadratic maps in the domain of different values are expressed as follows:

$$Z_{n+1} = Z_n^2 + c \tag{2}$$

where Z is a complex number equal to $Z = x_1 + iy_1$ and c is a constant value equal to $c = x_2 + iy_2$. This relationship is the base of fractal geometry in the models of the Julia and the Mandelbrot sets. In Julia's set, c is constant and Z is various. In this paper, a new method based on iterative complex two-dimensional maps is proposed. Two-dimensional models are better for use in image and video. The mathematical relation of the proposed two-dimensional map is as follows:

$$\begin{cases} Z_1(n+1) \equiv \left[\alpha \left(\frac{Z_1(n)}{Z_2(n)} \right)^2 + c_1 \right] \ CFOLD \ 1 \\ Z_2(n+1) \equiv \left[\beta \left(\frac{Z_2(n)}{Z_1(n)} \right)^2 + c_2 \right] \ CFOLD \ 1 \end{cases} \tag{3}$$

If Z is a complex number, the $CFOLD$(complex folding) is calculated conventionally by the following equation :

$$(Z \ CFOLD \ 1) = Z^{real} \, Mod \, 1 + (Z^{imag} \, Mod \, 1) \times 1i \tag{4}$$

where Mod is a modulo operator in computing and mathematics. In this equation $Z_1^{Real} \in [0, 1]$, $Z_1^{Imag} \in [0, 1]$, $Z_2^{Real} \in [0, 1]$, $Z_2^{Imag} \in [0, 1]$, $C_1^{Real} \in [0, 1]$, $C_2^{Real} \in [0, 1]$ are in the complex number domain and $\alpha \in [10, \infty]$, $\beta \in [10, \infty]$ are in the integer number domain.

3.1 The coloring scheme for the proposed dynamical system

Until the emergence of computer systems, computations were impossible to display graphical systems of dynamic systems in the complex domain. Mandelbrot was the first to use a computer to display of a dynamical system. Since 1980, many computer graphics professionals have created a variety of coloring algorithms for fractals such as Julia, Mandelbrot, and Newton. This art is famous to Fractal Art and it is still ongoing. Based on this graphical representation, you can see the interesting features of the fractal, such as self-similarity or self-affinity, with more focus.

In this paper, a simple method is used to the coloring of iterated maps in Eqs. 2 and 3. In this method, the real part of Z is used for the red channel of the output image and for the green channel of image is used from the imaginary part of Z. The blue channel of the output image is also the multiplication of the real and imaginary part.

The results of the proposed coloring method for several monic fractals are shown in Fig. 1 after 100 iterations. Figure 1a shows the image obtained from Eq. 2, which is known as the Mandelbrot fractal. These fractals are merely graphical and represent a self-similarity feature in mono fractals.

Figure 2 show the results of proposed coloring scheme based on Eq. 3 with a variety of iteration number for different control parameters ($\alpha, \beta \in [0, 10]$, $Z_1, Z_2 \in [0 + 0 \times 1i\,,\ 1 + 1 \times 1i]$). There are pieces of the flat surfaces in Fig. 2, which indicate that the obtained value from $\alpha, \beta < 1$ is closed to the zero. In control parameters ($\alpha, \beta > 4$) after 100 iterations, the fractal image is a completely random image indicating that there is a randomness feature or a fully chaotic feature in this interval and this is the best feature for a pseudo-random number generator and It can be said that the proposed chaotic map can be used as a cryptographic system.

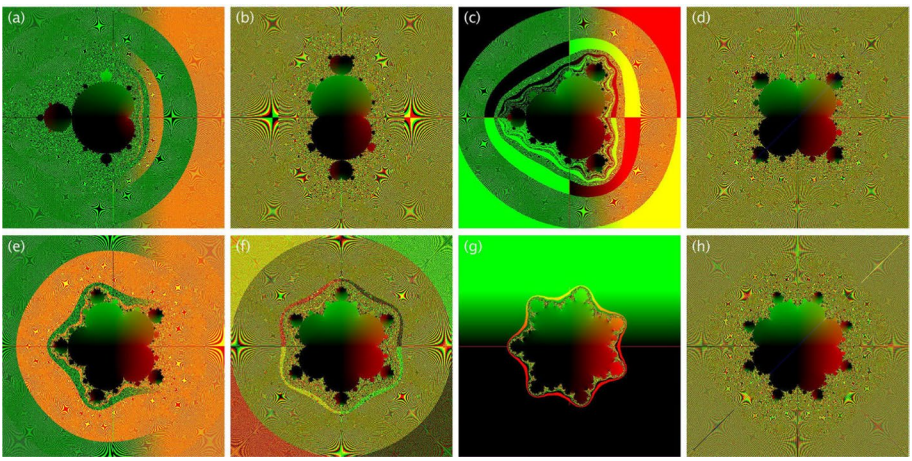

Fig. 1 The coloring scheme for several monic forms of polynomial fractals after 100 iteration , $z_0 = 0$, $c \in [-2 - 2 \times 1i, 2 + 2 \times 1i]$: **a** $z_{n+1} = z_n^2 + c$ **b** $z_{n+1} = z_n^3 + c$ **c** $z_{n+1} = z_n^4 + c$ **d** $z_{n+1} = z_n^5 + c$ **e** $z_{n+1} = z_n^6 + c$ **f** $z_{n+1} = z_n^7 + c$ **g** $z_{n+1} = z_n^8 + c$ **h** $z_{n+1} = z_n^9 + c$

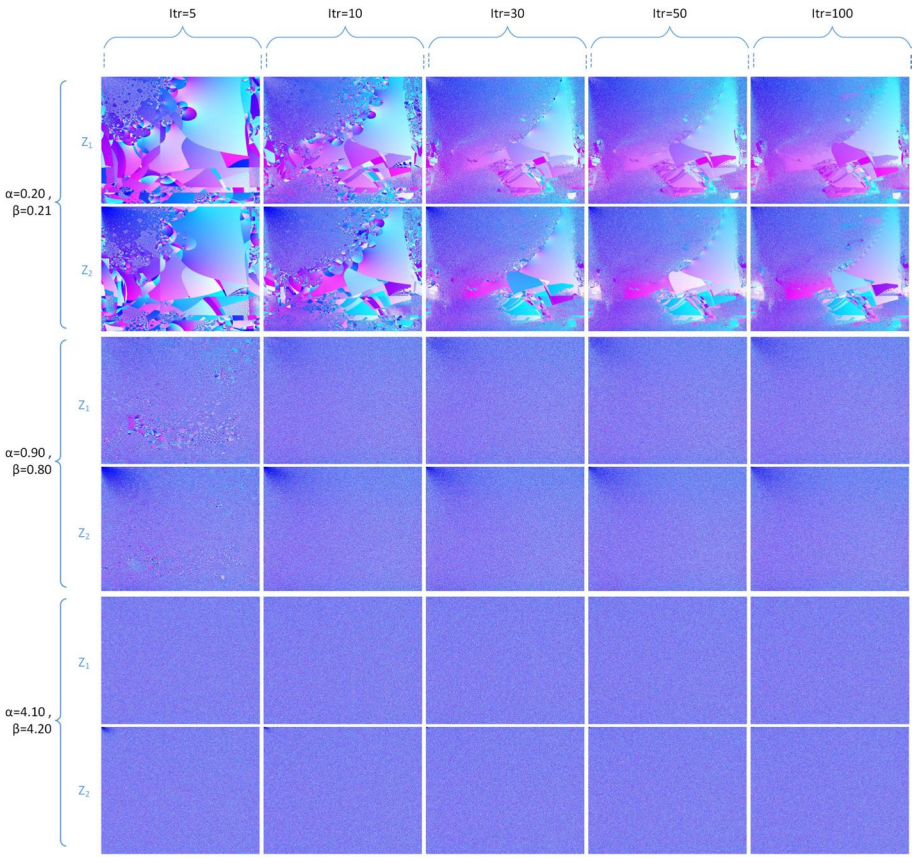

Fig. 2 The coloring scheme for proposed complex map with different iterations, $z_0 = 0.0001 + 0.0001 \times 1i$, $c \in [0 + 0 \times 1i, 1 + 1 \times 1i]$ and variety of values for control parameter α and β

3.2 Chaos trajectory, bifurcation diagram and histogram analysis

Chaos trajectory is used to investigate the dynamical behavior of a multidimensional system from an initial state over time. In fact, the trajectory shows the behavior of the system in the multidimensional phase space, which is also referred to as the phase curve. Systems with periodic behavior appear in a closed curve in the phase space, and systems with a chaotic behavior do not have closed curves or repetitive path. In the theory of dynamical systems, if multidimensional chaotic map occupies the phase space completely, then it has better random properties. In other words, a better randomness attribute will create more security in the encryption system.

Figure 3 shows the dynamical behavior of the 2D proposed map in phase space with 1,000,000 iterations. The 2D and 3D chaos trajectory is plotted based on the control parameters ($0 < \alpha, \beta < 10$). According to this figure, the existence of closed curves is probable and less occupation is observed in phase space ($\alpha, \beta < 0.5$). These figures are shown the trajectories based on the control parameters α and β in a variety of intervals, which intervals ($\alpha, \beta > 4$) has a better randomness characteristic than other intervals.

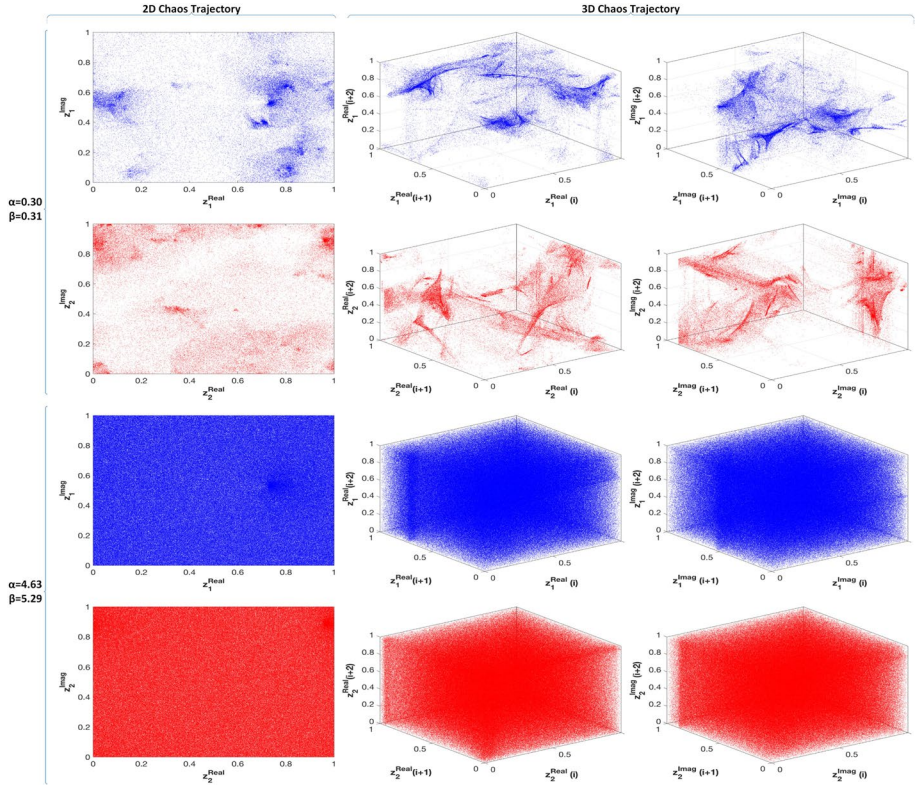

Fig. 3 The results of 2D chaos trajectory, histogram analysis, and 3D chaos trajectory, left to right, respectively based on real and imaginary parts of Z_1 and Z_2 for different values of control parameter α and β

In Fig. 4, in addition to the trajectory display, the histogram of the proposed complex map is shown in terms of the real and imaginary parts. If the histogram distribution of a *PRNG* has been uniform, its randomness is greater. Based on Fig. 4, the histogram of the proposed chaotic complex map for $(\alpha, \beta > 4)$ has approximately a uniform statistical distribution.

3.3 Bifurcation diagram

Henri Poincare used bifurcation analysis to show structural changes in the orbits of a dynamical system. Bifurcation is a measure to detect and depict the changes which occur when the parameter of a chaotic system is changed. Generally, fixpoint values can be deleted or created and also their stability could be changed. Evaluation and comparison of parameter values by the fix points of a dynamic system in a graphical form is known as a bifurcation diagram.

Figure 5 shows the bifurcation diagram of the proposed chaotic map. Figure 5a, b shows the relationship between real and imaginary Z_1 with α and Fig. 5c, d displays the relationship between $Z_2^{Real,Imag}$ and β. This figure shows that in entire interval $Z_1, Z_2 \in [0, 1]$ and $\alpha, \beta \in [2, 10]$ values are fully chaotic.

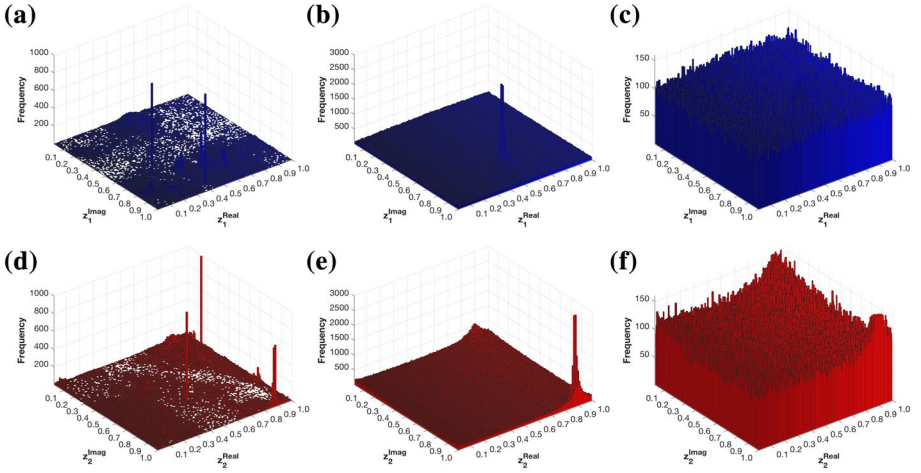

Fig. 4 The results of 3D histogram analysis based on real and imaginary parts of Z_1 and Z_2 for different values of control parameters: **a**, **d** $\alpha = 0.30$, $\beta = 0.31$, and **b**, **e** $\alpha = 0.75$, $\beta = 0.77$, and **c**, **f** $\alpha = 4.63$, $\beta = 5.29$

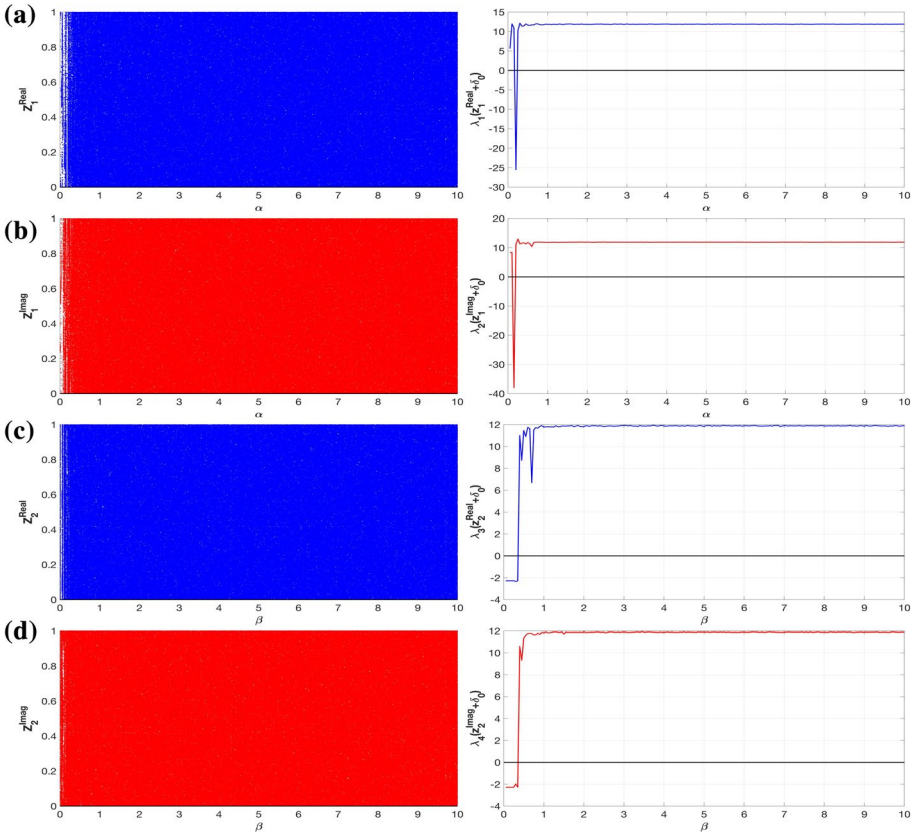

Fig. 5 Bifurcation and Lyapunov exponent, left to right, respectively for proposed chaotic complex map, **a** real part of Z_1, **b** imaginary part of Z_1, **c** real part of Z_2, **d** imaginary part of Z_1

3.4 Lyapunov exponent

The Lyapunov exponent, taken from the name of the Russian mathematician *A.M.Lyapunov*, shows the chaotic map sensitivity to the initial condition, which is represented by the λ parameter. Using Lyapunov exponent, we can show the convergence and divergence of two different circuits with different initial conditions. If λ is negative, then the paths close to each other will converge and the system won't have a chaotic state. However, if the λ is positive, the paths close to each other will diverge and the system will have a chaotic state and it will be sensitive to primary conditions. The several parameters for calculation of Lyapunov exponent are illustrated in the following equations:

$$\begin{aligned}
\lambda_1(Z_1^{real}+\delta_0) &= \frac{1}{10000}\Sigma_{n=1}^{10000} log\left(\left|\frac{f^n(Z_1^{real}+\delta_0)-f^n(Z_1^{real})}{\delta_0}\right|\right)\\
\lambda_2(Z_1^{imag}+\delta_0) &= \frac{1}{10000}\Sigma_{n=1}^{10000} log\left(\left|\frac{f^n(Z_1^{imag}+\delta_0)-f^n(Z_1^{imag})}{\delta_0}\right|\right)\\
\lambda_3(Z_2^{real}+\delta_0) &= \frac{1}{10000}\Sigma_{n=1}^{10000} log\left(\left|\frac{f^n(Z_2^{real}+\delta_0)-f^n(Z_2^{real})}{\delta_0}\right|\right)\\
\lambda_4(Z_2^{imag}+\delta_0) &= \frac{1}{10000}\Sigma_{n=1}^{10000} log\left(\left|\frac{f^n(Z_2^{imag}+\delta_0)-f^n(Z_2^{imag})}{\delta_0}\right|\right)
\end{aligned} \tag{5}$$

where Z_1^{real} , Z_1^{imag},Z_2^{real}, and Z_2^{imag} are the initial conditions of the proposed chaotic map and δ_0 is a very small value (10^{-14}).

The Lyapunov exponents of λ_1, λ_2, λ_3, and λ_4 are calculated and shown in Fig. 5 based on denoted parameters in Eq. 5. As shown in Fig. 5a–d, the proposed chaotic complex map is chaotic in $\alpha, \beta \in [1, \infty]$ $(\lambda_i > 0, i = 1, 2, 3, 4)$ and is periodic in $\alpha, \beta \in [0, 1](\lambda_i < 0)$.

3.5 Randomness test

In the computer security debate, criteria are required to examine the randomness feature of sequences generated by pseudo-random numbers generators (PRNGs). Use of statistical test suites is one of the methods for randomly checking of numbers. In this section, we introduce four commonly statistical tests for analyzing of randomness feature.

- *NIST* The NIST test is a statistical package with 15 tests developed by the National Institute of Standards and Technology (Rukhin et al. 2001). This test examines the various aspects of randomness over long strings and focuses on different states of non-randomness that may occur in sequences. The framework of this test, like other tests, is based on testing the hypotheses. To perform this test, the floating-point sequences were converted to 32-bit sequences. The results of the *NIST* test on the proposed 2D complex map is shown in Table 1.

  The NIST uses from a one-way statistical test and the 99% confidence interval. That is to say, the *pvalue* > 0.01 is successfully passed. Based on the results in Table 1, it can be seen that all the NIST tests have passed successfully.
- *Diehard* In 1995, George Marsaglia collected a set of 18 advanced tests in the *Diehard* test package, which shows how quantities are produced by pseudo-random numbers generators (Marsaglia 1998). The results of Diehard's test on the proposed 2D complex map is shown in Table 1. Unlike the NIST test, Diehard uses a two-way statistical test

Table 1 The results of randomness test suites on proposed PRNG

NIST : Test name	Z_{Real}			Z_{Imag}		
	P value	Proportion	Result	*P* value	Proportion	Result
Frequency Test	0.534938	100/100	Success	0.838077	100/100	Success
Block Frequency Test (m = 128)	0.246887	100/100	Success	0.876032	100/100	Success
Cumulative-Forward	0.851256	100/100	Success	0.605764	100/100	Success
Cumulative-Reverse	0.578499	100/100	Success	0.436805	100/100	Success
Run Test	0.827371	100/100	Success	0.70784	100/100	Success
Long Runs of Ones	0.223972	100/100	Success	0.848257	100/100	Success
Rank	0.27824	100/100	Success	0.617716	100/100	Success
Spectral DFT	0.778984	100/100	Success	0.453578	100/100	Success
Non-Overlapping-Min	0.579255	100/100	Success	0.451964	100/100	Success
Non-Overlapping-Max	0.579255	100/100	Success	0.451964	100/100	Success
Overlapping Temp. (m = 9)	0.303878	100/100	Success	0.829661	100/100	Success
Universal	0.77012	100/100	Success	0.578368	100/100	Success
Approximation Entropy (m = 10)	0.533902	100/100	Success	0.759071	100/100	Success
Random Excursions-Min	0.790371	100/100	Success	0.560561	100/100	Success
Random Excursions-Max	0.790371	100/100	Success	0.560561	100/100	Success
Random Excursions Variant-Min	0.020442	100/100	Success	0.693646	100/100	Success
Random Excursions Variant-Max	0.020442	100/100	Success	0.693646	100/100	Success
Serial (1)	0.028293	100/100	Success	0.929005	100/100	Success
Serial (2)	0.028293	100/100	Success	0.929005	100/100	Success
Linear Complexity (M = 500)	0.852094	100/100	Success	0.38483	100/100	Success

Diehard : Test Name	Z_{Real}		Z_{Imag}	
	P value	Result	*P* value	Result
Diehard Birthdays	0.02340644	Success	0.39965486	Success
Binary Rank 32 × 32	0.20890044	Success	0.42381923	Success

Table 1 (continued)

Diehard : Test Name	Z_{Real}		Z_{Imag}	
	P value	Result	*P* value	Result
Binary Rank 31×31	0.35474748	Success	0.63873637	Success
Binary Rank 6×8	0.82861985	Success	0.26149849	Success
Overlapping 5-Permutation	0.97590675	Success	0.944299	Success
Bitstream	0.6585842	Success	0.19812604	Success
Overlapping Pairs Sparse Occupancy	0.46584941	Success	0.60129876	Success
Overlapping Quadruples Sparse Occupancy	0.37409842			Success
DNA	0.78077457	Success	0.69231782	Success
Count The 1's Test a Stream of Bytes	0.13666287	Success	0.77441116	Success
Count The 1's Test a Specific of Bytes	0.3840272	Success	0.93934917	Success
Parking Lot	0.08478625	Success	0.77490362	Success
Minimum Distance	0.36045554	Success	0.40568184	Success
3D-Sphere	0.32447131	Success	0.99900354	Success
Squeeze	0.45135904	Success	0.74639153	Success
Sums	0.20912717	Success	0.41349664	Success
Runs	0.65484546	Success	0.18635408	Success
Craps	0.5842986	Success	0.79812833	Success

ENT : Test Name	Z_{Real}		Z_{Imag}	
	Value	Result	Value	Result
Entropy	7.999953	Success	7.999948	Success
Chi square	259.72	Success	285.81	Success
Arithmetic mean	127.4522	Success	127.4554	Success
Monte Carlo	3.142029142	Success	3.143349143	Success

Table 1 (continued)

ENT : Test Name	Z_{Real}		Z_{Imag}	
	Value	Result	Value	Result
Serial correlation coefficient	0.000346	Success	− 0.000323	Success
TestU01 : Battery	Parameters	Number of statistics	Results	
			Z_{Real}	Z_{Imag}
Small Crush	Standard	15	Pass	Pass
Crush	Standard	144	Pass	Pass
Big Crush	Standard	160	Pass	Pass

with a confidence interval of 99%. Therefore, $0.01 < pvalues < 0.99$ are successfully passed in this test. Based on the results in Table 1, it can be seen that the Diehard test is successfully passed.

- *ENT* This test was developed by John Walker in 1998 to test the randomness of the sequences (Walker 2008). The ENT program is used as a useful tool for evaluating pseudo-random number generators for cryptographic and statistical sampling applications, compression algorithms, and other applications where the information intensity of a given data is considered. The results of the *ENT* test on the proposed 2D complex map is shown in Table 1.

  In the ENT test, if the entropy value based on Shannon's theory is close to 8.00, it can be said to be completely random. In the Chi-square analysis, the value of Chi-square for the degree of freedom 255, and the confidence interval of 95% is $\chi^2(\alpha = 0.05, d = 255) = 293.24$, and the value obtained from the analysis, if lower than this value, is successfully passed the Chi-square test. In the arithmetic mean test, the random sequence are close to 127.50. In the Monte Carlo test, the pi is 3.1415926535897, and the obtained value with *errors* < 0.01 is acceptable. In the serial correlation test, if the value of the correlation is closer to zero, then it is more acceptable. Based on the results of the ENT test in Table 1, it can be concluded that the ENT test has also been successfully passed.
- *TestU01 TestU01* is a software library that is implemented in ANSI C. This test is a set of tools for the experimental statistical testing of the uniform random generators (L'Ecuyer and Simard 2007). This library presents several types of random number generators in general, which widely used in the literature of research. Three batteries of statistical tests are implemented by TESTU01: Big Crush (45 tests), Crush (60 tests) and Small Crush (10 tests). Table 1 shows the results of these tests.

4 Basic concepts

In the following subsections, details of some transform domains such as DWT, IWT, CT, and SVD are illustrated.

- *Discrete Wavelet Transform* In general, the basic idea of a discrete wavelet transform (*DWT*) is the multiresolution decomposition of signal and image. In a different type of images with various texture and structure, generally small image elements require a higher resolution, and the large elements of the image require a smaller resolution (Sundararajan 2016). In this transform, the main approach for image analysis is the use of low pass filter for large image components and high pass filter for small image components. The *DWT* is defined in the time and frequency domain, and is a tool for converting the time domain signal to the signal in the time/frequency domain and vice versa. This transform usually illustrated by (1) Matrix formulation, (2) Utilize low pass and high pass filters and (3) Polyphase matrix factorization (Lee 2014).
- *Integer Wavelet Transform* The integer wavelet transform (*IWT*) is actually a multiresolution theory based on a much simpler computation than its discrete version. This transform is an optimized version of the discrete wavelet transform, which can use the integer operation for transforms and avoid the problems caused by rounding the values (Chamlawi and Khan 2010). The *IWT* generally has four main parts includes: (1) Splitting, (2) Prediction, (3) Update and (4) Scaling.

- *Contourlet Transform* Due to limits of transforms such as Fourier transform and wavelet transform to fully understand the geometry of the edges of the image as well as display the inherent features of image geometry, the contourlet transform was proposed by Do and Vetterli (2005). In a geometric analysis of images, the main problem is because the data is discrete in visual information. Unlike other transforms, contourlet transform starts his work for decomposing the image from a discrete domain and then converge the resulting structure to a continuous domain (Wang et al. 2013). In contourlet transform, a multi-resolution and multi-directional expansion is done using filter banks.
- *Singular Value Decomposition* In linear algebra, the singular value decomposition (SVD) of A matrix is the decomposition of the matrix into the product of the three matrix elements in the form of $A = U\Sigma V^T$ .In SVD, the columns of the U and V matrixes are orthogonal, and the Σ diagonal matrix in this decomposition has positive integers. The A is $m \times n$ matrix and in this decomposition, the U is a $m \times m$ matrix which columns are eigenvalues of AA^T and V is a $n \times n$ diagonal matrix which columns are eigenvalues of A^TA (Klema and Laub 1980).

5 Proposed method

This section presents the proposed method for blind video watermarking. The block diagram of the embedding and extraction process is shown in Fig. 6. In the following subsections, the embedding and extraction process will be described separately.

5.1 Embedding process

Initially, the desired video is received from the input and is categorized by existing frames. Each frame is like a color image with three channels of red, blue and green. Other inputs

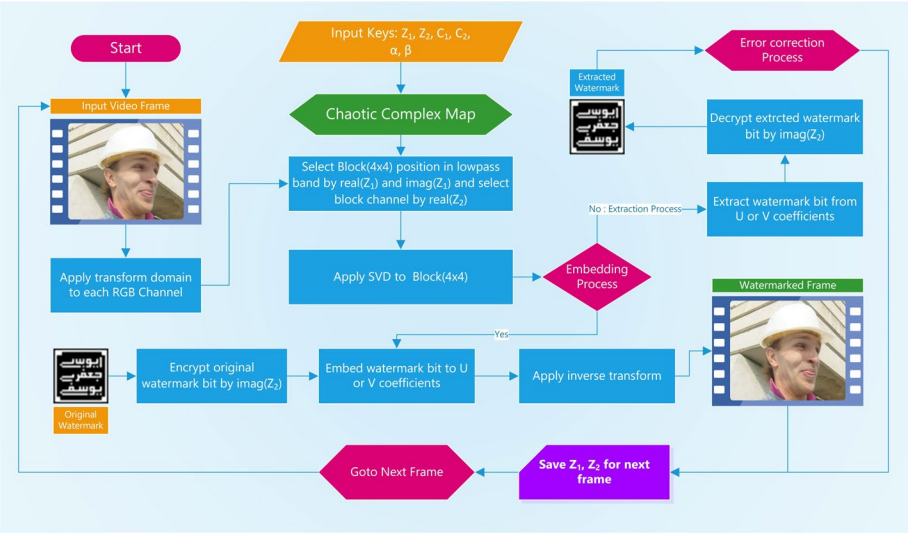

Fig. 6 Block diagram of proposed method for embedding and extracting process

to the system are chaotic map keys, which include Z_1,Z_2 ,C_1, C_2, α, and β, which will be used to locate the watermark as well as to encrypt the watermark logo. Proposed transforms apply to each color channel and the low-pass band of the transformed coefficients, which has the highest image energy, is selected for the embedding process. This band is divided into 4×4 blocks and each block selects randomly by the real and imaginary parts of Z_1. The real part of Z_2 is used to determine the channel of the selected block. To enhance watermarking security, the watermark bit as another input parameter is encrypted using the imaginary part of Z_2.

Now it's time to embed the watermark bit on the selected block. By using singular value decomposition, the selected block of coefficients is decomposed into three matrices U, S, and V. The best matrix for the insertion process is U or V, which has the least visual effect on the insertion block. Of course, the pseudo-code of the embedding and extraction process is presented based on the U matrix, which can be changed as well to the V matrix. After inserting a watermark bit, the inverse singular value decomposition is applied to the selected block, and this modified block is placed in its original location in the low-pass band. Then, using the chaotic iterated map in Eq.(3), another block is selected for the embedding process. In this algorithm, a 32×32 watermark is inserted for each frame of the video. After completing the insertion of a 32×32 watermark, the inverse transform is applied in the modified coefficients to obtain the watermarked frame. The last values of the Z_1 and Z_2 variables are stored to be used as system inputs in the next frame. Full details of the embedding process are shown with the mathematical relationships contained as pseudo-code in Algorithm 1.

5.2 Extraction process

The extraction process is very similar to the embedding process. In this algorithm, the transforms are applied independently, and after selecting the 4×4 blocks using the proposed chaos complex map, a singular value decomposition is applied. The only difference between extraction process and embedding process is in how to extract U or V coefficients in *SVD*. In this algorithm, there is no need to inverse singular value decomposition and inverse transforms. Finally, Z_1 and Z_2 values are stored for use in the next frame as initial conditions. The full details of the extraction part are displayed as pseudo-code in Algorithm 1.

Algorithm 1: Embedding and Extraction function in the proposed method.

Function *[WI/EW]= Embedding_ Extraction(I, W, α, β, Z_1, Z_2, Type)*
  // I: Input Frame, W: Original Watermark Logo, EW: Extracted Watermark Logo
  // Initial Condition: $Real(Z_1) \in [0,1]$, $Real(Z_2) \in [0,1]$, $Imag(Z_1) \in [0,1]$, $Imag(Z_2) \in [0,1]$.
  // Control parameters: $\alpha \in [4,10]$, $\beta \in [4,10]$
  // Type: (0 : Embedding Process , 1 : Extraction Process), rw,cw : Size of watermark Logo.
  $LLband = TransformDomain(I(Red, Green, Blue))$;
  $Mask = Zeros(\frac{rc}{4}, \frac{cc}{4}, 3)$;
  $[rw, cw] = GetSize(W)$;
  $[rc, cc] = GetSize(LLBand)$ **for** $i = 1$ **to** rw **do**
    for $j = 1$ **to** cw **do**
      while *1* **do**
        $Z_1 \equiv [\alpha(\frac{Z_1}{Z_2})^2 + c_1]\ CFOLD\ 1$;
        $Z_2 \equiv [\beta(\frac{Z_2}{Z_1})^2 + c_2]\ CFOLD\ 1$;
        $x = \lfloor Real(Z_1) \times 10^{14} \rfloor\ Mod\ \frac{rc}{4}$;
        $y = \lfloor Imag(Z_1) \times 10^{14} \rfloor\ Mod\ \frac{cc}{4}$;
        $Channel = \lfloor Real(Z_2) \times 10^{14} \rfloor\ Mod\ 3$; // 0 : Red Channel, 1 : Green Channel and 2 : Blue Channel
        $B = \lfloor Imag(Z_2) \times 10^{14} \rfloor\ Mod\ 2$;
        if $Mask([x+1][y+1][Channel]) == 0$ **then**
          break while ;
        end
      end
      $Block = LLband[x \times 4 + 1\ to\ x \times 4 + 4][y \times 4 + 1\ to\ y4 \times 4 + 4][Channel]$;
      $[U, S, V] = SVD(Block)$;
      if $Type == 0$ **then**
        $meanV = (|u[1][1]| + |u[2][1]|)/2$;
        if $W[i][j] == 0$ **then**
          if $|u[1][1]| > |u[2][1]|$ && $|u[2][1]| - |u[1][1]| < (T)$ **then**
            $u[1][1] = Sign(u[1][1]) \times (meanV + \frac{T}{2})$;
            $u[2][1] = Sign(u[2][1]) \times (meanV - \frac{T}{2})$;
          end
        end
        $W[i][j] = W[i][j] \oplus B$; // Encryption Process
        if $W[i][j] == 1$ **then**
          if $|u[2][1]| > |u[1][1]|$ && $|u[2][1]| - |u[1][1]| > (T)$ **then**
            $u[1][1] = Sign(u[1][1]) \times (meanV - \frac{T}{2})$;
            $u[2][1] = Sign(u[2][1]) \times (meanV + \frac{T}{2})$;
          end
        end
        $LLband[x \times 4 + 1\ to\ x \times 4 + 4][y \times 4 + 1\ to\ y \times 4 + 4][Channel] = u \times s \times v^T$;
      end
      if $Type == 1$ **then**
        if $|u[1][1]| > |u[2][1]|$ **then**
          $EW(i,j) = 0$;
        else
          $EW(i,j) = 1$;
        end
        $EW[i][j] = EW[i][j] \oplus B$; // Decryption Process
      end
      $Mask[x+1, y+1][Channel] = 1$;
    end
  end
  Save final Z_1, Z_2 for initial conditions of next frame ;
  if $Type == 0$ **then**
    WI=InverseTransformDomain(LLBand(Red, Green, Blue)) ;
    return Watermarked Image WI;
  else
    return Extracted Watermark EW;
  end
end

6 Experimental results

In this paper, standard CIF (352×288) videos (Video test media 2017) have been used to evaluate the performance of the proposed method (See Fig. 7). The characteristic of cover videos in the Xiph dataset is presented in Table 2. A logo with 32×32 pixels is used as a watermark binary logo. The simulation is performed on the MATLAB R2017a software on a PC with a MAC platform and an i5-3.2 GHz processor with 8 GB of RAM. The simulation software designed with MATLAB is shown in Fig. 8. The calculated results are done with $T = 0.025$. In the rest of this section, the qualitative and quantitative analysis includes histogram analysis, the measures for visual quality, resistance to attacks and

Fig. 7 Standard CIF video samples (Video test media 2017) **a** Akiyo, **b** Bowing, **c** Bus, **d** City, **e** Coast-guard, **f** Container, **g** Crew, **h** Flower, **i** Football, **j** Foreman, **k** Hall monitor, **l** Harbor, **m** Mother daughter, **n** News, **o** Sign irene, **p** Silent, **q** Soccer, **r** Waterfall

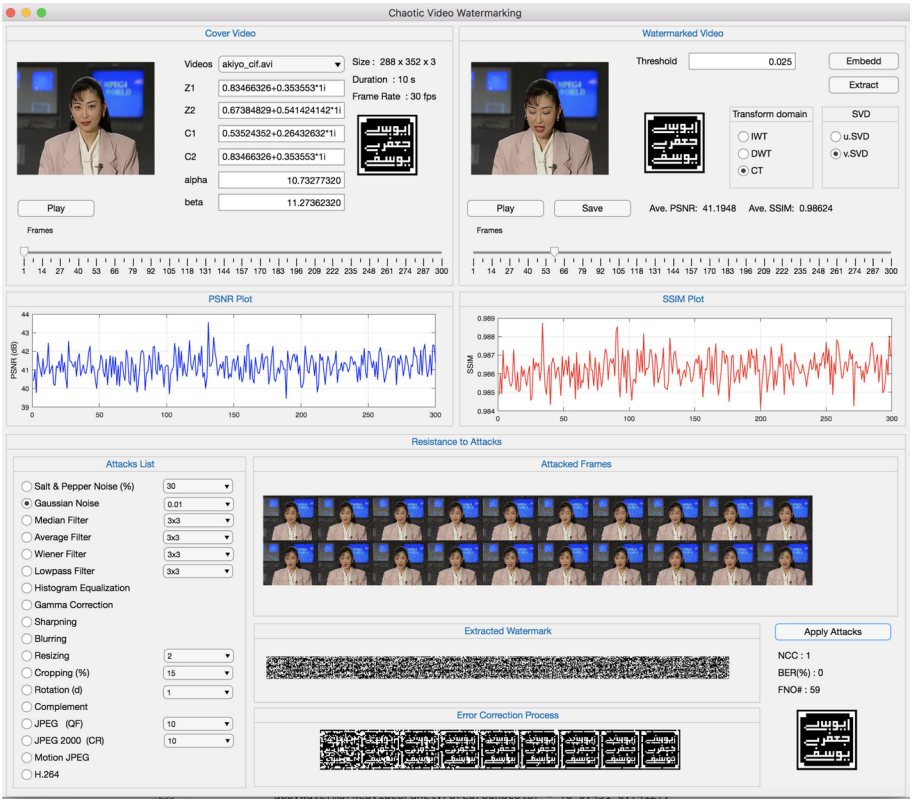

Fig. 8 Designed and implemented Matlab GUI for proposed video watermarking

security analysis will be discussed. Finally, the results of the proposed method will be compared with other similar methods.

6.1 u.SVD versus v.SVD

Before presenting the results of simulations and analyses, it is necessary to mention an important index in the process of insertion and extraction. In this paper, in addition to using different transform domain in the proposed method, two methods based on single value decomposition have been investigated. Based on the block diagram and pseudo-code provided, the watermark bit can be embedded in the U decomposed matrix, as well as in the V decomposed matrix. For this reason, the method that is included in the U matrix is called *u.SVD*, and is also called the *v.SVD* in the method that V matrix is used. In the following section, we examine the performance of methods *u.SVD* and *v.SVD* in combination with various methods of transform domains such as IWT, DWT, and CT.

6.2 Key space analysis

High sensitivity to initial conditions is an inherent characteristic of chaotic systems. In fact, the key is an important part of the proposed algorithms and has a direct impact on their security. In order to provide a high-security cryptosystem, the keyspace should be large enough to make the key search attacks ineffective. If the attacker has enough knowledge about the watermarking procedure but is not aware of the relevant key in the chaotic sequences, he will do his best to destroy the watermark and access the original media. For this reason, the key must be chosen in such a way that it is hard to guess and achieve. Table 3 lists the number of input variables and how to calculate the keyspace of the proposed chaotic complex map. Therefore, it can be said that the keyspace of the proposed method (460 bits) is large enough to resist attacks such as brute-force attacks.

6.3 Histogram analysis

Histogram plot is a graphical tool that can analyze the distribution of watermarked frames in each video and also can show the frame destruction after the embedding process. Figure 9 demonstrates the histogram of original Foreman frames (first 10 frames) and watermarked frame histograms. This figure clearly shows that the histograms of original and watermarked frames are similar and the proposed method destroys the bits of frames as low as possible. Also, in Fig. 9, the locations selected by the proposed chaotic complex map are shown in the transform domain for the RGB channels. In Fig. 9c, we can clearly see the results obtained from the watermark extraction with an incorrect key.

6.4 Visual quality analysis

Visual quality analysis is very important in video watermarking systems. The two most important criteria for visual quality analysis are PSNR and SSIM, which we will discuss in more detail later. Peak signal to noise ratio (*PSNR*) is used to calculate the ratio between the maximum possible power of a signal and the power of corrupting noise. *PSNR* is defined by the mean squared error (*MSE*) between the original and the watermarked frame. *PSNR* is defined by the following equation:

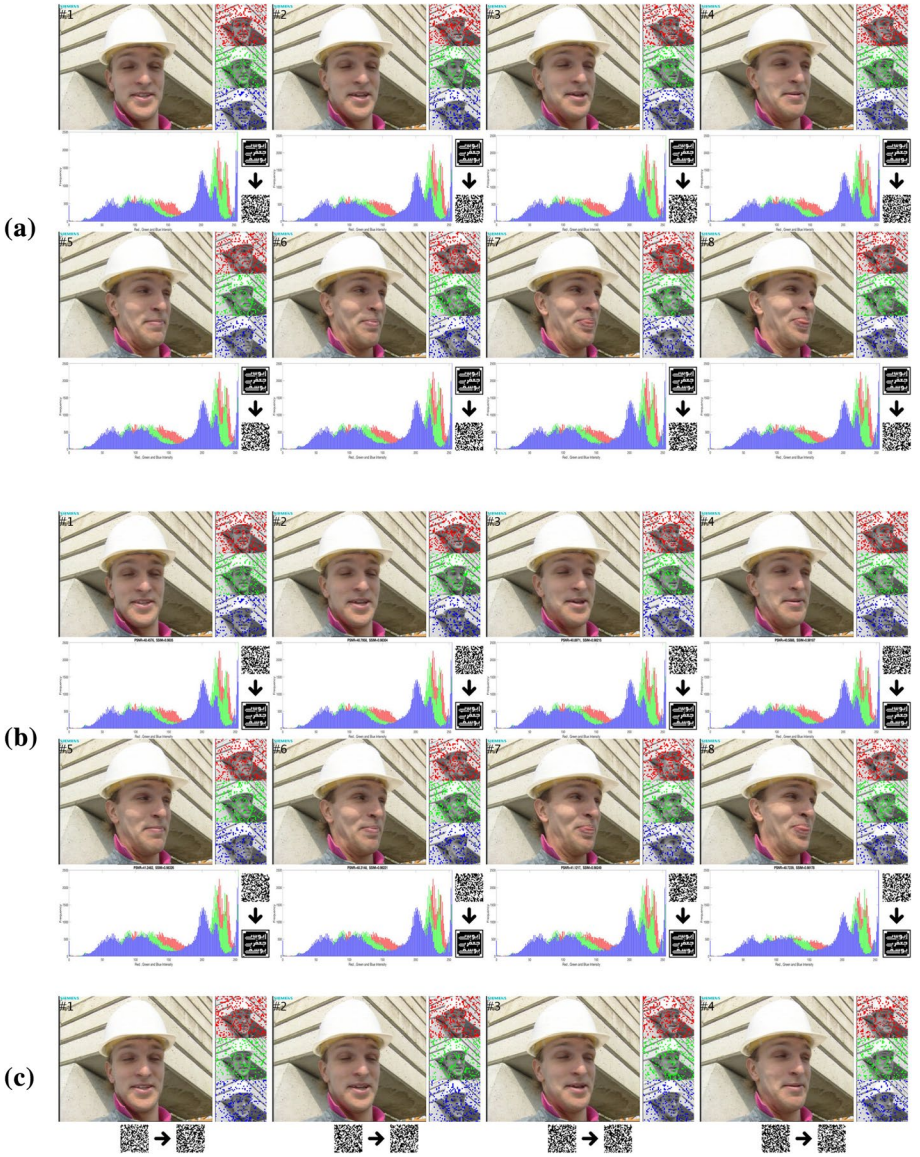

Fig. 9 Histogram analysis **a** original frame, LL band selected blocks by chaotic keys for R, G, and B channels, histogram analysis of original frame, original watermark and encrypted watermark for *Frame*#1 $\sim$ *Frame*#8 in Foreman video, **b** watermarked frame, LL band selected blocks by chaotic keys for R, G, and B channels, histogram analysis of watermarked frame, extracted encrypted watermark and final decrypted watermark for *Frame*#1 $\sim$ *Frame*#8 in Foreman video, **c** results of extraction process for incorrect input keys

Table 2 The characteristics of the cover videos in the Xiph dataset (Video test media 2017)

id	Name	Aspect Ratio	Format	#Frames	Resolution	Chroma format
V_1	Akiyo	4:3	CIF	300	352×288	4:2:2
V_2	Bowing	4:3	CIF	300	352×288	4:2:2
V_3	Bus	4:3	CIF	150	352×288	4:2:2
V_4	City	4:3	CIF	300	352×288	4:2:2
V_5	Coastguard	4:3	CIF	300	352×288	4:2:0
V_6	Container	4:3	CIF	300	352×288	4:2:0
V_7	Crew	4:3	CIF	300	352×288	4:2:2
V_8	Flower	4:3	CIF	250	352×288	4:2:2
V_9	Football	4:3	CIF	260	352×288	4:2:2
V_{10}	Foreman	4:3	CIF	300	352×288	4:2:0
V_{11}	Hall monitor	4:3	CIF	300	352×288	4:2:0
V_{12}	Harbour	4:3	CIF	300	352×288	4:2:2
V_{13}	Mother daughter	4:3	CIF	300	352×288	4:2:0
V_{14}	News	4:3	CIF	300	352×288	4:2:2
V_{15}	Sign irene	4:3	CIF	540	352×288	4:2:2
V_{16}	Silent	4:3	CIF	300	352×288	4:2:2
V_{17}	Soccer	4:3	CIF	300	352×288	4:2:2
V_{18}	Waterfall	4:3	CIF	260	352×288	4:2:2

Table 3 The key space of proposed 2-D chaotic complex map

Parameters	Best range	Precision (float)	Precision (binary bit)
Z_1^{real}	[0,1]	10^{-14}	46
Z_1^{imag}	[0,1]	10^{-14}	46
Z_2^{real}	[0,1]	10^{-14}	46
Z_2^{imag}	[0,1]	10^{-14}	46
C_1^{real}	[0,1]	10^{-14}	46
C_1^{imag}	[0,1]	10^{-14}	46
C_2^{real}	[0,1]	10^{-14}	46
C_2^{imag}	[0,1]	10^{-14}	46
α	[4,10]	10^{-14}	46
β	[4,10]	10^{-14}	46
Key space			$10 \times 46 = 460$ bit

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right) \tag{6}$$

and MSE is defined as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[OF(i,j) - WF(i,j)]^2 \tag{7}$$

where $OF(i, j)$ is the original video frame and $WF(i, j)$ is the watermarked frame. M and N are the size of original and watermarked frame. Structural similarity (*SSIM*) is used to show the similarity of original video frames and watermarked video frames. *SSIM* calculated by:

$$SSIM(O, W) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{8}$$

where the mean intensity of x and y are μ_x and μ_y. $\sigma_x^2 and\ \sigma_y^2$ are variance of x and y, the co-variance of x and y is σ_{xy}, respectively. Also, C_1 and C_2 are the variables for stabilizing.

The *PSNR* and *SSIM* are calculated for each frame independently, and finally, for all video frames, the average of these two criteria is calculated. Tables 4 and 5 show the results for the *PSNR* and SSIM criteria in a combination of different transform domains. In watermarking systems, the most ideal value is for $PSNR > 40$, and in the *SSIM* criterion, this value should be close to *1.00* for maximum performance. The FNO# variable in this table represents the maximum number of frames needed to extract a watermark without error.

6.5 Resistance to attacks

In watermarking systems, attackers try to destroy the embedded watermark by image processing attacks in the video due to the lack of a secret key and insertion location.For this reason, a robust watermarking system must be able to resistance to these attacks. These attacks are divided into geometric and non-geometric attacks. A number of these attacks, in Fig. 10, are applied to a frame of Foreman's video. In this article, attempts have been made to exploit attacks in popular benchmarks such as *Stirmark* (Stirmark 1997), *Checkmark* (Pereira et al. 2001), and popular public attacks on common articles (Asikuzzaman and Pickering 2018). These attacks include manipulations in the image processing field (such as adding noise, filters, re-sizing, rotation, changing in brightness, etc.), image and video compression (such as jpeg, jpeg2000, motion jpeg, H.264, etc.) and also a series of video specific attacks (such as frames averaging, frame dropping, moving frames, embedding new frames, etc).

Two criteria, NC and BER, are used to measure the algorithm's resistance to a variety of attacks. In fact, these metrics used to measuring of extracted watermark error. Normal correlation (NC) is used to show the similarity of watermark logo before and after applying attacks on video frames. This measure is calculated by:

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

where W is the original watermark and W' is the extracted watermark image. M and N are the size of original watermark logo.

BER is used to measure the robustness of proposed method against different attacks. *BER* is defined as:

$$BER(W, W') = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j) \oplus W'(i,j)}{M \times N} \times 100 \tag{10}$$

Table 4 The PSNR, SSIM results in proposed method based on IWT(u.SVD,v.SVD) and DWT(u.SVD,v.SVD)

Videos name	Frames#	IWT							
		u.SVD			v.SVD			NC	BER
		PSNR	SSIM	FNo#	PSNR	SSIM	FNo#		
Akiyo	300	43.78	0.9908	3	42.38	0.9901	3	1.0000	0.00
Bowing	300	43.90	0.9869	5	44.07	0.9866	5	1.0000	0.00
Bus	150	36.25	0.9917	3	38.21	0.9937	3	1.0000	0.00
City	300	42.00	0.9925	2	41.57	0.9907	2	1.0000	0.00
Coastguard	300	36.77	0.9863	3	41.47	0.9937	2	1.0000	0.00
Container	300	36.77	0.9833	3	39.44	0.9869	3	1.0000	0.00
Crew	300	45.04	0.9924	2	42.60	0.9904	2	1.0000	0.00
Flower	250	37.48	0.9867	3	38.70	0.9865	3	1.0000	0.00
Football	260	41.38	0.9900	3	41.35	0.9924	5	1.0000	0.00
Foreman	300	40.82	0.9845	2	38.39	0.9837	2	1.0000	0.00
Hall monitor	300	38.33	0.9853	3	39.43	0.9863	5	1.0000	0.00
Harbour	300	39.93	0.9931	3	34.43	0.9857	2	1.0000	0.00
Mother daughter	300	41.19	0.9869	4	45.12	0.9889	7	1.0000	0.00
News	300	42.74	0.9934	3	37.55	0.9920	3	1.0000	0.00
Sign irene	540	43.21	0.9929	5	43.13	0.9932	5	1.0000	0.00
Silent	300	41.63	0.9887	3	43.04	0.9896	2	1.0000	0.00
Soccer	300	41.54	0.9872	3	42.51	0.9899	3	1.0000	0.00
Waterfall	260	42.17	0.9934	3	42.23	0.9938	3	1.0000	0.00
Mean	–	40.83	0.9892	3.111	40.8670	0.9897	3.33	1.0000	0.00
Videos Name	Frames#	DWT							
		u.SVD			v.SVD			NC	BER
		PSNR	SSIM	FNo#	PSNR	SSIM	FNo#		
Akiyo	300	43.90	0.9913	3	42.47	0.9906	3	1.0000	0.00
Bowing	300	43.98	0.9871	5	44.18	0.9869	5	1.0000	0.00
Bus	150	36.26	0.9918	3	38.24	0.9939	3	1.0000	0.00
City	300	42.06	0.9927	2	41.63	0.9909	2	1.0000	0.00
Coastguard	300	36.79	0.9864	3	41.52	0.9938	2	1.0000	0.00
Container	300	36.81	0.9837	3	39.48	0.9872	3	1.0000	0.00
Crew	300	45.17	0.9926	2	42.69	0.9907	2	1.0000	0.00
Flower	250	37.57	0.9883	3	38.82	0.9882	3	1.0000	0.00
Football	260	41.44	0.9902	3	41.40	0.9926	5	1.0000	0.00
Foreman	300	40.89	0.9848	2	38.43	0.9840	2	1.0000	0.00
Hall monitor	300	38.39	0.9857	3	39.48	0.9867	3	1.0000	0.00
Harbour	300	39.97	0.9932	3	34.45	0.9857	2	1.0000	0.00
Mother daughter	300	41.26	0.9871	4	45.25	0.9892	7	1.0000	0.00
News	300	42.82	0.9937	3	37.56	0.9923	3	1.0000	0.00
Sign irene	540	43.29	0.9932	5	43.22	0.9935	5	1.0000	0.00
Silent	300	41.71	0.9889	3	43.14	0.9899	2	1.0000	0.00
Soccer	300	41.60	0.9874	3	42.59	0.9901	2	1.0000	0.00

Table 4 (continued)

Videos Name	Frames#	DWT							
		u.SVD			v.SVD			NC	BER
		PSNR	SSIM	FNo#	PSNR	SSIM	FNo#		
Waterfall	260	42.23	0.9935	2	42.22	0.9938	3	1.0000	0.00
Mean	–	40.90	0.9895	3.056	40.9309	0.9900	3.22	1.0000	0.00

Table 5 The PSNR, SSIM results in proposed method based on CT+u.SVD

Videos name	Frames#	CT							
		u.SVD			v.SVD			NC	BER
		PSNR	SSIM	FNo#	PSNR	SSIM	FNo#		
Akiyo	300	42.33	0.9872	3	41.16	0.9862	3	1.0000	0.00
Bowing	300	42.83	0.9835	7	43.03	0.9833	3	1.0000	0.00
Bus	150	35.19	0.9871	3	43.03	0.9833	3	1.0000	0.00
City	300	40.93	0.9899	2	40.72	0.9883	2	1.0000	0.00
Coastguard	300	40.79	0.9827	3	40.72	0.9913	2	1.0000	0.00
Container	300	35.84	0.9763	3	38.56	0.9819	3	1.0000	0.00
Crew	300	43.91	0.9898	2	41.50	0.9867	2	1.0000	0.00
Flower	250	38.83	0.9857	5	37.03	0.9834	3	1.0000	0.00
Football	260	39.71	0.9850	3	39.44	0.9881	3	1.0000	0.00
Foreman	300	41.64	0.9783	3	39.73	0.9805	2	1.0000	0.00
Hall monitor	300	36.21	0.9780	3	39.00	0.9824	3	1.0000	0.00
Harbour	300	38.87	0.9910	2	33.44	0.9811	2	1.0000	0.00
Mother daughter	300	41.80	0.9836	3	44.28	0.9862	4	1.0000	0.00
News	300	41.38	0.9898	3	36.39	0.9883	3	1.0000	0.00
Sign irene	540	41.89	0.9902	3	41.78	0.9905	3	1.0000	0.00
Silent	300	37.52	0.9799	3	41.30	0.9860	2	1.0000	0.00
Soccer	300	40.58	0.9833	2	41.53	0.9871	3	1.0000	0.00
Waterfall	260	40.46	0.9898	3	41.12	0.9915	3	1.0000	0.00
Mean	f–	40.04	0.9851	3.111	39.8807	0.9863	2.722	1.0000	0.00

where W is the original watermark and W' is the extracted watermark image. M and N are the size of original watermark image.

The results of these attacks with *NC*, *BER* and *FNo#* parameters for the DWT, IWD, and CT transforms in combination of u.SVD and v.SVD are shown in Tables 6 and 7, respectively. Ranking techniques based on the best values of BER, NC and FNo# are used to rank the algorithms, respectively. Average ranks are shown at the end of this table. Figure 11 demonstrates the extracted watermark form attacked videos.

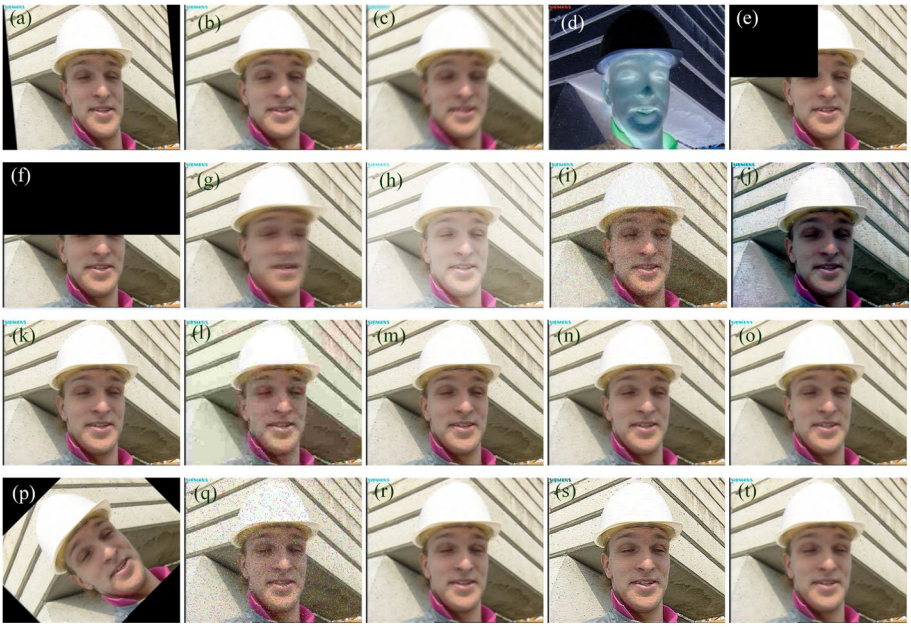

Fig. 10 Various attacks on foreman test video: **a** Affine transform, **b** average filter [3 × 3], **c** blurring (len = 10, $\theta = 45$), **d** complement, **e** cropping (25%), **f** cropping (50%), **g** frame averaging, **h** gamma correction ($\gamma = 0.5$), **i** Gaussian noise ($\sigma^2 = 0.01$), **j** histogram equalization, **k** Jpeg 2000 (Ratio = 10), **l** Jpeg compression (QF = 10), **m** Jpeg compression (QF = 75), **n** lowpass filter [3 × 3], **o** median filter [3 × 3], **p** rotation 45^o, **q** scaling 0.5, **r** sharpening, **s** Weiner filter [3 × 3], **t** salt & pepper (5%)

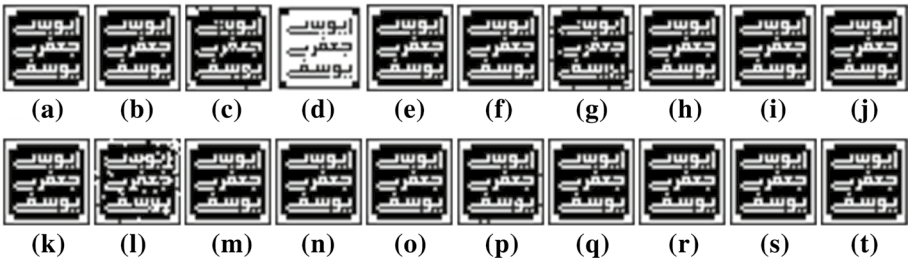

Fig. 11 Extracted watermark after confronting the attacks: **a** affine transform, **b** average filter [3 × 3], **c** blurring (len = 10, $\theta = 45$), **d** complement, **e** cropping (25%), **f** cropping (50%), **g** frame averaging, **h** gamma correction ($\gamma = 0.5$), **i** Gaussian noise ($\sigma^2 = 0.01$), **j** histogram equalization, **k** Jpeg 2000 (Ratio = 10), **l** Jpeg compression (QF = 10), **m** Jpeg compression (QF = 75), **n** lowpass filter [3 × 3], **o** median filter [3 × 3], **p** rotation 45°, **q** scaling 0.5, **r** sharpening, **s** Weiner filter [3 × 3], **t** salt & pepper (5%)

6.6 Impact of the error correction process against attacks

As stated in the extraction process, the proposed algorithm uses an error correction process. In fact, the embedding process, for each frame, embeds a watermark logo that the embedding location of the embedded watermark in each frame different from the

previous frames. This insertion redundancy helps the extraction process to easily detect and correct the errors with a ratio of $BER > 25\%$. Figure 12a shows the cropping attack at a rate of 25% for the first 15 frames of Foreman's video. Watermarks extracted for each frame from this video are shown in Fig. 12b. Finally, in Fig. 12c, we can clearly see the effect of the error correction, which after 15 frames, the bit error rate of the extracted watermark has reached zero.

6.7 Proposed automatic correction for rotation attacks

One of the major disadvantages of video watermarking methods in the chaotic domain is the lack of resistance to geometric attacks. The problem is very simple, the locations selected by the chaotic maps for embedding and extraction processes are changed by geometric attacks and the extraction process cannot be accessed to the original location. For this reason, in this paper, the most important geometric attack, the rotation attack, is investigated.

In watermarking algorithms, binary logos are similar to images, trademarks, etc. Hence, logos do not have a random structure and adjacent pixels have a statistical correlation. Therefore, in the proposed method after the watermark extraction, if the calculated correlation between adjacent pixels is less than threshold V, the rotational attack is detected and from 1 to 360 angles corrections are performed on the frame. For each correction angle, the correlation is calculated, and if its value exceeds the V threshold, the extraction of the watermark is correct and the correction process stops. Figure 13 shows the flowchart of the rotation attack correction and Fig. 14 illustrates some examples of correction results and calculates the correlation on the extracted logo.

6.8 Ranking of proposed methods

In this paper, a combination of three transforms domain and the *SVD* with two state yields a total of six different combinations. In this section, we are going to examine the six combinations mentioned above based on visual quality analysis and analysis of resistance to attacks. For this reason, the mean results of Tables 4, 5, 6, and 7 are summarized in Table 8. The *PSNR* criterion was used to analyze the visual quality and the proposed combination methods were sorted by the value of the *PSNR*. As can be seen in Table 8, the visual quality analysis in DWT + v.SVD performed better than other methods. Also, the analysis of resistance to attacks is arranged based on the *NC* criteria. Based on the results of these results, the combination of DWT + v.SVD of the other combinations performed better against the attacks.

6.9 Complexity analysis

In computer science, the performance of an algorithm is measured by the time complexity and space complexity. The proposed algorithm in this paper has a good space performance because of the linearity of the data computation. But in terms of time complexity, simulating the proposed algorithm on a PC with *core-i5* CPU takes a watermark insertion time of 0.0520, 0.0531, and 0.0834 seconds in IWT, DWT, and CT, respectively for each

Table 6 NC and BER(%) values of proposed algorithm against various attacks based on u.SVD for foreman video

Attacks	IWT+u.SVD				DWT+u.SVD				CT + u.SVD			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
No attack	1.0000	0.00	2	1	1.0000	0.00	2	1	1.0000	0.00	3	2
Salt & Pepper (0.1%)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Salt & Pepper (1%)	1.0000	0.00	7	1	1.0000	0.00	13	3	1.0000	0.00	8	2
Salt & Pepper (5%)	1.0000	0.00	23	2	1.0000	0.00	31	3	1.0000	0.00	19	1
Salt & Pepper (10%)	1.0000	0.00	68	2	1.0000	0.00	94	3	1.0000	0.00	43	1
Salt & Pepper (30%)	1.0000	0.00	277	3	1.0000	0.00	217	2	1.0000	0.00	211	1
Gaussian Noise ($\sigma^2 = 0.001$)	1.0000	0.00	5	1	1.0000	0.00	5	1	1.0000	0.00	5	1
Gaussian Noise ($\sigma^2 = 0.01$)	1.0000	0.00	15	1	1.0000	0.00	17	2	1.0000	0.00	21	3
Jpeg Compression (QF = 10)	0.7402	12.99	300	3	0.6855	15.72	300	2	0.8223	8.89	300	1
Jpeg Compression (QF = 50)	1.0000	0.00	64	1	1.0000	0.00	66	2	1.0000	0.00	64	1
Jpeg Compression (QF = 75)	1.0000	0.00	58	2	1.0000	0.00	56	1	1.0000	0.00	58	2
Jpeg Compression (QF = 90)	1.0000	0.00	32	1	1.0000	0.00	32	1	1.0000	0.00	54	2
Jpeg 2000 (Ratio = 10)	1.0000	0.00	5	2	1.0000	0.00	3	1	1.0000	0.00	3	1
Jpeg 2000 (Ratio = 20)	1.0000	0.00	50	3	1.0000	0.00	48	2	1.0000	0.00	13	1
Median Filter [3 × 3]	1.0000	0.00	11	1	1.0000	0.00	12	2	1.0000	0.00	11	1
Median Filter [5 × 5]	0.9805	0.98	300	3	0.9883	0.59	300	2	1.0000	0.00	79	1
Average Filter [3 × 3]	1.0000	0.00	14	2	1.0000	0.00	16	3	1.0000	0.00	11	1
Average Filter [5 × 5]	1.0000	0.00	190	3	1.0000	0.00	124	2	1.0000	0.00	51	1
Wiener Filter [3 × 3]	1.0000	0.00	14	2	1.0000	0.00	14	2	1.0000	0.00	7	1
Wiener Filter [5 × 5]	1.0000	0.00	118	3	1.0000	0.00	64	2	1.0000	0.00	45	1
Lowpass Filter ([3 × 3],$\sigma = 0.5$)	1.0000	0.00	3	1	1.0000	0.00	5	2	1.0000	0.00	3	1
Histogram Equalization	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Gamma Correction ($\gamma = 0.5$)	1.0000	0.00	2	1	1.0000	0.00	2	1	1.0000	0.00	3	2
Sharpning	1.0000	0.00	3	1	1.0000	0.00	5	2	1.0000	0.00	5	2
Blurring (len = 10, $\theta = 45$)	0.9453	2.73	300	3	0.9844	0.78	300	1	0.9590	2.05	300	2

Table 6 (continued)

Attacks	IWT+u.SVD				DWT+u.SVD				CT + u.SVD			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
Resizing (scale = 2)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Resizing (scale = 0.9)	1.0000	0.00	9	1	1.0000	0.00	9	1	1.0000	0.00	9	1
Resizing (scale = 0.5)	1.0000	0.00	11	1	1.0000	0.00	11	1	1.0000	0.00	13	2
Resizing (scale = 0.3)	1.0000	0.00	118	2	1.0000	0.00	150	3	1.0000	0.00	111	1
Cropping (15%)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Cropping (25%)	1.0000	0.00	24	2	1.0000	0.00	24	2	1.0000	0.00	10	1
Cropping (50%)	0.7012	14.94	300	2	0.7012	14.94	300	2	0.9902	0.49	300	1
Rotation (1°)	1.0000	0.00	9	2	1.0000	0.00	7	1	1.0000	0.00	7	1
Rotation (5°)	1.0000	0.00	9	2	1.0000	0.00	9	2	1.0000	0.00	7	1
Rotation (15°)	1.0000	0.00	12	2	1.0000	0.00	12	2	1.0000	0.00	9	1
Rotation (33°)	1.0000	0.00	18	2	1.0000	0.00	18	2	1.0000	0.00	13	1
Rotation (45°)	1.0000	0.00	16	2	1.0000	0.00	22	3	1.0000	0.00	11	1
Rotation (90°)	1.0000	0.00	14	2	1.0000	0.00	14	2	1.0000	0.00	12	1
Complement	− 1.0000	100.00	3	1	− 1.0000	100.00	3	1	− 1.0000	100.00	3	1
Frame Averaging (100%)	1.0000	0.00	11	1	1.0000	0.00	11	1	1.0000	0.00	17	2
Frame Dropping (10%)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	5	2
Frame Dropping (20%)	1.0000	0.00	5	1	1.0000	0.00	5	1	1.0000	0.00	8	2
Frame Swapping (10%)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	5	2
Frame Swapping (20%)	1.0000	0.00	6	1	1.0000	0.00	6	1	1.0000	0.00	8	2
Frame Insertion (10%)	1.0000	0.00	5	1	1.0000	0.00	5	1	1.0000	0.00	6	2
Frame Insertion (20%)	1.0000	0.00	7	1	1.0000	0.00	7	1	1.0000	0.00	10	2
H.264 Compression	1.0000	0.00	104	2	1.0000	0.00	90	1	1.0000	0.00	112	3
Motion Jpeg AVI	1.0000	0.00	58	2	1.0000	0.00	56	1	1.0000	0.00	58	2
Motion Jpeg 2000	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1

Table 6 (continued)

Attacks	IWT+u.SVD				DWT+u.SVD				CT + u.SVD			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
Mean	0.9463	2.6865	53.49	1.6326	0.9461	2.6944	51.14	1.6122	0.9545	2.2740	42.16	1.4081

Table 7 NC and BER(%) values of proposed algorithm against various attacks based on *v.SVD* for Foreman video

Attacks	IWT+*v.SVD*				DWT+*v.SVD*				CT + *v.SVD*			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
No attack	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Salt & Pepper (0.1%)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Salt & Pepper (1%)	1.0000	0.00	5	1	1.0000	0.00	7	2	1.0000	0.00	10	3
Salt & Pepper (5%)	1.0000	0.00	33	2	1.0000	0.00	35	3	1.0000	0.00	21	1
Salt & Pepper (10%)	1.0000	0.00	65	3	1.0000	0.00	55	2	1.0000	0.00	53	1
Salt & Pepper (30%)	1.0000	0.00	285	3	1.0000	0.00	219	2	1.0000	0.00	205	1
Gaussian Noise ($\sigma^2 = 0.001$)	1.0000	0.00	4	1	1.0000	0.00	5	2	1.0000	0.00	5	2
Gaussian Noise ($\sigma^2 = 0.01$)	1.0000	0.00	17	1	1.0000	0.00	21	2	1.0000	0.00	23	3
Jpeg Compression (QF = 10)	0.8301	8.50	300	3	0.8340	8.30	300	2	0.8398	8.01	300	1
Jpeg Compression (QF = 50)	1.0000	0.00	54	1	1.0000	0.00	60	3	1.0000	0.00	57	2
Jpeg Compression (QF = 75)	1.0000	0.00	53	3	1.0000	0.00	41	2	1.0000	0.00	39	1
Jpeg Compression (QF = 90)	1.0000	0.00	34	1	1.0000	0.00	34	1	1.0000	0.00	34	1
Jpeg 2000 (Ratio = 10)	1.0000	0.00	7	3	1.0000	0.00	5	2	1.0000	0.00	3	1
Jpeg 2000 (Ratio = 20)	1.0000	0.00	57	3	1.0000	0.00	43	2	1.0000	0.00	10	1
Median Filter [3 × 3]	1.0000	0.00	9	1	1.0000	0.00	9	1	1.0000	0.00	9	1
Median Filter [5 × 5]	1.0000	0.00	256	3	1.0000	0.00	220	2	1.0000	0.00	72	1
Average Filter [3 × 3]	1.0000	0.00	17	3	1.0000	0.00	14	2	1.0000	0.00	9	1
Average Filter [5 × 5]	1.0000	0.00	155	3	1.0000	0.00	151	2	1.0000	0.00	76	1
Wiener Filter [3 × 3]	1.0000	0.00	13	2	1.0000	0.00	13	2	1.0000	0.00	6	1
Wiener Filter [5 × 5]	1.0000	0.00	77	2	1.0000	0.00	87	3	1.0000	0.00	33	1
Lowpass Filter ([3 × 3],$\sigma = 0.5$)	1.0000	0.00	3	1	1.0000	0.00	5	2	1.0000	0.00	3	1
Histogram Equalization	1.0000	0.00	4	2	1.0000	0.00	3	1	1.0000	0.00	3	1
Gamma Correction ($\gamma = 0.5$)	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Sharpning	1.0000	0.00	3	1	1.0000	0.00	3	1	1.0000	0.00	3	1
Blurring (len = 10, $\theta = 45$)	0.9863	0.68	300	3	1.0000	0.00	215	1	0.9824	0.88	300	2

Table 7 (continued)

Attacks	IWT+*v.SVD*				DWT+*v.SVD*				CT + *v.SVD*			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
Resizing (scale = 2)	1.0000	0.00	3	2	1.0000	0.00	3	2	1.0000	0.00	2	1
Resizing (scale = 0.9)	1.0000	0.00	3	1	1.0000	0.00	5	2	1.0000	0.00	3	1
Resizing (scale = 0.5)	1.0000	0.00	9	1	1.0000	0.00	9	1	1.0000	0.00	13	2
Resizing (scale = 0.3)	1.0000	0.00	85	2	1.0000	0.00	131	3	1.0000	0.00	76	1
Cropping (15%)	1.0000	0.00	5	2	1.0000	0.00	5	2	1.0000	0.00	3	1
Cropping (25%)	1.0000	0.00	5	1	1.0000	0.00	5	1	1.0000	0.00	5	1
Cropping (50%)	1.0000	0.00	11	1	1.0000	0.00	11	1	1.0000	0.00	11	1
Rotation (1°)	1.0000	0.00	5	2	1.0000	0.00	5	2	1.0000	0.00	3	1
Rotation (5°)	1.0000	0.00	6	2	1.0000	0.00	7	3	1.0000	0.00	5	1
Rotation (15°)	1.0000	0.00	7	1	1.0000	0.00	7	1	1.0000	0.00	7	1
Rotation (33°)	1.0000	0.00	11	1	1.0000	0.00	11	1	1.0000	0.00	15	2
Rotation (45°)	1.0000	0.00	9	1	1.0000	0.00	9	1	1.0000	0.00	9	1
Rotation (90°)	1.0000	0.00	9	1	1.0000	0.00	9	1	1.0000	0.00	14	2
Complement	− 1.0000	100.00	4	1	− 1.0000	100.00	5	2	− 1.0000	100.00	4	1
Frame Averaging (100%)	1.0000	0.00	15	1	1.0000	0.00	15	1	1.0000	0.00	15	1
Frame Dropping (10%)	1.0000	0.00	7	2	1.0000	0.00	2	1	1.0000	0.00	2	1
Frame Dropping (20%)	1.0000	0.00	3	1	1.0000	0.00	41	3	1.0000	0.00	5	2
Frame Swapping (10%)	1.0000	0.00	7	2	1.0000	0.00	2	1	1.0000	0.00	2	1
Frame Swapping (20%)	1.0000	0.00	3	1	1.0000	0.00	41	3	1.0000	0.00	5	2
Frame Insertion (10%)	1.0000	0.00	6	2	1.0000	0.00	6	2	1.0000	0.00	4	1
Frame Insertion (20%)	1.0000	0.00	7	3	1.0000	0.00	6	2	1.0000	0.00	3	1
H.264 Compression	1.0000	0.00	55	3	1.0000	0.00	67	2	1.0000	0.00	51	1
Motion Jpeg AVI	1.0000	0.00	53	3	1.0000	0.00	41	2	1.0000	0.00	39	1
Motion Jpeg 2000	1.0000	0.00	7	3	1.0000	0.00	5	2	1.0000	0.00	3	1

Table 7 (continued)

Attacks	IWT+*v.SVD*				DWT+*v.SVD*				CT + *v.SVD*			
	NC	BER	FNo#	R#	NC	BER	FNo#	R#	NC	BER	FNo#	R#
Mean	0.9554	2.2282	42.75	1.8163	0.9558	2.2102	40.86	1.7755	0.9556	2.2222	32.28	1.2448

Fig. 12 The results of proposed error correction : **a** cropping attack (25%) **b** extracted watermark for each frame **c** error correction process for even frames

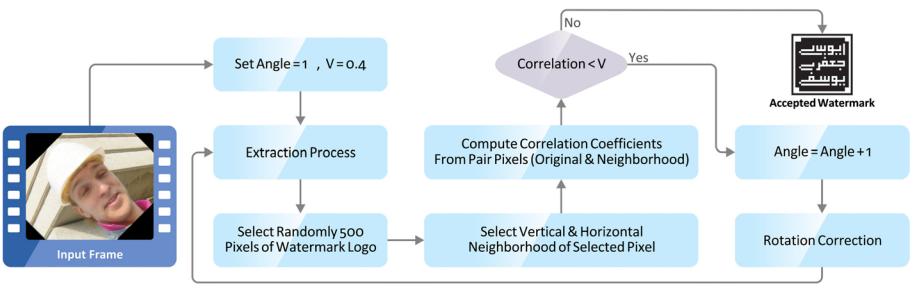

Fig. 13 The flowchart of correction algorithm for rotation attack

frame.Also, each watermark is extracted from a frame at IWT, DWT, and CT transforms, respectively, 8.8×10^{-5}, 9.11×10^{-5} and 1.39×10^{-4} s. This is a tolerable time for offline methods, especially copyright protection, which requires more careful work. But for online methods, this time speed is not very efficient and should be considered another way of

Fig. 14 The example of correction steps in rotation attack and correlation values for Foreman video

implementing the algorithm. One solution is not to include a watermark for embedding in each frame, but a watermark in a sequence of tens of frames to break it down into smaller intervals. As we know, unlike offline methods, there is no limit to the number of frames due to the long streams in online methods.

6.10 Analysis of payload capability

Based on the results of the simulation, the best payload capability for the videos in CIF format is a watermark with 1024-bit per frame. Inserting more than this amount greatly reduces the visual quality of a frame, as well as increases the artificial blocks in the watermarked video. It is natural that in videos in HD format several times of this amount can be inserted to watermarked video. Inserting values less than 1024-bit increases visual quality, but requires more frames to extract watermark and may be less effective in videos with limited frames.

7 Comparison with similar methods

In order to show the performance and quality of the presented algorithm, this section compares the imperceptibility and robustness results of similar video watermarking techniques with the proposed algorithm. In the first part, different types of transform domain methods are selected for comparative analysis. These algorithms are based on *DWT*, *IWT*, *CT*, and *DCT*, respectively. Table 9 demonstrates the comparison results of *PSNR* and *SSIM* measures between the selected approaches and the proposed scheme based on various standard cover video. It can be clearly seen that the proposed method outperformed the most similar methods in the imperceptibility and visual quality analysis with respect to the results of similar approaches.

In the second part of this section, the robustness of the proposed technique is compared with some similar methods based on the quality of the extracted watermark. Generally, similar approaches used standard video datasets in the embedding and extraction process. Moreover, the *NC* and *BER* results are used to measure the quality between the original

Table 8 Ranking of combination methods in proposed video watermarking based on visual quality analysis and resistance to attacks

Rank#	Method	Visual quality analysis			Rank#	Method	Resistance to attacks			
		PSNR*	SSIM	FNo#			NC*	BER(%)	FNo#	R#
1	DWT + v.SVD	40.930	0.9900	3.220	1	DWT + v.SVD	0.9558	2.2102	40.86	1.7755
2	DWT + u.SVD	40.900	0.9895	3.056	2	CT + v.SVD	0.9556	2.2222	32.28	1.2448
3	IWT + v.SVD	40.867	0.9897	3.333	3	IWT + v.SVD	0.9554	2.2282	42.75	1.8163
4	IWT + u.SVD	40.830	0.9892	3.111	4	CT + u.SVD	0.9545	2.2740	42.16	1.4081
5	CT + u.SVD	40.040	0.9851	3.111	5	IWT + u.SVD	0.9463	2.6865	53.49	1.6326
6	CT + v.SVD	39.880	0.9863	2.722	6	DWT + u.SVD	0.9461	2.6944	51.14	1.6122

Table 9 The comparison of PSNR and SSIM results between the proposed method and similar algorithms

Videos	Chen and Zhao (2017b)	Li and Wang (2019)	Tian et al. (2019)	Agilandeeswari and Ganesan (2016b)	Amiri et al. (2019)		Farri and Ayubi (2018)		Barani et al. (2020b)		DWT + v.SVD	
	PSNR	PSNR	PSNR	PSNR	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Akiyo	–	–	–	36.11	–	–	37.62	0.904			**42.47**	0.9906
Container	–	36.55	–	36.67	–	–	–	–	–	–	**39.44**	**0.9869**
Mother–Daughter	–	–	–	36.99	–	–	39.33	0.986	–	–	**45.12**	**0.9889**
Flower	38.64	–	**41.60**	–	38.92	0.9591	–	–	–	–	38.70	0.9865
Mobile	40.31	33.06	39.50		39.09	0.9625	41.56	0.9830	–	-	**42.93**	**0.9829**
Foreman	42.32	36.41	–	–	38.98	0.9619	**45.07**	0.9040	–	–	38.39	0.9837
Coastguard	–	34.10	–	–	39.06	0.9611	–	–	–	–	**41.47**	**0.9937**
Stefan	41.93	–	–	–	–	–	40.00	0.9750	–	–	**43.25**	**0.9864**
Aspen	–	–	–	–	–	–	–	–	47.29	0.9957	**48.36**	**0.9961**

*The best values compared to other methods are indicated by the bold symbol

Table 10 The comparison of NC results between the proposed method and similar algorithms based on DWT

Attacks	El'Arbi et al. (2011)	Singh et al. (2013)	Youssef et al. (2014)	Faragallah (2013)	Li et al. (2015)	Wang et al. (2015)	Himeur and Boukabou (2017)	DWT + v.SVD
MJPEG	**1.000**	0.973	0.950	**1.000**	0.540	0.909	**1.000**	**1.000**
H264/AVC (QP = 20)	0.960	0.909	0.781	0.921	**1.000**	0.454	0.997	**1.000**
Cropping (15%)	0.663	0.960	0.893	**1.000**	0.980	0.909	0.996	**1.000**
Gaussian noise (var = 0.01)	0.982	0.982	0.946	**1.000**	0.918	0.979	1.000	**1.000**
Salt and pepper (var = 0.01)	0.975	0.991	0.951	0.980	0.900	0.979	1.000	**1.000**
Scaling (100%)	0.670	0.948	0.920	0.952	0.870	0.636	0.992	**1.000**
Blurring	0.941	0.965	0.967	0.974	0.953	0.945	0.978	**1.000**
Sharpening	0.976	0.991	0.900	0.981	0.961	0.909	**1.000**	**1.000**
Histogram equalization	**1.000**	**1.000**	**1.000**	**1.000**	0.982	**1.000**	**1.000**	**1.000**
Median Filter (3 × 3)	0.918	0.989	0.931	0.991	0.906	0.633	1.000	**1.000**
Frame averaging	0.890	0.983	0.960	0.952	**1.000**	0.818	0.990	**1.000**

*The best values compared to other methods are indicated by the bold symbol

Table 11 The comparison of BER (%) results between the proposed method and similar algorithms based on DWT

Attacks	El'Arbi et al. (2011)	Singh et al. (2013)	Youssef et al. (2014)	Faragallah (2013)	Li et al. (2015)	Wang et al. (2015)	Himeur and Boukabou (2017)	Proposed DWT + v.SVD
MJPEG	**0.00**	2.69	5.14	**0.00**	46.01	9.21	0.10	**0.00**
H264/AVC (QP = 20)	4.13	9.15	12.9	7.91	0.00	54.60	1.00	**0.00**
Cropping (15%)	33.69	4.08	10.73	**0.00**	2.03	9.70	0.30	**0.00**
Gaussian noise (var = 0.01)	1.84	1.89	5.44	**0.00**	8.17	2.09	**0.00**	**0.00**
Salt and pepper (var = 0.01)	2.51	0.93	4.92	2.30	9.98	2.10	**0.00**	**0.00**
Scaling (100%)	33.12	5.26	8.06	4.84	12.95	36.40	0.20	**0.00**
Blurring	5.95	3.50	3.37	2.62	13.02	5.50	0.70	**0.00**
Sharpening	2.46	0.99	10.07	1.98	3.91	9.10	**0.00**	**0.00**
Histogram equalization	**0.00**	**0.00**	**0.00**	**0.00**	1.86	**0.00**	**0.00**	**0.00**
Median Filter (3 × 3)	8.22	1.18	6.92	0.97	9.43	36.70	**0.00**	**0.00**
Frame averaging	11.18	1.77	4.03	4.88	**0.00**	18.20	1.30	**0.00**

*The best values compared to other methods are indicated by the bold symbol

watermark and extracted watermark from the attacked videos. Tables 10 and 11 illustrate the comparison results between some *DWT* based video watermarking schemes and the proposed DWT + v.SVD method. In these tables, the *NC* and *BER(%)* results are calculated between the original watermark and the extracted watermark from attacked videos. In these tables, the watermarked Foreman video is used for comparison. It can be seen that the most results of the proposed method highly outperform those obtained by similar algorithms.

In the following, this paper chooses some Contourlet transform (*CT*) based approaches to show the robustness of the presented method. In these methods, the Mobile, Aspen, Rhino, and Foreman videos are selected to apply rotation, aspect to 16/9, frame averaging, gaussian noise, salt & pepper Noise, median filtering, histogram equalization, and compression attacks. Then the results of NC between the original watermark and extracted watermarks are calculated. The results of this comparison are shown in Table 12 for *NC* measure. Based on results of this table, the proposed CT + v.SVD performs better than other *CT* based similar methods.

Moreover, a few similar algorithms based on integer wavelet transform (*IWT*) are utilized to compare results of the *BER* and *NC* measures between the original watermark and extracted watermarks after applying scaling, cropping, median filter, average filter, and lossy JPEG attacks. These results are shown in Tables 13 and 14. These two tables show that the proposed approach has better robustness against different types of attacks in the *IWT* transform domain and outperforms those obtained by similar algorithms.

In addition to the comparisons made, we tried to represent temporal attacks including frame averaging, frame dropping, and frame insertion in a separate table. Table 15 shows the results of this comparison. Based on the results of this table, the proposed method and method (Farri and Ayubi 2018) showed better performance than the other methods.

8 Conclusion

This article presents a secure video watermarking based on a new chaotic map. Analysis of the dynamical system in the proposed two-dimensional complex map, such as chaos trajectory, bifurcation diagram, Lyapunov exponent, and randomness tests showed that the proposed iterative map could be used in a cryptographic system. The 460-bit keyspace also represents a fully secure system to ensure the security of the watermarking system.

In the embedding and extraction process, IWT, DWT, and CT transforms were used along with single value decomposition (SVD) with u.SVD and v.SVD states. In the visual quality analysis, and analysis of resistance to attacks, the combination of DWT + v.SVD performed better than other combinations. Also, a new correlation-based process was used for the geometric rotation attack that the proposed method was able to successfully overcome the rotation attack. The results of simulation and comparison with other methods showed that the proposed algorithm performs better than other methods so that in all types of attacks, the NC criterion has a value of 1.00. In terms of time complexity, the proposed process of inserting and extracting watermark for offline methods is relatively acceptable. But for online methods, there has to be some change in the embedding process. This paper focuses on presenting a new chaotic map to enhance the security of the watermarking system. Also, one of the problems with chaotic watermarking systems in geometric attacks, especially the rotation attack, has been fixed. In future work, a variety of geometrical

Table 12 The comparison of NC results between the proposed method and similar algorithms based on CT

Attacks	Barani et al. (2020b)	Agilandeeswari and Ganesan (2016a)	Chen and Zhao (2017b)			CT + v.SVD			
	Aspen	Rhino	Mobile	Flower	Foreman	Rhino	Mobile	Foreman	Aspen
Rotation (1°)	0.9217	0.8129	0.9039	0.8619	0.9123	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Rotation (3°)	–	0.8082	0.8763	0.8381	0.8805	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Rotation (5°)	0.8925	0.8073	0.8517	0.8160	0.8692	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Aspect to 16/9	–	–	0.8165	0.8691	0.8352	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Frame averaging	–	–	0.9370	0.9317	0.9526	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Gaussian noise ($\sigma^2 = 0.01$)	–	0.8941	0.7692	0.7260	0.7689	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Salt and pepper noise	–	0.9861	0.8362	0.8351	0.8564	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Median filtering (5×5)	–	0.7533	0.9325	0.9519	0.9632	**1.0000**	**1.0000**	**1.0000**	**1.0000**
Histogram equalization	–	0.7140	0.9725	0.9753	0.9668	**1.0000**	**1.0000**	**1.0000**	**1.0000**
JPEG (QF = 10)	0.6797	–	-	–	–	0.4609	0.9707	0.9062	**0.8329**
JPEG (QF = 30)	1.0000		–	–	–	0.9929	1.0000	1.0000	**1.0000**
JPEG2000 (Ratio = 60)	1.0000	–	–	–	–	0.9804	0.8261	0.9843	**1.0000**
MJPEG	0.9640	–	–	–	–	1.0000	1.0000	1.0000	**1.0000**
H.264	0.8950	–	–	–	–	0.9960	0.8808	1.0000	**0.9235**

*The best values compared to other methods are indicated by the bold symbol

Table 13 The comparison of BER (%) results between the proposed method and similar algorithms based on IWT

Attacks	Farri and Ayubi (2018)		Mohammadi (2015)	Bhardwaj et al. (2018)		IWT + v.SVD	
	Akiyo	Foreman	Foreman	Akiyo	Foreman	Akiyo	Foreman
Amplification (1.5)	–	–	–	9.18	**0.00**	**0.00**	**0.00**
Scaling (0.5)	–	–	**0.00**	2.34	0.49	**0.00**	**0.00**
Scaling (0.9)	–	–	–	0.09	**0.00**	**0.00**	**0.00**
Cropping (1/4)	**0.00**	**0.00**	–	4.79	4.98	**0.00**	**0.00**
Cropping (1/2)	–	–	–	16.70	16.31	**0.51**	**0.49**
Gaussian Noise (0.01)	**0.00**	**0.00**	–	7.42	9.47	**0.00**	**0.00**
Salt & Pepper Noise (0.01)	0.29	**0.00**	–	3.22	3.03	**0.00**	**0.00**
Salt & Pepper Noise (0.001)	–	–	**0.00**	1.07	0.59	**0.00**	**0.00**
Median Filter (3 × 3)	**0.00**	**0.00**	1.00	0.98	**0.00**	**0.00**	**0.00**
Median Filter (5×5)	–	–	4.00	3.71	0.78	**0.00**	**0.00**
Average Filter (3×3)	**0.00**	**0.00**	–	6.05	4.39	**0.00**	**0.00**
Average Filter (5×5)	–	–	–	16.02	14.36	**0.00**	**0.00**
Histogram Equalization	**0.00**	**0.00**	–	11.04	5.66	**0.00**	**0.00**
Sharpening	**0.00**	**0.00**	–	0.20	**0.00**	**0.00**	**0.00**
JPEG (40)	–	–	–	0.78	0.09	**0.00**	**0.00**
JPEG (50)	–	–	3.00	0.29	**0.00**	**0.00**	**0.00**
JPEG (60)	–	–	–	0.20	**0.00**	**0.00**	**0.00**
JPEG (70)	**0.00**	–	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
JPEG (80)	–	–	–	0.09	**0.00**	**0.00**	**0.00**
JPEG (90)	–	–	**0.00**	0.09	**0.00**	**0.00**	**0.00**

*The best values compared to other methods are indicated by the bold symbol

Table 14 Comparison of NCC values based on IWT

Attacks	IWT Agilandeeswari and Ganesan (2016b)		IWT + SVD Farri and Ayubi (2018)		Proposed (IWT + v.SVD)	
	Mother_Daughter	Akiyo	Mother_Daughter	Akiyo	Mother_Daughter	Akiyo
No Attack	0.999	0.999	**1.000**	**1.000**	**1.000**	**1.000**
Salt & Papper	0.877	0.888	**1.000**	0.994	**1.000**	**1.000**
Gaussian Noise	0.888	0.999	0.986	0.974	**1.000**	**1.000**
Median Filter	0.537	0.523	**1.000**	**1.000**	**1.000**	**1.000**
Rotation	0.873	0.928	0.972	0.404	**1.000**	**1.000**
Cropping	0.844	0.885	**1.000**	**1.000**	**1.000**	**1.000**

*The best values compared to other methods are indicated by the bold symbol

attacks will be attempted to increase the resistance of the chaotic watermarking algorithm to such attacks.

Table 15 Comparison of NCC values against temporal attacks

Video	References	Attacks		
		Frame Dropping	Frame Swapping	Frame Averaging
Akiyo	Agilandeeswari and Ganesan (2016b)	0.985	–	0.985
	Joshi et al. (2017)	0.933	0.935	0.921
	Farri and Ayubi (2018)	**1.000**	**1.000**	**1.000**
	Proposed	**1.000**	**1.000**	**1.000**
Foreman	Chen and Zhao (2017b)	–	–	0.952
	Himeur and Boukabou (2017)	–	–	0.990
	Akhlaghian and Bahrami (2015)	0.941	–	0.989
	Farri and Ayubi (2018)	**1.000**	**1.000**	**1.000**
	Proposed	**1.000**	**1.000**	**1.000**
Mobile	Chen and Zhao (2017b)	–	–	0.937
	Farri and Ayubi (2018)	**1.000**	**1.000**	**1.000**
	Proposed	**1.000**	**1.000**	**1.000**
News	Bhardwaj et al. (2018)	0.690	–	–
	Farri and Ayubi (2018)	**1.000**	**1.000**	**1.000**
	Proposed	**1.000**	**1.000**	**1.000**

*The best values compared to other methods are indicated by the bold symbol

Acknowledgements I am dedicated to Imam Hussein, who has all my scientific life from his love. I am grateful to the editor-in-chief, the editors, and the esteemed reviewers who have contributed to the improvement of the quality of this article with careful and scientific comments. I would also like to express my special thanks to my dear students who helped me with the simulation and implementation of this article despite their graduation.

Compliance with ethical standards

Conflict of interest The authors of this paper confirm that any part of this work was not published or submitted for publication elsewhere, and authors do not have any conflict of interest with anybody else.

References

Agilandeeswari L, Ganesan K (2016a) A robust color video watermarking scheme based on hybrid embedding techniques. Multimed Tools Appl 75(14):8745–8780

Agilandeeswari L, Ganesan K (2016b) An efficient hilbert and integer wavelet transform based video watermarking. J Eng Sci Technol 11(3):327–345

Akhlaghian F, Bahrami Z (2015) A new robust video watermarking algorithm against cropping and rotating attacks, In: 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), IEEE, pp. 122–127

Akhshani A, Behnia S, Akhavan A, Jafarizadeh M, Hassan HA, Hassan Z (2009) Hash function based on hierarchy of 2D piecewise nonlinear chaotic maps. Chaos Solitons Fractals 42(4):2405–2412

Akhshani A, Akhavan A, Mobaraki A, Lim S-C, Hassan Z (2014) Pseudo random number generator based on quantum chaotic map. Commun Nonlinear Sci Numer Simul 19(1):101–111

Al-Otum HM (2014) Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique. J Vis Commun Image Represent 25(5):1064–1081

Amiri MD, Amiri A, Meghdadi M (2019) HVS-based scalable video watermarking. Multimed Syst 25(4):273–291

Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recognit Lett 94(Supplement C):228–236
Asikuzzaman M, Pickering MR (2018) An overview of digital video watermarking. IEEE Trans Circuits Syst Video Technol 28(9):2131–2153
Ayubi P, Setayeshi S, Rahmani AM (2020) Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application. J Inf Secur Appl 52:102472
Barani MJ, Valandar MY, Ayubi P (2015a) A secure watermark embedding approach based on chaotic map for image tamper detection. In: 2015 7th conference on information and knowledge technology (IKT). IEEE, pp 1–5
Barani MJ, Ayubi P, Jalili F, Valandar MY, Azariyun E (2015b) Image forgery detection in contourlet transform domain based on new chaotic cellular automata. Secur Commun Netw 8(18):4343–4361
Barani MJ, Valandar MY, Ayubi P (2019) A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3d quantum map. Optik 187:205–222
Barani MJ, Ayubi P, Yousefi Valandar M, Irani BY (2020a) A new pseudo random number generator based on generalized newton complex map with dynamic key. J Inf Secur Appl 53:102509
Barani MJ, Ayubi P, Valandar MY, Irani BY (2020b) A blind video watermarking algorithm robust to lossy video compression attacks based on generalized newton complex map and contourlet transform. Multimed Tools Appl 79(3):2127–2159
Batool SI, Shah T, Khan M (2014) A color image watermarking scheme based on affine transformation and S4 permutation. Neural Comput Appl 25(7):2037–2045
Bayoudh I, Jabra SB, Zagrouba E (2017) Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications. Multimed Tools Appl 77:14361–14379
Behnia S, Teshnehlab M, Ayubi P (2010) Multiple-watermarking scheme based on improved chaotic maps. Commun Nonlinear Sci Numer Simul 15(9):2469–2478
Behnia S, Ayubi P, Soltanpoor W (2012) Image encryption based on quantum chaotic map and FSM transforms. In: 2012 XVth international conference on telecommunications network strategy and planning symposium (NETWORKS). IEEE, pp 1–6
Behnia S, Ahadpour S, Ayubi P (2014) Design and implementation of coupled chaotic maps in watermarking. Appl Soft Comput 21:481–490
Belhaj M, Mitrea M, Prêteux F, Duta S (2010) MPEG-4 AVC robust video watermarking based on QIM and perceptual masking. In: 2010 8th international conference on communications, pp 477–480
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
Boisvert J, Drouin M-A, Jodoin P-M (2015) High-speed transition patterns for video projection, 3d reconstruction, and copyright protection. Pattern Recognit 48(3):720–731
Caragata D, Mucarquer JA, Koscina M, Assad SE (2016) Cryptanalysis of an improved fragile watermarking scheme. AEU Int J Electron Commun 70(6):777–785
Chamlawi R, Khan A (2010) Digital image authentication and recovery: employing integer transform based information embedding and extraction. Inf Sci 180(24):4909–4928
Chang C-C, Chen K-N, Lee C-F, Liu L-J (2011) A secure fragile watermarking scheme based on chaos-and-hamming code. J Syst Softw 84(9):1462–1470
Chen L, Zhao J (2017a) Robust contourlet-based blind watermarking for depth-image-based rendering 3D images. Sig Process Image Commun 54(Supplement C):56–65
Chen L, Zhao J (2017b) Contourlet-based image and video watermarking robust to geometric attacks and compressions. Multimed Tools Appl 77:7187–7204
Do MN, Vetterli M (2005) The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans Image Process 14(12):2091–2106
Dutta T, Gupta HP (2016) A robust watermarking framework for high efficiency video coding (HEVC)-encoded video with blind extraction process. J Vis Commun Image Represent 38:29–44
El'Arbi M, Koubaa M, Charfeddine M, Amar CB (2011) A dynamic video watermarking algorithm in fast motion areas in the wavelet domain. Multimed Tools Appl 55(3):579–600
Faragallah OS (2013) Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. AEU Int J Electron Commun 67(3):189–196
Farri E, Ayubi P (2018) A blind and robust video watermarking based on IWT and new 3D generalized chaotic sine map. Nonlinear Dyn 93:1875–1897
Hadi RM, Ayubi P (2012) Blind digital image watermarking based on CT-SVD and chaotic cellular automata. In: 2012 2nd international conference on computer and knowledge engineering (ICCKE). IEEE, pp 301–306

Himeur Y, Boukabou A (2017) A robust and secure key-frames based video watermarking system using chaotic encryption. Multimed Tools Appl 77:8603–8627
Inceoglu F (2015) Copyright protection and entry deterrence. Inf Econ Policy 32(Supplement C):38–45 big Media: Economics and Regulation of Digital Markets
Irani BY, Ayubi P, Jabalkandi FA, Valandar MY, Barani MJ (2019) Digital image scrambling based on a new one-dimensional coupled sine map. Nonlinear Dyn 97(4):2693–2721
Joshi AM, Gupta S, Girdhar M, Agarwal P, Sarker R (2017) Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique, In: Proceedings of the international conference on data engineering and communication technology. Springer, pp 455–463
Keyvanpour M, Merrikh-Bayat F (2011) An effective chaos-based image watermarking scheme using fractal coding. Procedia Comput Sci 3(Supplement C):89–95 world Conference on Information Technology
Khalilian H, Bajic IV (2013) Video watermarking with empirical PCA-based decoding. IEEE Trans Image Process 22(12):4825–4840
Klema V, Laub A (1980) The singular value decomposition: its computation and some applications. IEEE Trans Autom Control 25(2):164–176
Kocarev L, Lian S (2011) Chaos-based cryptography: theory, algorithms and applications, vol 354. Springer, Berlin
L'Ecuyer P, Simard R (2007) Testu01: AC library for empirical testing of random number generators. ACM Trans Math Softw (TOMS) 33(4):22
Lee S-H (2014) DWT based coding dna watermarking for dna copyright protection. Inf Sci 273:263–286
Li Y, Wang H-X (2019) Robust H.264/AVC video watermarking without intra distortion drift. Multimed Tools Appl 78(7):8535–8557
Li Z, Chen X-W, Ma J (2015) Adaptively imperceptible video watermarking based on the local motion entropy. Multimed Tools Appl 74(8):2781–2802
Li C, Yang R, Liu Z, Li J, Guo Z (2016) Semi-fragile self-recoverable watermarking scheme for face image protection. Comput Electr Eng 54(Supplement C):484–493
Lin ZX, Peng F, Long M (2017) A reversible watermarking for authenticating 2d vector graphics based on bionic spider web. Sig Process Image Commun 57(Supplement C):134–146
Liu Y, Zhao J (2010) A new video watermarking algorithm based on 1D DFT and radon transform. Sig Process 90(2):626–639
Liu J, Wang Y, Li Y, Liu R, Chen J (2017) A robust and blind 3D watermarking algorithm using multiresolution adaptive parameterization of surface. Neurocomputing 237(Supplement C):304–315
Loganathan A, Kaliyaperumal G (2016) An adaptive hvs based video watermarking scheme for multiple watermarks using bam neural networks and fuzzy inference system. Expert Syst Appl 63:412–434
Makbol NM, Khoo BE, Rassem TH, Loukhaoukha K (2017) A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf Sci 417(Supplement C):381–400
Marsaglia G (1998) Diehard test suite. http://www.stat.fsu.edu/pub/diehard/. Accessed 8 Jan 2014
Mohammadi S (2015) A chaos-based video watermarking in wavelet domain. Ciência e Natura 37(6–2):364–370
Moosazadeh M, Ekbatanifard G (2017) An improved robust image watermarking method using DCT and YCoCg-R color space. Optik Int J Light Electron Opt 140(Supplement C):975–988
Panahi N, Amirani M, Behnia S, Ayubi P (2013) A new colour image watermarking scheme using cellular automata transform and Schur decomposition. In: 2013 21st Iranian conference on electrical engineering (ICEE). IEEE, pp 1–5
Pereira S, Voloshynovskiy S, Madueno M, Marchand-Maillet S, Pun T (2001) Second generation benchmarking and application oriented evaluation. In: Moskowitz IS (ed) Information hiding. Springer, Heidelberg, pp 340–353
Renza D, Lemus DMBLC (2018) Authenticity verification of audio signals based on fragile watermarking for audio forensics. Expert Syst Appl 91(Supplement C):211–222
Rukhin A, Soto J, Nechvatal J, Smid M, Barker E (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report, Booz-Allen and Hamilton Inc Mclean, VA
Selvam P, Balachandran S, Iyer SP, Jayabal R (2017) Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. Optik Int J Light Electron Opt 145(Supplement C):655–671
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
Soliman MM, Hassanien AE, Onsi HM (2016) An adaptive watermarking approach based on weighted quantum particle swarm optimization. Neural Comput Appl 27(2):469–481

Stirmark benchmark 4.0 (1997). https://www.petitcolas.net/watermarking/stirmark/
Strogatz SH (2014) Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. Westview Press, Boulder
Stütz T, Autrusseau F, Uhl A (2014) Non-blind structure-preserving substitution watermarking of H.264/CAVLC inter-frames. IEEE Trans Multimed 16(5):1337–1349
Su Q, Chen B (2017) A novel blind color image watermarking using upper Hessenberg matrix. AEU Int J Electron Commun 78(Supplement C):64–71
Su Q, Niu Y, Wang Q, Sheng G (2013) A blind color image watermarking based on DC component in the spatial domain. Optik Int J Light Electron Opt 124(23):6255–6260
Sun Z, Liu J, Sun J, Sun X, Ling J (2009) A motion location based video watermarking scheme using ICA to extract dynamic frames. Neural Comput Appl 18(5):507–514
Sun L, Xu J, Liu S, Zhang S, Li Y, Shen C (2018) A robust image watermarking scheme using Arnold transform and BP neural network. Neural Comput Appl 30:2425–2440
Sundararajan D (2016) Discrete wavelet transform: a signal processing approach. Wiley, Hoboken
Tian L, Dai H, Li C (2019) A semi-fragile video watermarking algorithm based on chromatic residual DCT. Multimed Tools Appl 77:1759–1779
Valandar MY, Ayubi P, Barani MJ (2015) High secure digital image steganography based on 3D chaotic map. In: 2015 7th conference on information and knowledge technology (IKT). IEEE, pp 1–6
Valandar MY, Ayubi P, Barani MJ (2017) A new transform domain steganography based on modified logistic chaotic map for color images. J Inf Secur Appl 34(Part 2):142–151
Valandar MY, Barani MJ, Ayubi P (2019a) A fast color image encryption technique based on three dimensional chaotic map. Optik 193:162921
Valandar MY, Barani MJ, Ayubi P, Aghazadeh M (2019b) An integer wavelet transform image steganography method based on 3d sine chaotic map. Multimed Tools Appl 78(8):9971–9989
Valandar MY, Barani MJ, Ayubi P (2020) A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map. Soft Comput 24(2):771–794
Video test media (2017). https://media.xiph.org/video/derf/
Walker J (2008) ENT: a pseudorandom number sequence test program. Software and documentation. www.fourmilab.ch/random/S
Wang X-Y, Yang H-Y, Zhang Y, Fu Z-K (2013) Image denoising using svm classification in nonsubsampled contourlet transform domain. Inf Sci 246:155–176
Wang X-Y, Liu Y-N, Li S, Yang H-Y, Niu P-P, Zhang Y (2015) A new robust digital watermarking using local polar harmonic transform. Comput Electr Eng 46:403–418
Wu C, Zheng Y, Ip W, Chan C, Yung K, Lu Z (2011) A flexible H.264/AVC compressed video watermarking scheme using particle swarm optimization based dither modulation. AEU Int J Electron Commun 65(1):27–36
Xu D-W, Wang R-d, Wang J-c (2010) Low complexity video watermarking algorithm by exploiting CAVLC in H.264/AVC. In: 2010 IEEE international conference on wireless communications, networking and information security (WCNIS). IEEE, pp 411–415
Yassin NI, Salem NM, El Adawy MI (2014) Qim blind video watermarking scheme based on wavelet transform and principal component analysis. Alex Eng J 53(4):833–842
Youssef SM, ElFarag AA, Ghatwary NM (2014) Adaptive video watermarking integrating a fuzzy wavelet-based human visual system perceptual model. Multimed Tools Appl 73(3):1545–1573
Yu M, Wang J, Jiang G, Peng Z, Shao F, Luo T (2015) New fragile watermarking method for stereo image authentication with localization and recovery. AEU Int J Electron Commun 69(1):361–370
Zhang F, Zhang X, Shang D (2012) Digital watermarking algorithm based on kalman filtering and image fusion. Neural Comput Appl 21(6):1149–1157