 CMC, vol.58, no.1, pp.263-285, 2019

A Robust Image Watermarking Scheme Using Z-Transform, Discrete Wavelet Transform and Bidiagonal Singular Value Decomposition

N. Jayashree[1, *] and R. S. Bhuvaneswaran[1]

Abstract: Watermarking is a widely used solution to the problems of authentication and copyright protection of digital media especially for images, videos, and audio data. Chaos is one of the emerging techniques adopted in image watermarking schemes due to its intrinsic cryptographic properties. This paper proposes a new chaotic hybrid watermarking method combining Discrete Wavelet Transform (DWT), Z-transform (ZT) and Bidiagonal Singular Value Decomposition (BSVD). The original image is decomposed into 3-level DWT, and then, ZT is applied on the HH3 and HL3 sub-bands. The watermark image is encrypted using Arnold Cat Map. BSVD for the watermark and transformed original image were computed, and the watermark was embedded by modifying singular values of the host image with the singular values of the watermark image. Robustness of the proposed scheme was examined using standard test images and assessed against common signal processing and geometric attacks. Experiments indicated that the proposed method is transparent and highly robust.

Keywords: Digital watermarking, chaotic mapping, z-transform, arnold cat map, discrete wavelet transform (DWT), bidiagonal singular value decomposition (BSVD).

1 Introduction

Increased usage of the internet and the availability of high-speed digital data networks made online transmission and distribution of multimedia contents over the web to grow exponentially. Copyright protection and authentication of these data are of primary concern since it can be duplicated, modified and re-transmitted easily. Digital watermarking is not only a solution to address security concerns of digital media but also facilitates copyright protection and authentication. It is also an important branch of information hiding, as it can be applied to high strength secure communication. A watermark is a sequence, carrying information, embedded into a digital image [Cox, Kilian, Leighton et al. (1997)]. It provides an excellent method for copyright protection of multimedia by embedding copyright information in them.

Watermarking algorithms can be broadly classified into two categories based on the embedding process; one is spatial domain and second is frequency domain schemes. The spatial domain method directly alters the pixel values of the original image to embed the

[1] Ramanujan Computing Centre, Anna University, Chennai, 600025, India.

[*] Corresponding Author: N. Jayashree. Email: jaisri8@gmail.com.

watermark. Although algorithms in this category are simple to implement, sophisticated operations require more computing resources and time. This drawback makes schemes in this category unsuitable for real-time situations. Transform domain schemes were proposed to overcome the limitations of the spatial domain method. The transform domain schemes, in the process, convert the original data, which is in the spatial domain, into a transform domain and vice versa. These conversions are made by utilizing mathematical transformation such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Z-transform (ZT) and Discrete Wavelet Transform (DWT). DWT is most commonly used in frequency domain watermarking due to its excellent spatiotemporal characteristics. Imperceptibility and robustness are two significant characteristics used to evaluate watermarking schemes. In order to improve robustness and imperceptibility, many hybrid watermarking schemes have been proposed combining various mathematical transformation.

A hybrid watermarking technique developed by Lai et al. [Lai and Tsai (2010)] employing single-level Haar DWT and SVD. In this scheme, the watermark image is divided into two parts and embedded into two different sub-bands to improve robustness and imperceptibility.

The image watermarking algorithm combining DWT, DCT, and SVD proposed by Fazli et al. [Fazli and Moeini (2016)] seeks to achieve robustness against geometric attacks. In this scheme, the host image is divided into four non-overlapping sub-images and the watermark is embedded in each sub-image independently. The semi-blind image watermarking scheme proposed by Saxena et al. [Saxena, Saxena and Rastogi (2014)], using trigonometric functions is robust against geometric distortions. The scheme is based on DWT, DCT, and SVD.

Bhatnagar et al. [Bhatnagar and Raman (2009)] introduced a robust semi-blind reference watermarking scheme based on DWT and SVD. In their another scheme [Bhatnagar, Wu and Raman (2012)] combining fractional wavelet packet transform, quadratic residues and SVD, the watermark strength for each embedding location is chosen from two candidate strengths using quadratic residue properties.

Shi [Shi (2014)] presented a robust scheme using DWT and SVD with circulation. In this scheme, Chebyshev map is used for scrambling the watermark information. In the hybrid image watermarking scheme based on DCT [Sverdlov, Dexter and Eskicioglu (2005)], the coefficients are mapped into four quadrants using the zig-zag sequence and show that watermark embedded in lower frequencies are robust against a set of attacks while watermark embedded in higher frequencies withstand against a different set of attacks.

Although, SVD is a widely used technique in the design of robust watermarking algorithms, the issue of the false positive problem (FPP) is a severe drawback. [Ling, Phan and Heng (2013); Makbol, Khoo and Rassem (2018); Xing and Tan (2010)]. Many FPP resistant SVD-based schemes have been proposed.

Ansari et al. [Ansari, Pant and Ahn (2016)] proposed a solution to the FPP in their method by embedding a signature generated using the UV matrices it in the HH sub-band of the host image. This signature is authenticated during the extraction process.

A block-based DWT-SVD watermarking scheme developed by Makbol et al. [Makbol, Khoo and Rassem (2016)] employed human visual system (HVS) characteristics for block selection and embedded a binary watermark in the U matrix to overcome the false positive problem.

Z-transform has been widely used for several image processing applications such as authentication, copyright protection and tamper detection [Ho, Zhu and Shen (2004); Ho, Zhu, Shen et al. (2008); Khan, Boda and Bhukya (2012); Mandal (2012); Rabiner, Schafer and Rader (1969); Stillings (1972); Takaya, Shimizu, Kitama et al. (1990); Vich (1987)]. The locations of the zeros of the z-transform are highly sensitive to changes in the pixel value, which is suitable for fragile watermarking. It is also easy to implement and provides better data hiding property. Based on these properties of Z-transform, Ho et al. [Ho, Zhu, Shen et al. (2008)] proposed a fragile watermarking scheme by encoding the zeros of the Z-transform. Ho et al. [Ho, Zhu and Shen (2004)] proposed another scheme for authentication of biomedical images based on zero location watermarking. Z-transform is also used in image steganography for grayscale images [Mandal (2012)]. A Z-transform-DWT based scheme was proposed by Jayashree and Bhuavaneswaran [Jayashree and Bhuvaneswaran (2016)].

In this paper, a watermarking algorithm using Z-transform, DWT, and BSVD is proposed. Arnold cat map is used to encrypt the watermark image to improve the security of the scheme. The rest of the paper is organized as follows: The Next part of the paper is Section 2 where, the Arnold Cat map, DWT, Z-transform, and BSVD are explained. In Section 3, the proposed algorithm is discussed in detail. Experimental results and performance analysis are presented in Section 4 before concluding the paper in Section 5.

2 Preliminaries

2.1 Discrete wavelet transform

Wavelet is a powerful mathematical tool used in a wide variety of applications like image denoising, data compression, watermarking and fingerprint verification [Sifuzzaman, Islam and Ali (2009)]. It provides a better representation of data by using Multi-Resolution Analysis (MRA). When DWT is applied to an input signal, it is decomposed into four sub-bands namely LL (low frequency), HH (high-frequency), HL (horizontal level frequency) and LH (vertical level frequency) sub-bands. The LL sub-band can be further decomposed into similar four sub-bands. Similarly, the input signal can be decomposed up to n-levels. DWT has both spatial and frequency information simultaneously thus provides the spatiotemporal representation of the data. It is also considered that the DWT represents the characteristics of the human visual system efficiently than other transform methods. The advantages of using wavelet transform include (1) simultaneous localization of data both in time and frequency domain and, (2) finer approximation of the data with few coefficients of the wavelets.

2.2 Z-transform

The z-transform plays a pivotal role in processing discrete data [Ho, Zhu, Shen et. al. (2008)]. Z-transform is a suitable and valuable tool for representing, analyzing and designing discrete-time signals and systems [Ho, Zhu, Shen et al. (2008)].

The z-transform of a discrete time signal x[n] is defined as

$$X[z] = \sum_{n=-\infty}^{\infty} x[n] z^{-n} \tag{1}$$

where, z is a complex variable. In the case of a sequence of image pixels, x(n) may be nonzero only in the interval $0 \leq n \leq \infty$, and the Eq. (3) reduces to one-sided z-transform.

$$X[z] = \sum_{n=0}^{\infty} x[n] z^{-n} \tag{2}$$

The inverse Z-transform is used to recover the discrete time sequence, x(n), given its Z-transform. Symbolically, the inverse Z-transform may be defined as

$$X'[n] = Z^{-1}[X(z)] \tag{3}$$

where X(z) is the Z-transform and Z^{-1} is the function for the inverse Z-transform. An algorithm for numerically calculating the Z-transform of a sequence of N samples is proposed by Rabiner et al. [Rabiner, Schafer and Rader (1969)]. This algorithm is termed as chirp Z-transform (CZT), and it is used to compute the Z-transform effectively at points in z-plane which lie on a spiral or circular contour at any arbitrary point. Application of this algorithm in digital watermarking improves the robustness and imperceptibility of the watermarked image. It is also best suited for many other image processing applications such as filtering, interpolation, and correlation.

There are many potential applications wherein the CZT algorithm is used like spectral analysis of speech, to the individual periods of voice with great success [Ho, Zhu and Shen (2004)]. The ability to evaluate the Z-transform inside and outside the unit circle and to efficiently analyze high resolution, narrow frequency spectrum bands help watermarking algorithms to improve robustness and imperceptibility of the watermarked image.

2.3 BSVD

The decomposition of a matrix into the orthogonal matrix and the diagonal matrix is termed as singular value decomposition. It is given by the formula

$$A=USV^T \tag{4}$$

where, S is the singular value matrix, and U and V are orthogonal matrices, generally termed as left and right singular matrices respectively.

The properties of the singular value decomposition are (1) the singular values of the image matrix remain less altered when it is subjected to various attacks (2) also, the singular values of the image matrix depict intrinsic algebraic characteristics which shows that SVD can be used in image processing methods.

The spectral decomposition based on SVD can be considered as bidiagonal SVD. The singular values obtained using BSVD are similar to SVD, although the method of calculating BSVD and SVD are different. The BSVD is calculated by bidiagonalizing A, and subsequently taking SVD on the upper bidiagonal values, as shown below:

$$A = P_A \, B \, Q_A^T \tag{5}$$

where, A is an orthonormal matrix, P_A and Q_A are unitary matrices and B is the upper bidiagonal matrix.

$$B = P_B S Q_B^T \quad (6)$$

where, P_B and Q_B are unitary matrices and S is the singular values of the matrix.

The calculation of SVD, which uses iterative schemes to calculate the singular values, differs from that of BSVD, where it uses finite operations. The performance of BSVD is better than SVD [Deift, Demmel and Tomei (1991)].

2.4 Arnold cat map

Arnold Cat Map (ACM), named after Vladimir Arnold, is a chaotic map. Arnold's cat map is the transformation

$$\Gamma : T^2 \to T^2 \quad (7)$$

given by the formula

$$\Gamma : (x, y) \to (2x + y, x + y) \bmod 2 \quad (8)$$

where x, $y \in \{0,1,2 \ldots,n-1\}$ and n is the size of the image.

When the image is encrypted using Arnold cat map, the original image is obtained back, after N number of times, and N is called the period of the function [Chen, Wong, Liao et al. (2013)].

3 Proposed scheme

3.1 Watermark embedding

Let the cover image of size M×N be denoted by *I* and the grayscale watermark logo image of size $M_1 \times N_1$ be represented by *W*, the steps for embedding the watermark are given below:

1. The watermark image W, scrambled and encrypted using the Arnold transformation is divided into two parts: W_1 and W_2.
2. Apply *n*-level discrete wavelet transform on the cover image *I* to obtain the following four sub-bands LL_n, LH_n, HL_n, HH_n. Of these, HL_n and HH_n are considered for embedding the watermark. In the proposed method, the host image is decomposed up to 3 levels, i.e. *n*=3 levels.

   $[LL_3, LH_3, HL_3, HH_3]$=DWT (I);
3. Perform Z-Transformation on the sub-band HL_3.

   I_1=ZT (HL_3);
4. Apply BSVD on the Z-transformed sub-band of the cover image. The watermark is embedded by modifying the singular values of sub-band with the watermark image. The value of scaling factor (alpha) α is chosen in such a way that the robustness and the imperceptibility of the watermarked image are well adjusted. In this experiment, the value of alpha is taken as 0.2.

   I_1'=bsvd (I_1);

$I_1''=I_1'+\alpha\ W_1'$;

5. The inverse Z-transform is performed on the modified frequency sub-bands as follows:

   $HL_{31}=iZT\ (I_1'')$;

   Repeat Steps 2-5, for the sub-band HH_3 to embed the other half of the watermark. Apply the 3-level inverse DWT using the modified coefficients HL_{31} and HH_{31}, to generate the watermarked image I'.

   I'=3-level iDWT (LL_3, LH_3, HL_{31}, HH_{31});

3.2 Watermark extraction scheme

The watermark is extracted using the keys generated during the embedding process. The steps for extracting watermark are given below:

1. The watermarked image I' is decomposed into sub-bands by applying 3-level DWT

   $[LL_3, LH_3, HL_3, HH_3]$=DWT (I');

2. Z-transform is computed for the sub-band HL_3;

   $I'_1=ZT\ (HL_3)$;

3. Apply BSVD on I'_1 and calculate D_1 by subtracting the singular values from the keys generated during the embedding process and dividing the values by the scaling factor (alpha) α as follows:

   $[U_7, S_7, V_7]$=BSVD (I'_1);

   $D_1=(S_7–key_1)/alpha$;

4. The above steps are repeated for the sub-band HH_3 to compute W_2', which is the second half of the watermark image. The values W_1' and W_2' are combined, and the watermark image is generated by applying Arnold Transformation.

   G=[W1' W2']; W=ACM2 (G)

   where, W is the extracted watermark.

4 Experimental results and analysis

Watermarking algorithms are generally evaluated in terms of imperceptibility and robustness. Imperceptibility is the measure of indistinguishable between the original and embedded images. In other words, there should not be any difference to view between the original and watermarked image. Robustness is the measure of a watermark to resist against intentional and random attacks.

Several experiments using image processing and geometric attacks were carried out to verify the invisibility and the robustness of the proposed watermarking scheme. The tests were conducted using MATLAB software on standard test images of size 512×512, namely Lena, Baboon, Barbara, Boat (Bridge), Peppers, Jetplane, Man (Pirate) and a logo grayscale image of size 64×64 is used as the watermark (shown in Fig. 1).

The invisibility of the proposed scheme was carried out by considering two parameters as follows:

4.1 Peak Signal Noise Ratio (PSNR)

4.2 Structural Similarity Index (SSIM)

The test images after embedding the watermark logo and the extracted watermark logo from each of the test images are shown in Fig. 5. The efficiency of the proposed method is evaluated by computing PSNR, SSIM, Image Fidelity, Entropy and CC.

(a) (g) (m) (s)

(b) (h) (n) (t)

(c) (i) (o) (u)

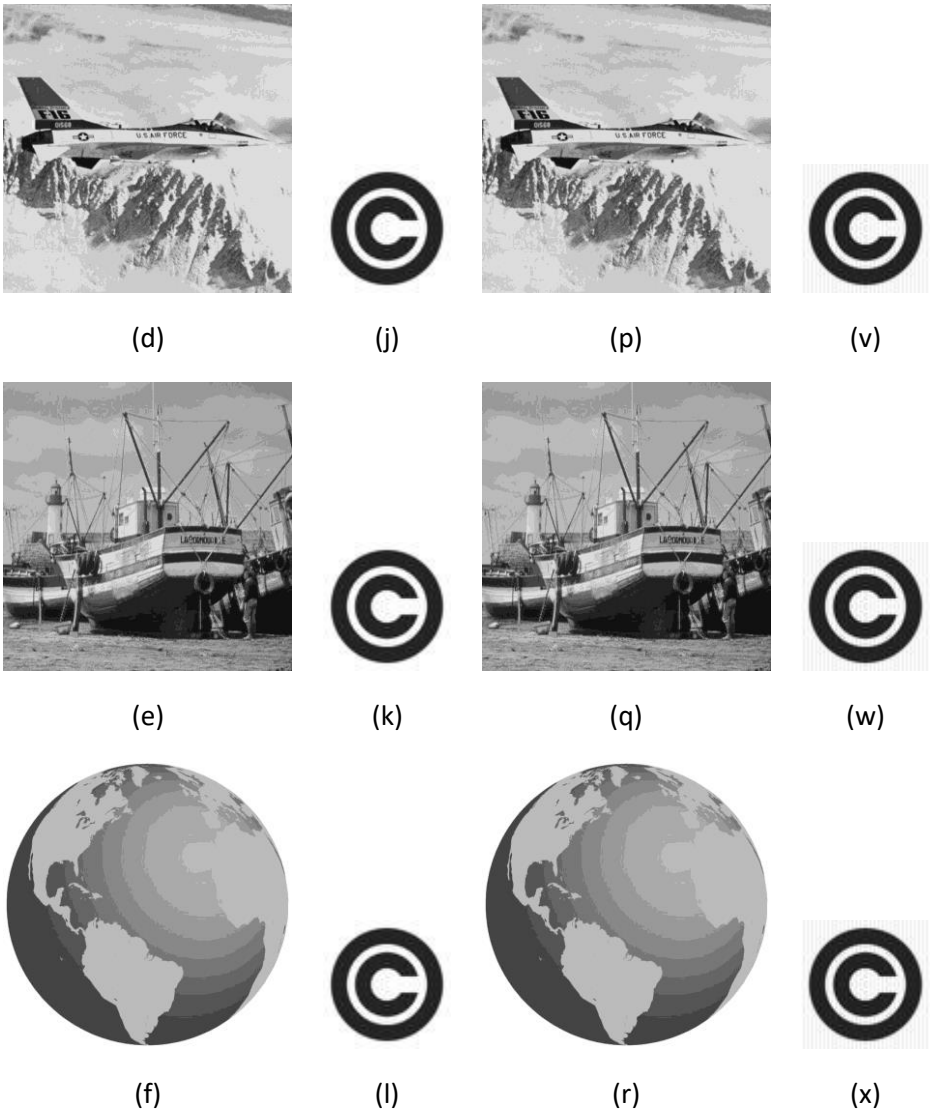

Figure 1: (a-f) original host images; (g-l) original watermark images (m-r) watermarked host images (s-x) extracted watermark images

Table 1: PSNR Values obtained (without attacks)

IMAGE NAME	Lena	Peppers	Jetplane	Elaine	Houses	Boat	Globe
PSNR	71.7109	72.6763	68.8925	71.0227	72.4207	70.9076	69.0419

Table 2: Comparison of PSNR values of the proposed scheme with different schemes

IMAGE NAME	Proposed	Makbol T=0.002	Lai & Tsai T=0.002	Ansari
Lena	71.7109	61.31	61.69	52.34
Peppers	72.6763	57.94	56.20	53.21

4.3 Robustness to attacks

The robustness of the proposed scheme was evaluated by applying various image processing attacks which includes common image processing attacks such as Gaussian noise, salt & pepper noise, Average filtering, median filtering, Blurring, Histogram Equalization, Gamma Correction and geometric distortions like scaling and rotation.

4.3.1 Filtering attacks

The most common signal processing attack is filtering. The watermark is extracted from the watermarked images after applying average and median filters of sizes: 3×3, 5×5, and 13×13. The results are shown in Fig. 2.

Average Filtering 3×3

Average Filtering 5×5

Figure 2: Average and Median Filtering Attacks with 3×3 and 5×5 filters and the extracted watermarks

4.3.2 Noising attacks

Additive and multiplicative noise account for the transformation and the degradation of the images. It also results in degrading the watermark information during the extraction. In this experiment, the watermarked image is subjected to 100% salt and pepper noise and the extracted watermark in Fig. 3 shows the robustness of the proposed algorithm.

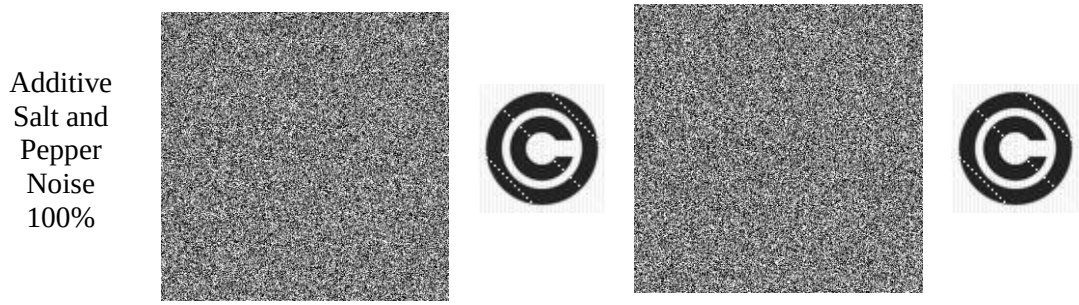

Figure 3: Watermarked images with 100% Additive Salt and Pepper Noise and the extracted watermark

4.3.3 Geometric attacks

Geometric transformations or attacks include flipping, rotation, cropping and scaling of images. Cropping of images is the most common geometric attack in real time situations. Cropping is done by removing a part of the image either by hiding or deleting the rows or

columns of the image. Much information is lost during this process. In this experiment, the image is cropped to 50% and the watermark is extracted as shown in Fig. 4.

The flipping of images generally does not result in loss of information. The vertically and horizontally flipped watermarked image and the extracted watermark is shown in Fig. 4.

Figure 4: Watermarked images subjected to horizontal flip attack and the extracted watermark

Rotating an image to a certain degree can result in loss of information, making the watermark nondetectable. Fig. 5 shows the watermark extracted, after rotating the watermarked image to 50°.

Figure 5: Watermarked images rotated to 50° and the extracted watermark

Scaling an image involves resizing the image to fit into the desired size. The image is enlarged or reduced, resulting in information loss of the embedded watermark. Two different scaling attacks are considered, and in the first case, the image is enlarged to 1024×1024 and it is again resized to its original size 512×512. Secondly, the image is reduced to 128×128 and brought back to 512×512. The attacked image and the extracted watermark images are shown in Fig. 6.

Figure 6: Watermarked images subjected to scaling and shearing and the extracted watermark

Shearing is also another form of generalised geometric transformation usually combined with scaling and rotation. The watermarked image subjected to shearing and the extracted watermark image is shown in Fig. 6.

4.3.4 JPEG compression

Another common attack or manipulation of images is the JPEG compression of images. The watermarked image is tested using different compression ratios and the watermark shown below is extracted from 80:1 as well as 10:1 compressed watermark image as shown in Fig. 7.

JPEG Q=80

Figure 7: Watermarked images with JPEG compression 10:1 and 80:1 ratio and the extracted watermark

4.3.5 Image-processing attacks

Some of the general image enhancement techniques or attacks include sharpening, histogram equalisation, gamma correction, and motion blur. For sharpening of images attack, the watermark image is sharpened by choosing two scaling factors, 0.2 and 0.9. Histogram equalisation is the intensity-level equalisation of the image, resulting in a higher contrast of the image. It increases or sometimes decreases the image contrast to obtain the histogram of uniform distribution. The results of gamma correction, image sharpening, histogram equalisation, and motion blur are shown in Fig. 8.

Gamma Correction (0.5)

Gamma Correction (0.9)

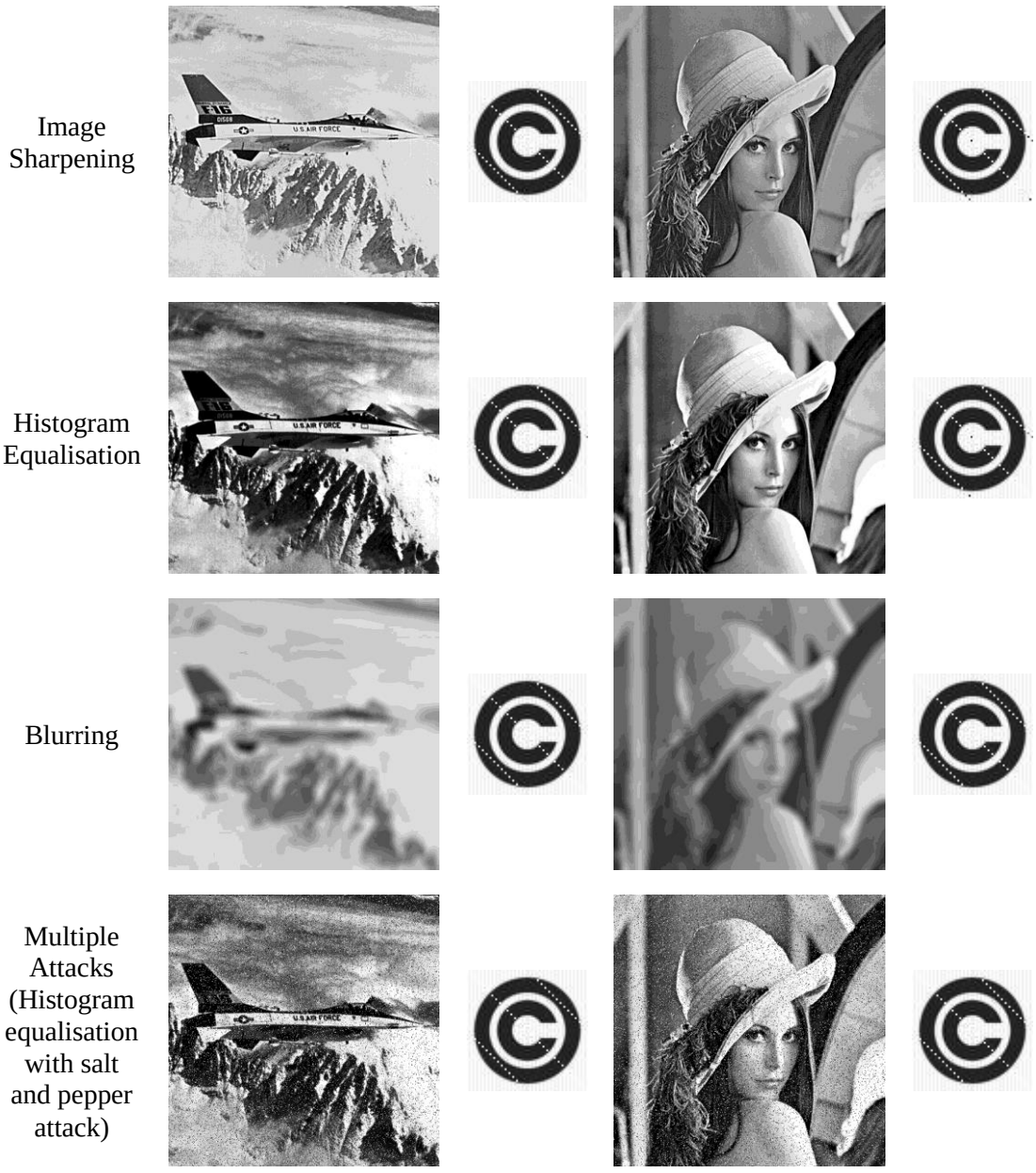

Figure 8: Watermarked images under different image processing attacks and the extracted watermark

The watermarked images are subjected to various image processing attacks, and the watermark is extracted from the attacked image. The correlation coefficients of the original watermark and the extracted watermark are calculated for each attack to verify the ability of the proposed scheme to withstand intentional and non-intentional attacks. Tab. 2 gives the

correlation coefficient of all extracted watermarks after the watermarked images are subjected to various kinds of attacks.

4.3.5 False positive attacks

The proposed scheme overcomes the false positive problem by (1) embedding a scrambled watermark (using the Arnold transformation), and (2) the scrambled watermark is divided into two halves and embedded in two different coefficients of the host image. The extracted watermark requires the valid keys and the parameters of the Arnold transformation. From the Fig. 9, it can be seen that the watermark can be extracted with the valid keys and the parameters whereas the watermark cannot be extracted when invalid keys or parameters are provided.

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

Figure 9: (a) original image, (b) watermarked image, (c) original watermark (d) extracted watermark using correct keys, (e) extracted watermark using the wrong keys

Table 3: Correlation coefficients of the original and the extracted watermark

ATTACK NAME	Lena	Peppers	Jetplane	Elaine	Houses	Boat	Globe
Additive White Gaussian Noise 75%	0.9985	0.9984	0.9985	0.9986	0.9985	0.9984	0.9986
Average 13×13	0.9793	0.9795	0.9805	0.9809	0.9791	0.9787	0.9792
Blurring	0.9795	0.9778	0.9785	0.9785	0.9790	0.9787	0.9794
Centre Cropping	0.9868	0.9870	0.9911	0.9891	0.9888	0.9857	0.9903
Contrast Adjustment	0.9789	0.9790	0.9788	0.9790	0.9790	0.9790	0.9790
Cropping All Sides	0.9780	0.9784	0.9766	0.9748	0.9764	0.9767	0.9799
Flipping Horizontal	0.9802	0.9778	0.9812	0.9790	0.9805	0.9773	0.9790

Flipping Vertical	0.9872	0.9840	0.9811	0.9853	0.9848	0.9844	0.9855
Gamma Correction 0.6	0.9795	0.9868	0.9790	0.9794	0.9790	0.9790	0.9790
Gamma Correction 0.8	0.9883	0.9876	0.9796	0.9825	0.9824	0.9811	0.9794
Gaussian Low Pass Filter 5	0.9823	0.9833	0.9838	0.9863	0.9833	0.9822	0.9826
Gaussian Noise 0.1	0.9790	0.9787	0.9790	0.9790	0.9790	0.9790	0.9790
Gaussian Noise 0.05	0.9793	0.9827	0.9809	0.9775	0.9812	0.9775	0.9830
Histogram Equalisation	0.9777	0.9777	0.9789	0.9786	0.9783	0.9790	0.9782
Image Sharpening 0.2	0.9917	0.9952	0.9907	0.9955	0.9920	0.9914	0.9929
Image Sharpening 0.9	0.9802	0.9770	0.9798	0.9822	0.9794	0.9793	0.9797
JPEG Compression Q=10	0.9852	0.9845	0.9881	0.9793	0.9826	0.9804	0.9862
JPEG Compression Q=80	0.9961	0.9964	0.9970	0.9957	0.9955	0.9975	0.9972
Log Transformation	0.9809	0.9820	0.9832	0.9852	0.9809	0.9806	0.9892
Median Filtering 5×5	0.9790	0.9801	0.9795	0.9798	0.9790	0.9790	0.9842
Motion Blur 20,45	0.9780	0.9784	0.9766	0.9748	0.9764	0.9767	0.9799
Multiple Attacks - HistEq_SPNoise01	0.9846	0.9891	0.9902	0.9815	0.9851	0.9837	0.9881
Resizing 512-1024-512	0.9967	0.9974	0.9979	0.9957	0.9942	0.9963	0.9968
Resizing 512-256-512	0.9822	0.9833	0.9840	0.9853	0.9822	0.9812	0.9827
Rotation Anticlockwise 50 Degrees	0.9813	0.9797	0.9790	0.9782	0.9790	0.9790	0.9801
Rotation Clockwise 50 Degrees	0.9806	0.9790	0.9790	0.9787	0.9782	0.9790	0.9803
Salt and Pepper Noise 0.1	0.9846	0.9901	0.9903	0.9920	0.9901	0.9910	0.9897

Salt and Pepper Noise 100%	0.9790	0.9790	0.9790	0.9790	0.9790	0.9790	0.9790
Shearing 1,2	0.9800	0.9779	0.9790	0.9787	0.9829	0.9790	0.9790
Speckle Noise 0.001	0.9905	0.9914	0.9869	0.9881	0.9909	0.9882	0.9908
Speckle Noise 0.01	0.9811	0.9779	0.9784	0.9775	0.9735	0.9774	0.9803

Tab. 3 shows reasonably good CC values against all the signal processing attacks and geometric distortions considered for evaluating the robustness of the proposed algorithm.

All these experimental results suggest that the proposed method is extremely robust against common signal processing attacks and geometric distortions.

Comparative study of the correlation coefficient values of the proposed method and the method proposed by Singh et al. [Singh and Singh (2017)] (Tab. 4), Lai et al. [Lai and Tsai (2010)] (Tab. 5), Bhatnagar et al. [Bhatnagar and Raman (2009)] (Tab. 6), and Makbol et al. [Makbol, Khoo and Rassem (2016)] (Tab. 7) are given in Tabs. 4-7. It can be seen that the proposed scheme performs better under various image processing attacks and geometric distortions considered as well as in JPEG compression.

Table 4: Comparison of the correlation coefficients for Bhatnagar et al. [Bhatnagar and Raman (2009)] and the proposed method

Kind of Attack	Singh	Proposed
Average filtering attack 13×13	0.8736	0.9793
Median filtering 9×9	0.9075	0.9636
Motion blur	0.7682	0.9785
Histogram equalisation	0.8472	0.9777
JPEG compression70	0.9724	0.9954
Cropping 50%	0.9768	0.9868
Sharpen (by factor 100)	0.8616	0.9762
Log Transformation	0.8506	0.9809
Scaling $1\rightarrow1/2\rightarrow1$	0.8976	0.9812
Gamma Correction γ=0.6	0.9230	0.9795
Speckle noise σ=0.1	0.8943	0.9785
Gaussian noise σ=0.1	0.9636	0.9790

The correlation coefficient of the extracted watermark is also compared with the method proposed by Lai et al. [Lai and Tsai (2010)], as given in Tab. 4 below:

Table 5: Comparison of correlation coefficients for Lai et al. [Lai and Tsai (2010)], and the proposed method

KIND OF ATTACK		Cropping (all sides)	Rotation (50°)	Gaussian noise (0.001)	Average filtering (3×3)
[Lai and Tsai, (2010)]	Best	0.9840	0.9900	0.9760	0.9600
	Average	0.9728	0.9772	0.9567	0.9500
Proposed	Best	0.9799	0.9806	0.983	0.9809
	Average	0.9733	0.9793	0.9803	0.9796
KIND OF ATTACK		JPEG compression (50%)	Histogram Equalisation	Contrast adjustment	Gamma correction (0.5)
[Lai and Tsai, (2010)]	Best	0.977	0.9890	0.9960	0.9990
	Average	0.9658	0.9862	0.9930	0.9957
Proposed	Best	0.9949	0.9790	0.9790	0.9865
	Average	0.9916	0.9784	0.9790	0.9801

Table 6: Comparison of correlation coefficients for Bhatnagar et al. [Bhatnagar and Raman (2009)], and the proposed method

Scheme	Average filtering attack (13×13)	Median filtering (13×13)	Motion blur (10, 15)	Rotation (50° Clockwise)	Histogram equalisation
Proposed	0.9795	0.9790	0.9778	0.9806	0.9777
Bhatnagar	-0.3696	-0.3233	-0.3280	0.3309	0.8620
Scheme	Cropping ((1/4) th area remaining	Sharpen (by factor 100)	Contrast adjustment (50% increased)	Scaling 512→128→512	JPEG compression 80%
Proposed	0.9784	0.9783	0.9789	0.9711	0.9964
Bhatnagar	0.3840	0.6784	0.7557	0.5648	0.9922

Table 7: Comparison of Correlation Coefficients for Makbol et al. [Makbol, Khoo and Rassem (2016)] and the proposed method

Scheme	Contrast Adjustment	Average filtering (13×13)	Centered cropping (50)	Gaussian noise (3%)	Gaussian noise (0.001)
Makbol	0.9932	0.9672	0.9199	0.9053	0.8027
Proposed	0.9789	0.9793	0.9868	0.9824	0.9782
	Jpeg compression (70%)	Jpeg compression (10%)	Jpeg compression (30%)	Histogram Equalisation	Rotation (50°)
Makbol	1.0000	0.3584	0.9521	0.9922	0.4258
Proposed	0.9954	0.9852	0.9868	0.9777	0.9806
	Rotation (50° anti-clockwise)	Sharpening (by factor 100)	Median filter (3×3)	Median filter (5×5)	Shearing (1, 0.2)
Makbol	0.4619	1.0000	0.9951	0.7041	0.5098
Proposed	0.9813	0.9762	0.9809	0.979	0.98
	Speckle Noise Attack (0.01)	Salt and pepper attack (0.001)	Salt and pepper attack (0.01)	Scaling (0.25)	Scaling (0.5)
Makbol	0.8555	0.9971	0.9521	0.8076	0.998
Proposed	0.9811	0.9846	0.978	0.979	0.9822

Table 8: Comparison of correlation coefficients for DWT-SVD and firefly algorithm [Mishra, Agarwal, Sharma et al. (2014)] and the proposed method

Scheme	Image	Gaussian Filter (3×3)	Sharpening (0.2)	Histogram Equalisation
Proposed	Lena	0.982	0.992	0.977
	Pepper	0.983	0.996	0.978
[Mishra, Agarwal, Sharma et al. (2014)]	Lena	0.97	0.991	0.991
	Pepper	0.965	0.849	0.995
Scheme	Image	Scaling (2)	Cropping (1/8)	Salt and pepper noise (5%)
Proposed	Lena	0.997	0.979	0.98
	Pepper	0.998	0.978	0.988
[Mishra, Agarwal, Sharma et al. (2014)]	Lena	0.997	0.421	0.7
	Pepper	1	0.188	0.609

The comparative study of the proposed method with previously reported schemes based on DWT-SVD techniques provided in Tabs. 4-7 shows the proposed scheme combining DWT-ZT-BSVD gives better results.

The proposed scheme is also compared with the scheme proposed by Mishra et al. [Mishra, Agarwal, Sharma et al. (2014)] which is an optimized image watermarking algorithm using DWT-SVD and Firefly algorithm. In their experiment, the authors used two different scaling factors viz. SSF (Single Scaling Factor) and MSF (Multiple Scaling Factor). The proposed method implements a single scaling factor and hence, compared with the correlation coefficient of SSF proposed by Mishra et al. [Mishra, Agarwal, Sharma et al. (2014)]. The comparative results are given in Tab. 8.

5 Conclusion

In this paper, a chaos-based hybrid image watermarking technique has been proposed, based on DWT, Z-transform and BSVD. The scheme combines the benefits of DWT, ZT, BSVD and the chaotic map. Z-transform can efficiently analyze high resolution and narrow frequency spectrum bands, and it has better data hiding properties. The zeros of the Z-transform are very sensitive to minute changes in the pixel values. Hence it is widely employed in fragile watermarking and image authentication applications. The proposed algorithm combines the properties of Z-transform with the widely-adopted DWT to design a robust watermarking scheme. This algorithm concurrently utilizes two sub-bands of the DWT decomposition viz., HL and the HH. The scrambled watermark is divided into two equal blocks, and they are separately embedded into the HL and HH sub-bands, thereby enhancing the robustness. The watermark is embedded in singular values of the bidiagonal SVD, which gives better performance than implementing SVD[21]. Further, the use of Arnold-Cat map for scrambling of the watermark image before embedding improves the security as the extracted image need to be decrypted correctly to obtain the watermark. Experiments were conducted using standard test images, and the results were analysed for imperceptibility and robustness. The PSNR, CC, Entropy, Image Fidelity and SSIM values of the experiments show that the proposed scheme is more secure and robust.

References

Ansari, I. A.; Pant, M.; Ahn, C. W. (2016): Robust and false positive free watermarking in IWT domain using SVD and ABC. *Engineering Applications of Artificial Intelligence*, vol. 49, pp. 114-125.

Bhatnagar, G.; Raman, B. (2009): A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 1002-1013.

Bhatnagar, G.; Wu, Q. M. J.; Raman, B. (2012): A new robust adjustable logo watermarking scheme. *Computers & Security*, vol. 31, no. 1, pp. 40-58.

Chen, F.; Wong, K. W.; Liao, X.; Xiang, T. (2013): Period distribution of the generalized discrete Arnold cat map for $N=2^e$. *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3249-3255.

Cox, I. J.; Kilian, J.; Leighton, F. T.; Shamoon, T. (1997): Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687.

Deift, P.; Demmel, J.; Li, L.; Tomei, C. (1991): The bidiagonal singular value decomposition and Hamiltonian mechanics. *SIAM Journal on Numerical Analysis*, vol. 28, no. 5, pp. 1463-1516.

Fazli, S.; Moeini, M. (2016): A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik-International Journal for Light and Electron Optics*, vol. 127, no. 2, pp. 964-972.

Ho, A. T. S.; Zhu, X.; Shen, J. (2004): Authentication of biomedical images based on zero location watermarking. *ICARCV 2004 8th Control, Automation, Robotics and Vision Conference*, vol. 2, pp. 973-976.

Ho, A. T. S.; Zhu, X.; Shen, J.; Marziliano, P. (2008): Fragile watermarking based on encoding of the zeroes of the Z-transform. *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 567-569.

Jayashree, N.; Bhuvaneswaran, R. S. (2016): Z-transform based digital image watermarking scheme with DWT and chaos. *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, pp. 289-297.

Khan, M. S.; Boda, R.; Bhukya, V. V. (2012): A copyright protection scheme and tamper detection using Z-transform. *International Journal Computers, Electrical and Advanced Communications Engineering*, vol. 1, no. 1, pp. 119-124.

Lai, C. C.; Tsai, C. C. (2010): Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060-3063.

Ling, H. C.; Phan, R. C. W.; Heng, S. H. (2013): Comment on "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition". *AEU-International Journal of Electronics and Communications*, vol. 67, no. 10, pp. 894-897.

Makbol, N. M.; Khoo, B. E.; Rassem, T. H. (2016): Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, vol. 10, no. 1, pp. 34-52.

Makbol, N. M.; Khoo, B. E.; Rassem, T. H. (2018): Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26845-26879.

Mandal, J. K. (2012): A frequency domain steganography using Z transform (FDSZT). *International Workshop on Embedded Computing and Communication System.*

Mishra, A.; Agarwal, C.; Sharma, A.; Bedi, P. (2014): Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm. *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858-7867.

Rabiner, L. R.; Schafer, R. W.; Rader, C. M. (1969): The chirp z-transform algorithm and its application. *Bell System Technical Journal*, vol. 48, no. 5, pp. 1249-1292.

Saxena, H.; Saxena, P.; Rastogi, S. (2014): DWT-DCT-SVD based semi-blind reference image watermarking scheme using trigonometric function. *International Journal of Conceptions on Computing and Information Technology*, vol. 2, no. 2, pp. 14-18.

Shi, H. (2014): DWT and SVD based watermarking scheme with circulation. *Journal of Software*, vol. 9, no. 3, pp. 655-662.

Sifuzzaman, M.; R. Islam, M.; Ali, M. (2009): Application of wavelet transform and its advantages compared to fourier transform. *Journal of Physical Sciences*, vol. 13, pp. 121-134.

Singh, D.; Singh, S. K. (2017): DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13001-13024.

Stillings, S. (1972): *A Study of the Chirp Z-Transform Algorithm and Its Applications*. Kansas State University, Manhattan, KS.

Sverdlov, A.; Dexter, S.; Eskicioglu, A. M. (2005): Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies. *13th European Signal Processing Conference*, pp. 1-4.

Takaya, K.; Ma, T.; Shimizu, K.; Kitama, M.; Mikami, T. (1990): Application of image reconstruction by means of chirp z-transform. *IAPR Workshop on Machine Vision Applications*, pp. 77-80.

Vich, R. (1987): *Z Transform Theory and Applications*. Springer, Netherlands.

Xing, Y.; Tan, J. (2010): Mistakes in the paper entitled "A singular-value decomposition-based image watermarking using genetic algorithm". *AEU-International Journal of Electronics and Communications*, vol. 64, no. 1, pp. 80-81.