



Efficient hybrid digital image watermarking

Amany F. Eldaoushy¹ · Moawad I. Desouky¹ ·
Sami A. El-Dolil¹ · Adel S. El-Fishawy¹ ·
Fathi E. Abd El-Samie^{1,2}

Received: 8 December 2022 / Accepted: 22 February 2023 / Published online: 17 June 2023
© The Author(s) 2023

Abstract Nowadays, multimedia security is a major issue. Images, video, audio, and text files lose credibility in most times, because they face several attacks related to illegal distribution, duplication, and manipulation of the information conveyed by them. Digital watermarking is an important tool for protecting digital content. This paper introduces an efficient hybrid digital image watermarking scheme. It consists of two stages of Singular Value Decomposition (SVD). The first one is the embedding stage, which is performed by using SVD followed by block-based SVD (B-SVD). The second stage is the extraction stage, which depends on the SVD on the whole image and then B-SVD to get the original watermarks. In this scheme, the watermarking requirements are satisfied, while capacity is increased. Furthermore, watermark detection, robustness, and security are improved. The performance of the proposed scheme is evaluated by the correlation coefficient C_r between the original and extracted watermarks, and the Peak Signal-to-Noise Ratio ($PSNR$) between the original and watermarked images. The experimental results demonstrate that the proposed scheme has a good performance, where C_r reaches 0.9975 and $PSNR$ reaches 45.8605. It is more secure than the previous schemes, when subjected to attacks. In addition, the proposed scheme is compared to the most recent schemes, revealing its superiority.

Keywords Digital watermarking · SVD · Block-based SVD

Introduction

Today, the Internet is the most important and easiest way to connect people all over the world. It allows users to communicate and share multimedia content, such as text, images, audio, and video, with low cost and high quality. However, the most important problem that arises is how to protect critical data during transmission from illegal use [1, 2]. Protecting confidential information is a moral and legal requirement. Data hiding is a method for protecting information by hiding it in a multimedia object for the authentication purpose. This process is carried out in such a way that the embedded data is not visible to the naked eye, but it is easily detected by a detector. Data hiding has two main types: digital watermarking and steganography [3, 4]. The insertion of a part of information into the multimedia content, where it is not visible to the human eye but can be detected with a detector, is called digital watermarking. Figure 1 introduces the watermarking framework, which consists of the embedding and detection processes. It is suitable for several applications such as fingerprinting, copyright protection, and content authentication, because it has a very important feature that the content is inseparable from the watermark [5, 6].

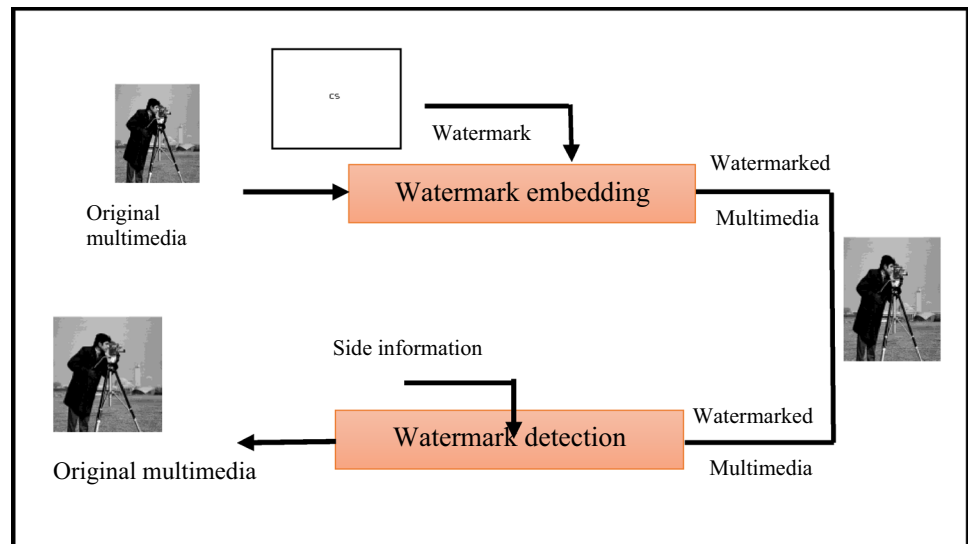
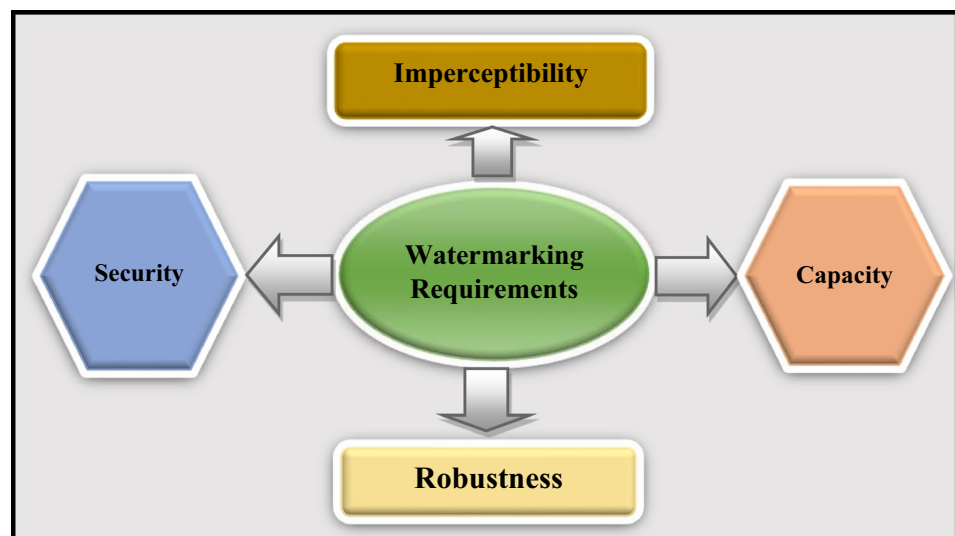
Digital watermarking techniques include embedding of a watermark in a multimedia content to ensure authenticity and protect copyright holders from unauthorized data alteration [7]. Consequently, it is vital to specify the prerequisites or properties of a watermarking scheme. The specifications for watermarking schemes are shown in Fig. 2.

These requirements guarantee the effectiveness of watermarking schemes. The ideal characteristics of digital

✉ Amany F. Eldaoushy
amanybas@yahoo.com

¹ Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Minufya, Egypt

² Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Fig. 1 Watermarking system**Fig. 2** Image watermarking requirements

watermarking include imperceptibility, robustness, capacity, and security [8, 9].

1. **Imperceptibility:** Imperceptibility is crucial, when assessing the watermarking scheme effectiveness. It is reflected in faithfulness and invisibility. The watermarked image in this instance needs to look exactly like the original image [10].
2. **Robustness:** Robustness is the property that a watermark must have to be detectable after various typical signal-processing operations used in digital image watermarking systems have been applied. Among them are spatial filtering, color mapping, scanning and printing, compression, scaling, translation, and rotation [10].
3. **Capacity:** The amount of embedded data in the host signal should be as large as possible.

4. **Security:** The authorized person is the only one, who can detect the watermark.

Consequently, Fig. 2 summarizes the general requirements for a digital watermarking scheme [9].

The motivation of this paper is introducing an efficient image watermarking scheme for different applications. This scheme depends on two cascaded stages of the SVD and B-SVD. It achieves a trade-off between the watermarking requirements, where embedding of more than one watermark increases capacity, robustness, and imperceptibility. Furthermore, the security is improved through the scheme complexity.

The paper organization is as follows. Section "[Traditional singular value decomposition \(SVD\) watermarking](#)" gives an explanation of the traditional SVD watermarking with

the method of Liu. Section "The block-based SVD (B-SVD) watermarking algorithm" presents the B-SVD watermarking algorithm. Section "Obtain the SVs of each (Swi matrix) by applying SVD on each Di matrix." presents an explanation of the proposed watermarking scheme. Section "The watermarked blocks in the spatial domain will be built by using the SVs of each Di matrix (Swi matrix)." shows the experimental results. Finally, Section 6 provides the conclusion.

Traditional singular value decomposition (SVD) watermarking

In the traditional method of Liu for SVD watermarking, a matrix is decomposed into three matrices. A matrix \mathbf{B} can be decomposed into a product of three matrices as follows [12]:

$$\mathbf{B} = \mathbf{X}\mathbf{S}\mathbf{Y}^T \quad (1)$$

where \mathbf{X} and \mathbf{Y} are orthogonal matrices, such that $\mathbf{X}^T \mathbf{X} = \mathbf{I}$, and $\mathbf{Y}^T \mathbf{Y} = \mathbf{I}$, and \mathbf{I} is an identity matrix. \mathbf{S} is a diagonal matrix, where its diagonal elements are the singular values of \mathbf{B} .

From the perspective of image processing, the traditional SVD method of Liu is a mathematical technique with the following main properties:

- Image Singular Values (SVs) have good stability, which means that even if a small change is made to an image, its SVs do not change noticeably, making the method resistant to various attacks.
- The image algebraic properties can be represented by its SVs.

Using these properties of the SVs of an image, the watermark can be settled into this matrix without great

variations in the watermarked image. Liu et al. [9] introduced a watermarking algorithm based on the spatial SVD. Recently, watermarking schemes based on the SVD have gained popularity due to their simplicity of implementation and the attractive mathematical features of the SVD.

Figure 3 presents the traditional method of Liu et al. [13], and the steps of the watermark embedding process are explained as follows:

The original image (\mathbf{B} matrix) is decomposed with the SVD.

$$\mathbf{B} = \mathbf{X}\mathbf{S}\mathbf{Y}^T \quad (2)$$

The matrix \mathbf{D} can be obtained by adding the watermark (\mathbf{W} matrix) to the SVs of the original matrix.

$$\mathbf{D} = \mathbf{S} + \mathbf{K}\mathbf{W} \quad (3)$$

The new modified matrix (\mathbf{D}) is decomposed with SVD.

$$\mathbf{D} = \mathbf{X}_w \mathbf{S}_w \mathbf{Y}_w^T \quad (4)$$

By knowing the obtained matrix (\mathbf{S}_w), the watermarked image can be obtained.

$$\mathbf{B}_w = \mathbf{X} \mathbf{S}_w \mathbf{Y}^T \quad (5)$$

With \mathbf{X}_w , \mathbf{S}_w , and \mathbf{Y}_w matrices and the potentially distorted image \mathbf{B}_w^* , the corrupted watermark is extracted from the potentially-corrupted watermarked image, and it is presented as follows:

- The corrupted watermarked image (\mathbf{B}_w^* matrix) is decomposed with SVD.

$$\mathbf{B}_w^* = \mathbf{X}_w^* \mathbf{S}_w^* \mathbf{Y}_w^{*T} \quad (6)$$

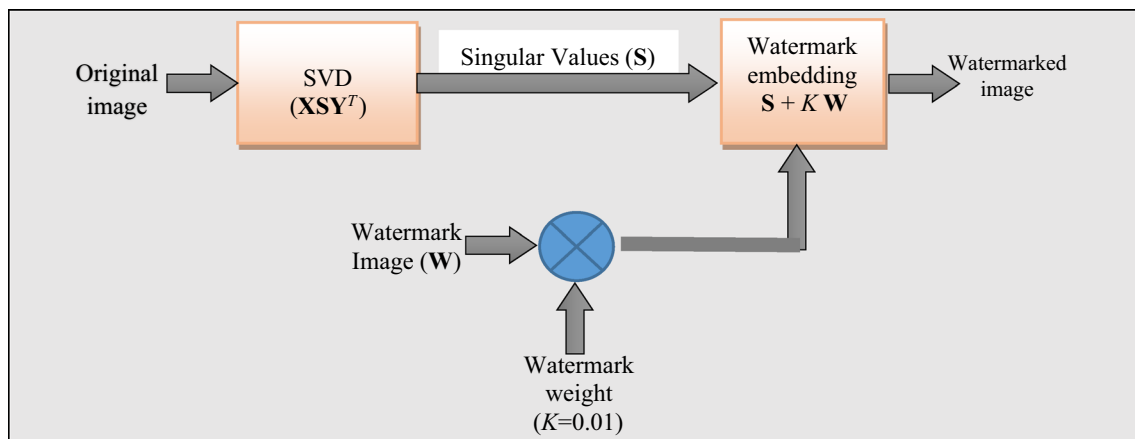


Fig. 3 Mathematical SVD

2. By knowing \mathbf{X}_w and \mathbf{Y}_w^T , the matrix \mathbf{D}^* can be obtained.

$$\mathbf{D}^* = \mathbf{X}_w \mathbf{S}_w^* \mathbf{Y}_w^T \quad (7)$$

3. Using the \mathbf{D}^* and \mathbf{S} matrices, the watermark is obtained.

$$\mathbf{W}^* = (\mathbf{D}^* - \mathbf{S}) / K \quad (8)$$

where K is the watermark gain and the corruption caused by the attacks is denoted by the symbol $*$.

Block-based SVD (B-SVD) watermarking

To give the chance for embedding of more watermarks to override attacks, the B-SVD watermarking is used. The original image is divided into non-overlapping blocks before embedding the watermark in the SVs of each block, separately [14, 15].

Watermark embedding

The steps of B-SVD watermarking are presented as follows. First, the original image (\mathbf{G} matrix) is segmented into several blocks, none of which overlapping with others. The new matrices are obtained by inserting the watermark into the SVs (\mathbf{S} matrix) of each block. To get the \mathbf{S} matrices of the watermarked blocks, we apply an SVD to each of these new matrices. The watermarked image \mathbf{G}_w is built in the spatial domain. By rearranging the blocks again into one matrix of the same dimensions as the original image, the watermarked image is obtained.

The steps of the embedding process are explained as follows [14]:

1. The original image (\mathbf{G} matrix) is divided into non-overlapping blocks.
2. To obtain the SVs of the \mathbf{S}_i matrix of each block, the SVD is performed on each block \mathbf{C}_i matrix, where $i = 1, 2, 3, \dots, N$, and N is the number of blocks.

$$\mathbf{C}_i = \mathbf{X}_i \mathbf{S}_i \mathbf{Y}_i^T \quad (9)$$

3. The watermark image (\mathbf{W} matrix) is added to the \mathbf{S} matrix of each block, giving the new matrices \mathbf{D}_i .

$$\mathbf{D}_i = \mathbf{S}_i + K\mathbf{W} \quad (10)$$

4. The SVs of each (\mathbf{S}_{wi} matrix) are obtained by applying SVD on each \mathbf{D}_i matrix.

$$\mathbf{D}_i = \mathbf{X}_{wi} \mathbf{S}_{wi} \quad (11)$$

5. The watermarked blocks in the spatial domain are built using the SVs of each \mathbf{D}_i matrix (\mathbf{S}_{wi} matrix).

$$\mathbf{C}_{wi} = \mathbf{X}_i \mathbf{S}_{wi} \mathbf{Y}_i^T \quad (12)$$

6. The watermarked image in the time domain (\mathbf{G}_w matrix) is obtained by combining the watermarked blocks back into a single matrix.

Watermark detection

To get the watermark that may be corrupted, by knowing the \mathbf{X}_{wi} , \mathbf{Y}_{wi} , \mathbf{S}_i matrices, and the corrupted watermarked image \mathbf{G}_w^* , we apply the following steps [15].

1. Before applying the SVD, the corrupted watermarked image (\mathbf{G}_w^* matrix) is divided into the same-size blocks as in the embedding process.
2. The SVs of each one (\mathbf{S}_{wi}^* matrix) are obtained and the SVD is applied on each possibly-corrupted watermarked block (\mathbf{C}_{wi}^* matrix).

$$\mathbf{C}_{wi}^* = \mathbf{X}_{wi}^* \mathbf{S}_{wi}^* \mathbf{Y}_{wi}^{*T} \quad (13)$$

3. Using \mathbf{X}_{wi} , \mathbf{Y}_{wi} , and \mathbf{S}_{wi}^* matrices, the matrices that contain the watermark are obtained

$$\mathbf{D}_i^* = \mathbf{X}_{wi} \mathbf{S}_{wi}^* \mathbf{Y}_{wi}^T \quad (14)$$

$$(\mathbf{D}_i^* - \mathbf{S}_i) / K = \mathbf{W}_i^* \quad (15)$$

The proposed hybrid digital image watermarking scheme

The proposed scheme depends on two cascaded stages of the SVD and B-SVD. The suggested scheme aims to fulfill the following watermarking requirements:

1. Improving the level of security through the scheme complexity.
2. Maintaining imperceptibility by increasing the capacity of embedded information without affecting the quality of the original image.
3. Enhancement of the correlation coefficient (C_r) to increase watermarking robustness.
4. Increasing Peak Signal-to-Noise Ratio (P_{SNR}) of the watermarked image to enhance its fidelity by ensuring that the watermark is not noticeable to the human eye.

Basic idea

The proposed watermarking scheme consists of embedding and (detection/extraction) processes. Figure 4 shows the watermark embedding process, which consists of two stages. In the first stage, watermark 1 is embedded into the original image using the B-SVD algorithm to obtain the primary watermarked image. Then, watermark 2 is embedded into the primary watermarked image using the SVD watermarking algorithm in the second stage to obtain the final watermarked image. Figure 5 shows the detection/extraction process, which consists of two stages: first, the extracted watermark 1 is detected and extracted from the final watermarked image. Then, the extracted watermark 2 is extracted from the primary watermarked image in the second stage.

The scheme description

Embedding process

In the embedding process, we apply the B-SVD and the SVD algorithms, respectively as shown in Fig. 6.

1. First, the original image (\mathbf{A} matrix) is divided into non-overlapping blocks with the same size. The size of the block is chosen to be 16×16 as indicated in [19]. Then, the SVD is applied on each block (\mathbf{C}_i matrix) for obtaining the SVs (\mathbf{S}_i matrix) of each block, where $i = 1, 2, 3, \dots, N$ and N is the number of blocks.

$$\mathbf{C}_i = \mathbf{X}_i \mathbf{S}_i \mathbf{Y}_i^T \quad (16)$$

2. The watermark image (\mathbf{W}_1 matrix) is added to each block \mathbf{S} matrix.

$$\mathbf{D}_i = \mathbf{S}_i + K \mathbf{W}_1 \quad (17)$$

3. The SVD is applied on each \mathbf{D}_i matrix to obtain the SVs of each (\mathbf{S}_{wi} matrix).

$$\mathbf{D}_i = \mathbf{X}_{wi} \mathbf{S}_{wi} \mathbf{Y}_{wi}^T \quad (18)$$

4. The watermarked blocks in the spatial domain are built by using the SVs of each \mathbf{D}_i matrix (\mathbf{S}_{wi} matrix).

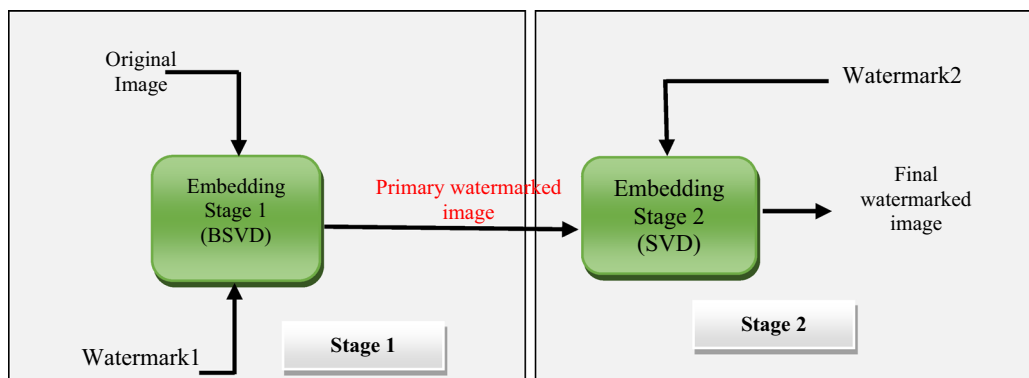


Fig. 4 Proposed algorithm (embedding stage)

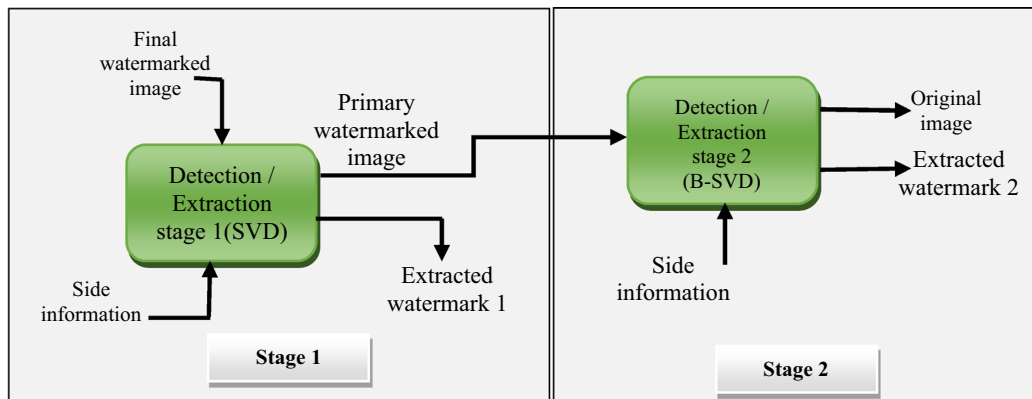
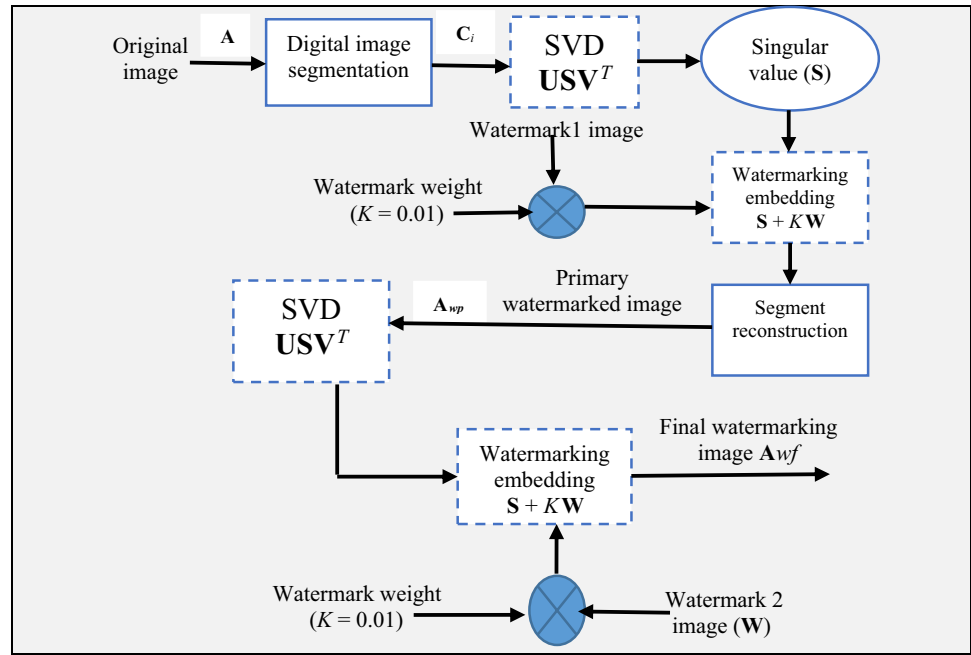


Fig. 5 Proposed algorithm (detection/extraction stage)

Fig. 6 The embedding block diagram of the proposed algorithm



$$C_{wi} = X_i S_{wi} Y_i^T \quad (19)$$

5. The watermarked image in the time domain (A_{wp} matrix) is built by combining the watermarked blocks back into one matrix.

From the previous steps, we get the primary watermarked image which will be the input for the second stage.

6. The SVD is applied on the primary watermarked image.

$$A_{wp} = X S_{wp} Y^T \quad (20)$$

7. To obtain the matrix D , the watermark (W_2 matrix) is added to the SVs of the primary watermarked matrix, then the SVD is applied

$$D = S_{wp} + K W_2 \quad (21)$$

$$D = X_w S_{wp} Y^T \quad (22)$$

8. Using the modified matrix (S_{wp}), the final watermarked image (A_{wf}) is obtained.

$$A_{wf} = X S_{wp} Y^T \quad (23)$$

(Extraction/Detection) Process

Figure 7 shows the watermarking (extraction/detection) process, which comprises application of the SVD and B-SVD watermarking algorithms, respectively. The new extraction process consists of several steps as follows:

The SVD is applied on the distorted final watermarked image (A_{wf}^* matrix).

$$A_{wf}^* = X^* S_{wf}^* Y^{*T} \quad (24)$$

The matrix which contains the watermark is computed.

$$D^* = X_{wf}^* S_{wf}^* Y_{wf}^{*T} \quad (25)$$

Using the matrix D^* and S_{wf}^* we get the watermark 2, which may be corrupted.

$$W_2^* = (D^* - S_{wf}^*)/K \quad (26)$$

The corruption due to attacks will be referred to as $*$.

To get the watermark that may be corrupted, by knowing X_{wi} , Y_{wi} , S_i matrices, and the possibly corrupted primary watermarked image A_{wp}^* , the steps below are applied.

The corrupted primary watermarked image (A_{wp}^*) is divided into blocks that have the same size as that in the embedding process.

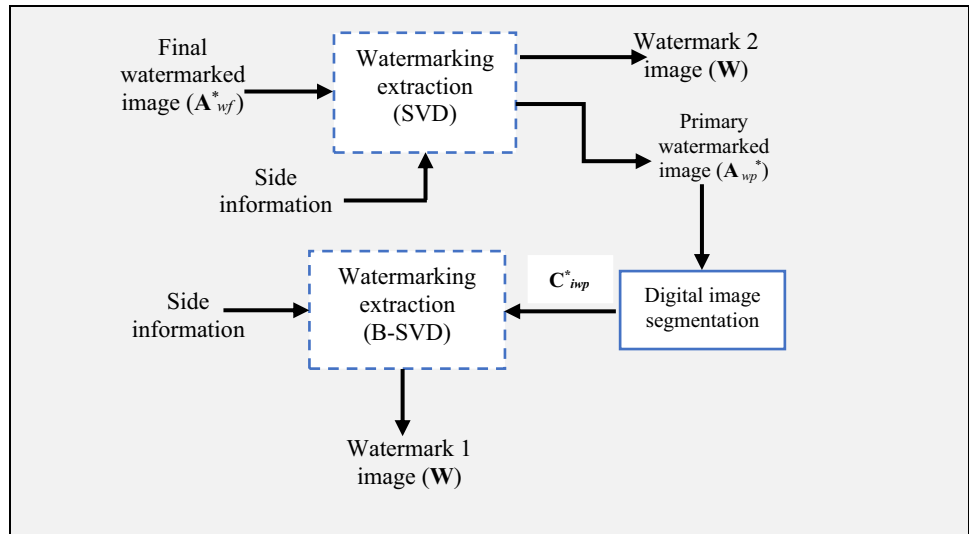
The SVs of each matrix (S_{wpi}^*) are obtained by applying SVD on each corrupted watermarked block (C_{wpi}^* matrix) to get

$$C_{wpi}^* = X_i^* S_{wpi}^* Y_i^{*T} \quad (27)$$

The X_{wi}^* , Y_{wi}^* , and S_{wi}^* matrices are used to obtain the D_i^* matrices that contain the watermark.

$$D_i^* = X_{wpi}^* S_{wpi}^* Y_{wpi}^{*T} \quad (28)$$

Fig. 7 (Detection/extract) block diagram for the proposed algorithm



From the \mathbf{D}_i^* matrices, the corrupted watermark 1 (\mathbf{W}_{1i}^*) is extracted.

$$(\mathbf{D}_i^* - \mathbf{S}_{wpi}) / K = \mathbf{W}_{1i}^* \quad (29)$$

Experimental results

Performance metrics

The performance evaluation for most work in watermarking techniques depends mainly on two image quality metrics [16, 17]:

1. Imperceptibility Quality Metric.

P_{SNR} is a metric used to describe the quality of a watermarked image. A large P_{SNR} is desirable. The P_{SNR} should be infinite, but this is not possible for a watermarked image. The mathematical representation of the P_{SNR} is given as:

$$P_{SNR} = 10 \log_{10} \left(\frac{255^2}{\frac{1}{N^2} \sum_{x,y} (A_w(x,y) - A(x,y))^2} \right) \quad (30)$$

where: $A(x,y)$ is the original image and $A_w(x,y)$ is the watermarked image.

2. Robustness Quality Metric:

The difference between the extracted and the original watermarks is measured by the correlation coefficient (C_r), which is a metric of resilience. The mathematical expression

of the C_r is shown below. The stronger the robustness, the closer the C_r value to one [17].

$$C_r(\mathbf{W}, \mathbf{W}') = \frac{\sum_y W(y)W'(y)}{\sqrt{\sum_y W^2(y) \sum_y W'^2(y)}} \quad (31)$$

where \mathbf{W} and \mathbf{W}' are the original and extracted watermarks, respectively.

Experimental result analysis

The performance of the proposed hybrid scheme is assessed in this section, along with that of the Liu et al. for a single watermark [13], the DWT-SVD with fused watermark [18], and the hybrid digital image watermarking scheme (SVD-BSVD).

The proposed hybrid digital image watermarking scheme (BSVD-SVD) is simulated using MATLAB on an Intel(R) Core(TM) i3 CPU with 2GB RAM, and several simulations are carried out. The used parameters in the simulations are summarized in Table 1.

To evaluate and illustrate the performance of the proposed algorithm, several test experiments are carried out for different original images with and without attacks. In each test, both the C_r of the extracted watermark and P_{SNR} of the watermarked images are measured.

Figures 8 and 9 show the variation of C_r and P_{SNR} with the gain factor of the watermark K . The figures indicate that the optimum value of K equals 0.01, where the best values of C_r and P_{SNR} are obtained. If the K is lower than 0.01, the C_r will decrease and the watermark cannot be successfully extracted. If K is larger than 0.01, P_{SNR} will decrease and the original image will be distorted.

Figure 10 shows the outcome of the Liu method with this sequence, 10 (a) is the original image, 10 (b) is the watermark of the same size as the original image, 10 (c) is the watermarked image, and 10 (d) is the extracted watermark without attacks. The correlation coefficient C_r between the

extracted watermark and the original one is 0.8543 in the case of using a single watermark.

The proposed algorithm BSVD-SVD simulation results in the embedding process and extraction process in the absence of attacks are shown in Fig 11 as follows: 11(a) is the original image, 11(b) is the watermark added to each block, 11(c)

Table 1 Specification of simulation parameter

Parameter	Specification
Original image	Camera man with size (256×256) & Different test images such as(rice, pout, Mandi, and peppers as a color image)
Watermark image	Copyright_big with size (256×256)
Block size	(16×16) [19]
Gain factor	$K=0.01$
Applied Attack	
Gaussian distribution noise	Zero mean and variance 0.01 (0, 0.01)
Blurring attack	LPF with window (3×3)
Cropping	50%
Rotating	30 degree

Fig. 8 Variation of the C_r of the watermarked image versus the watermark gain k

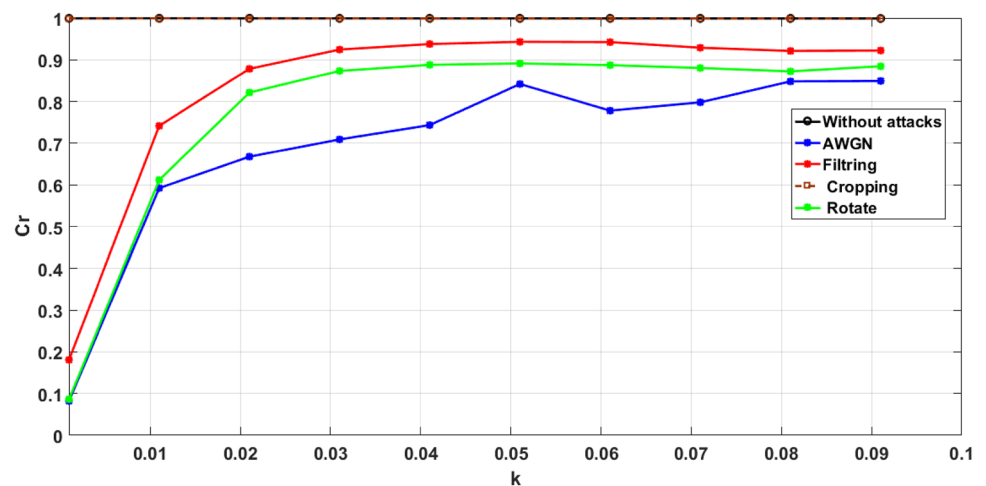
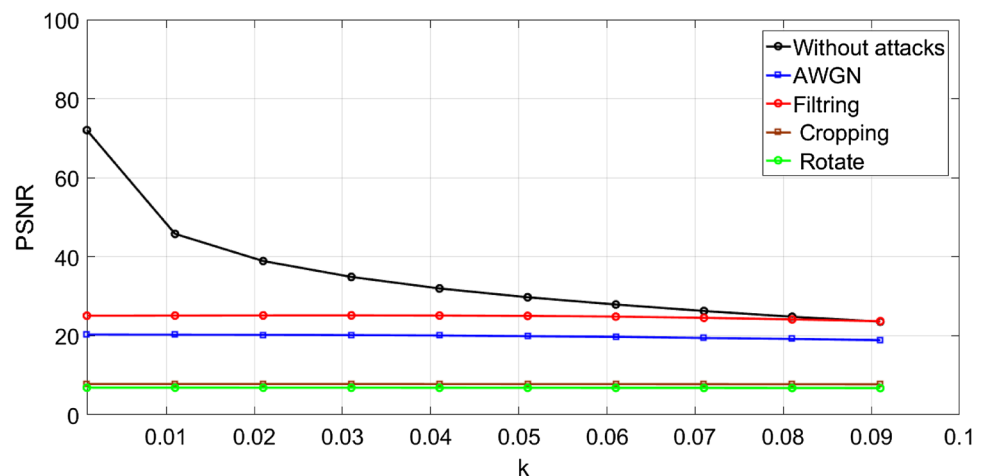


Fig. 9 Variation of the P_{SNR} of the watermarked image versus the watermark gain k



is the primary watermarked image using B-SVD, which gives $P_{SNR}=45.8605$ and 11(d) is the final watermarked image using BSVD-SVD, which gives $P_{SNR}=45.5193$. On the other hand, the extraction process has been completed. The extracted watermark1 from the final watermarked image by SVD has a C_{r2} equal to 0.0121, while the extracted watermark 1 (from BSVD) has a C_{rmax} of 0.9975, as shown in Fig. 11e,f, g. The proposed scheme gives a high correlation coefficient between the original watermark and the extracted watermark, closer to 1. According to the results, the proposed scheme extracts watermarks perfectly in the absence of attacks, increasing the capacity of embedded information.

The high fidelity of the proposed scheme is noticed, where there is no visual difference between the original image and the watermarked image. An improved level of security is achieved by increasing the scheme complexity. The proposed scheme is also tested on different original images, as shown in Fig. 12. From the behavior of the proposed schemes it is proved that it is not dependent on the type of image used as the original image. The correlation

coefficients for extracted watermarks are high and close to one in the absence of attacks. This means that the proposed scheme works efficiently with different original images.

As shown in Figs. 13 and 14, the Liu method and the proposed scheme were tested in the presence of some attacks, such as cropping with 50%, Gaussian noise with zero mean and 0.01 variance, and blurring with the LPF window of size 3×3 . Figs. 15 and 16 represent the extracted watermarks and their correlation coefficients between the original watermark and each extracted watermark for the method of Liu and the proposed scheme, respectively.

Table 2 gives the numerical values of correlation coefficient for different noise variances. The table indicates that there is a degradation in the correlation values with the increase in noise variance, in addition to the degradation in P_{SNR} due to the noise. Table 3 indicates the effect of increasing the filter window in blurring attack on the C_r and P_{SNR} . It is clear that increasing the filter window has a negative effect on the watermarking process. Rotation attack has a different effect on the watermarking process, where C_r and P_{SNR}

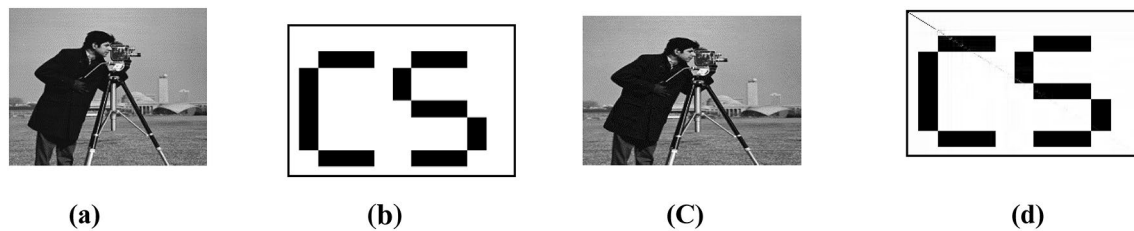


Fig. 10 **a** Original image, Size=63.5 Kilo Byte (KB). **b** Watermark image, Size=64.1 KB. **c** Watermarked image without attacks, PSNR=60.5250, Size=63.6 KB. **d** Extracted watermark for Liu method $c_r=0.8543$

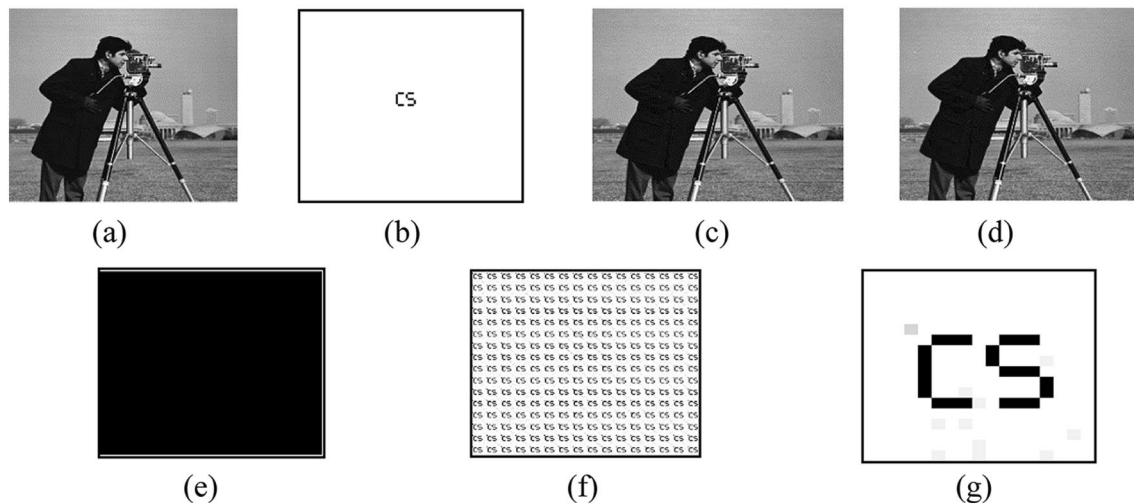


Fig. 11 **a** Original image, Size=63.5 KB. **b** Watermark image, Size=1.3 KB with block size (16×16) . **c** Primary Watermarked image, PSNR 1=45.8605. **d** Final watermarked image, PSNR 2=45.5193. **e** Extracted watermark1 (from the final water-

marked image by SVD), $Cr1=0.0121$ **f** Extracted watermark 2 (From stage 2 by using BSVD). **g** The Extracted watermark 2 (From stage 2 by using BSVD) which gives max correlation ($C_{r2max}=0.9975$), after magnification

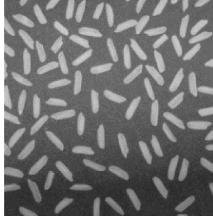

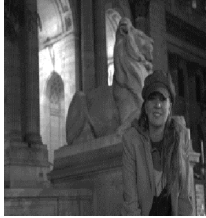

			
a) rice	(b) Pout	(c) Mandi	(d) Peppers
PSNR1=48.1720	PSNR1=50.2885	PSNR1=61.4618	PSNR1=61.6617
PSNR2=47.5720	PSNR2=49.5720	PSNR2=60.5720	PSNR2=60.3720
$C_{r1}=0.0384$	$C_{r1}=0.121$	$C_{r1}=0.0134$	$C_{r1}=0.0122$
$C_{r2}=0.9695$	$C_{r2}=0.9975$	$C_{r2}=0.9596$	$C_{r2}=0.9785$
Different Test Images			

Fig. 12 Different test images




		
Gaussian noise .01	Blurring 3x3	Cropping (50%)

Fig. 13 Attacked watermarked images for the method of Liu




		
Gaussian distribution Noise(0,0.01)	Blurring LPF (3x3)	Cropping (50%)

Fig. 14 Attacked watermarked images for the proposed method

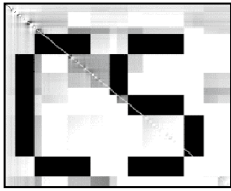
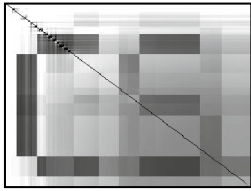
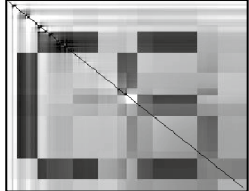
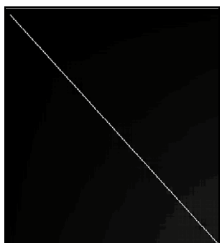
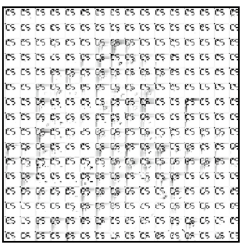
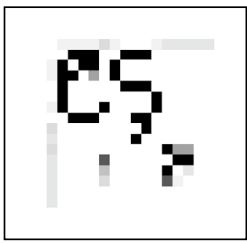
		
Gaussian Noise (0,0.01) Cr = 0.1373	Blurring LPF (3x3) Cr = 0.0670	Cropping (50%) Cr = 0.0106

Fig. 15 The extracted watermarks for the method of Liu after applying different attacks

		
Extracted watermark1 (from final watermarked image) Cr1= -0.00020	Extracted watermark2 (From primary watermarked image in stage2)	Extracted watermark2 Which give max correlation Cr2=0.5482
Gaussian distribution with (zero mean and variance 0.01)		


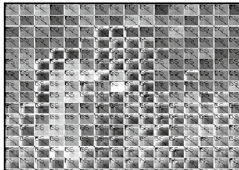

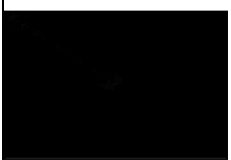


		
Extracted watermark1 (from final watermarked image by SVD) Cr1= 0.0199	Extracted watermark2 (From primary watermarked image in stage2)	Extracted watermark2 Which give max correlation Cr2=0.7072
Blurring attack with LPF (3×3)		
		
Extracted watermark1 (from final watermarked image by SVD) Cr1= 0.0068	Extracted watermark2 (From primary watermarked image in stage2)	Extracted watermark2 Which give max correlation Cr2=0.9975
Cropping attack (50%)		

Fig. 16 Extracted watermarks for different attacks using the proposed method

Table 2 Correlation coefficients and PSNR for various values of Gaussian noise variance

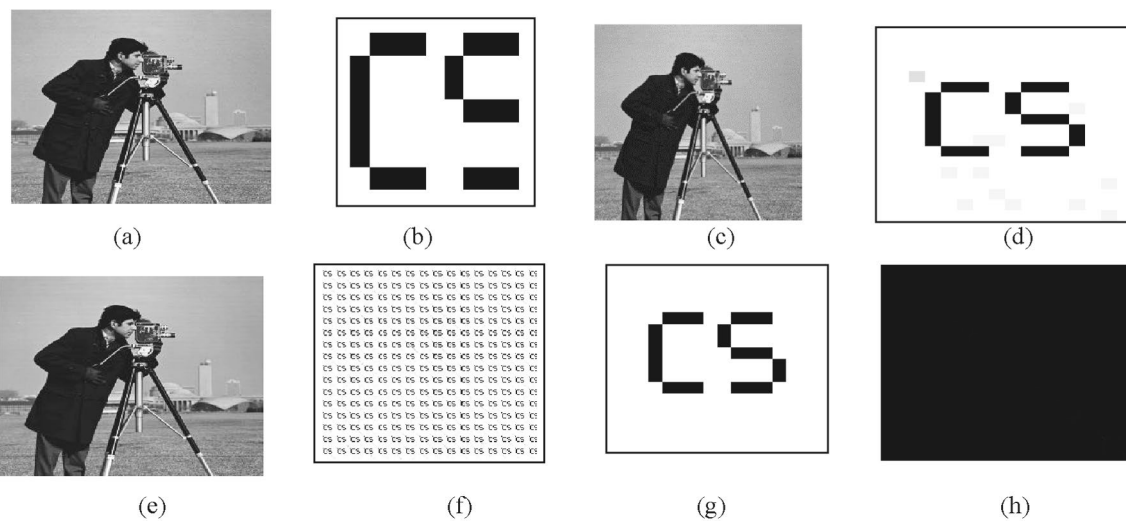
Variance	0.001	0.005	0.01	0.05	0.1	0.5	1
C_r	0.8896	0.6244	0.5643	0.5563	0.5247	0.4704	0.4744
P_{SNR}	39.9307	23.1776	20.2924	13.7677	11.4458	7.6965	0.8393

Table 3 Correlation coefficients between the extracted watermarks and the original watermark for various values of low pass filter windows

Window size	3×3	4×4	5×5	6×6
C_r	0.7107	0.5838	0.6531	0.5576
P_{SNR}	25.1258	22.8089	22.222	21.2976

Table 4 Correlation coefficients between the extracted watermarks and the original watermark under the rotation attack with different rotation angles

Rotation angle	30	45	60	75	90
C_r	0.5757	0.5281	0.6105	0.8458	0.9087
P_{SNR}	6.8917	6.5558	6.5626	7.1381	9.6838

**Fig. 17** **a** Original image with Size=63.5 KB. **b** Watermark image with Size (256×256) **c** Primary watermarked image by (SVD), PSNR 1=113.3409. **d** Watermark image with block size (16×16). **e** Final watermarked image by (BSVD) PSNR 2=45.1884. **f** Extracted watermark1 from the final watermarked image by (BSVD). **g**

Extracted watermark 1 from stage 1 using BSVD which gives max correlation $C_{r_{\max}}=0.9975$ **(f)** Extracted watermark 2 (From stage 2 by using BSVD). **h** The Extracted watermark 2 from stage 2 by using SVD ($C_{r_2}=0.0030$), after magnification

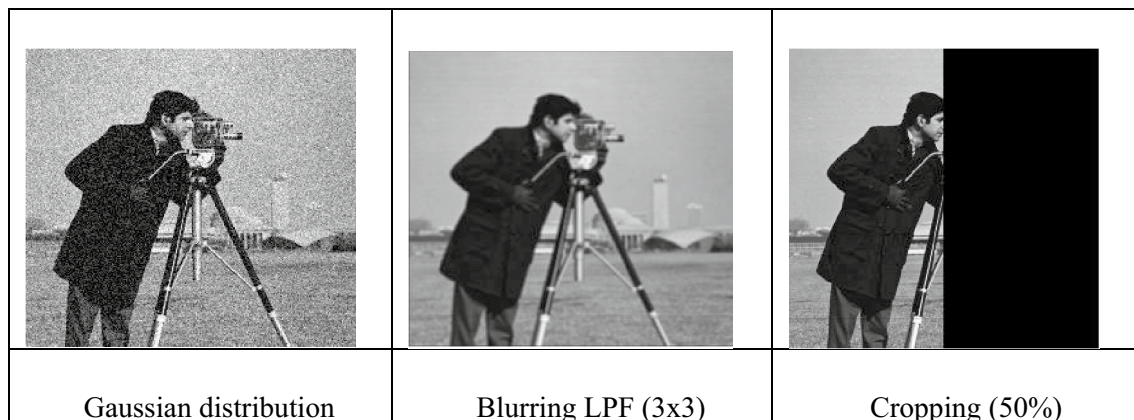


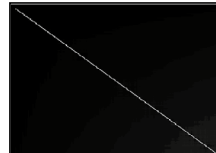
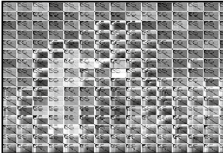


**Fig. 18** Attacked watermarked images for the Reverse Hybrid Digital Image Watermarking Algorithm (SVD-BSVD)

Fig. 19 Extracted watermarks for different attacks using attacked watermarked images for the Reverse Hybrid Digital Image Watermarking Algorithm (SVD-BSVD).

		
Extracted watermark1 From final watermarked image by (BSVD)	Extracted watermark1 From stage1 by using BSVD (Which give max correlation) $Cr1=0.5408$	Extracted watermark2 (From stage2 by using SVD) $Cr2= 0.0092$
Gaussian distribution with (zero mean and variance 0.01)		

		
Extracted watermark1 From final watermarked image by (BSVD)	Extracted watermark1 From stage1 by using BSVD (Which give max correlation) $Cr1=0.7072$	Extracted watermark2 (From stage2 by using SVD) $Cr2= 0.0092$
Blurring attack LPF (3×3)		




		
Extracted watermark1 From final watermarked image by (BSVD)	Extracted watermark1 From stage1 by using BSVD (Which give max correlation) $Cr1=0.9975$	Extracted watermark2 (From stage2 by using SVD) $Cr2=0.0092$
Cropping attack (50%)		

Table 5 Comparison between the correlation coefficients for the proposed Hybrid (BSVD-SVD) Digital Watermarking Algorithm and other methods

Technique	SVD only with one watermark [10]	DWT-SVD with one watermark [17]	Proposed hybrid Digital Image Watermarking Algorithm (BSVD-SVD)	Reverse Hybrid Digital Image Watermarking Algorithm (SVD-BSVD)	DWT-SVD with fused watermark [16]
Attack					
No Attack	0.8508	0.8524	1	0.0030	0.9975
Gaussian distribution noise (0,0.01)	0.1373	0.1332	0.5124	0.0092	0.5482
Blurring LPF window (3x3)	0.0670	0.0916	0.1360	-0.0136	0.7072
Cropping (50%)	0.0106	0.0089	0.2529	0.0092	0.9975

increase with rotation angle. The best values are obtained at 90 degree rotation (Table 4).

The same simulation is repeated on a reverse hybrid digital image watermarking scheme by reversing the stages of the proposed scheme (SVD-BSVD), and its results are

shown in Figs. 17, 18 and 19. The results of this simulation reveal the superiority of the proposed hybrid digital image watermarking scheme (BSVD-SVD) over the reverse hybrid digital image watermarking scheme (SVD-BSVD). Tables 5 and 6 give a comparison study of the C_r and P_{SNR} for the

Table 6 Comparison between PSNR for the proposed Hybrid (BSVD-SVD) Digital Watermarking Algorithm and other methods.

Technique	Proposed hybrid Digital Image Watermarking Algorithm (BSVD-SVD)	Hybrid Digital Image Watermarking Algorithm (SVD-BSVD)	DWT-SVD with fused watermark [18]	DWT-SVD with one watermark [18]	SVD only with one watermark [13]
Attack					
No Attack	60.5775	61.1391	64.3155	45.1884	45.8605
Gaussian distribution noise (0,0.01)	20.3733	20.4082	20.4017	20.2765	20.2588
Blurring LPF window (3x3)	20.6968	20.6968	20.6928	22.5218	22.1678
Cropping	7.8124	7.8124	7.8166	7.8085	7.8085

Table 7 Comparison between processing time (sec) of the proposed Hybrid (BSVD-SVD) Digital Watermarking Algorithm and (only one stage (SVD)).

Technique	Only one stage (SVD) [13]	Proposed hybrid Digital Image Watermarking Algorithm (BSVD-SVD)
Attack		
No Attack	2.332	7.900
Gaussian distribution noise (0,0.01)	2.300	7.176
Blurring LPF window (3x3)	2.160	11.530
Cropping	1.954	8.728

proposed scheme and other schemes for different attacks. In the presence of attacks such as low-pass filtering attack, Gaussian noise attack, and cropping attack, the proposed scheme proves its superiority over the other compared ones. Table 5 presents the C_r using SVD with only one watermark, hybrid DWT-SVD with a fused watermark, a reverse hybrid digital image watermarking scheme (SVD-BSVD), and the proposed scheme. The results show that the proposed scheme (BSVD-SVD) improves the C_r compared with other ones, where the value of C_r for the proposed scheme is higher than that for other ones. From these results, the proposed scheme proves its ability to extract watermarks perfectly compared to other ones (Fig. 19).

Table 6 presents the P_{SNR} using SVD with only one watermark, hybrid DWT-SVD with a fused watermark, a reverse hybrid digital image watermarking scheme (SVD-BSVD), and the proposed scheme. The results show that the proposed scheme has a higher P_{SNR} and a better chance of detecting watermarks, even in the presence of severe attacks, ensuring its fidelity. Table 7 gives the comparison of the processing time (sec) between the SVD with only one watermark and the proposed scheme. Despite increasing the processing time for the proposed scheme, this scheme improves the level of security by increasing the complexity of the system.

Conclusion

In this paper, an efficient image watermarking scheme has been presented. The proposed scheme is implemented through the SVD and B-SVD. The SVD is recognized as a robust watermarking algorithm by exploiting its stability characteristic. The proposed scheme is used to embed more than one watermark into the original image, which means a large capacity. The B-SVD implementation gives more chances to survive different attacks and achieve robust watermarking. The watermarks are embedded with a weight equal to 0.01 to preserve the original image quality and achieve imperceptibility. The complexity of the proposed scheme increases the security level. In addition, improving fidelity means achieving suitable values for PSNR, where there is no visual difference between the original image and the watermarked image. We have concluded that the proposed algorithm is superior to other methods, because it satisfies the watermarking requirement, but the complexity will increase.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. S. Laura, "Cryptography Role in Information Security", Proceedings of the 5th World Scientific and Engineering Academy and Society (WSEAS), international conference on Communications and information technology. 36–41 (2011)
2. C-S. Lu, "Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property", Idea Group Publishing. (2005)
3. D. Mistry, Comparison of digital watermarking methods. *Int J Comput Sci Eng.* **02**(09), 2905–2909 (2010)
4. L. Singh, A.K. Singh, P.K. Singh, Secure data hiding techniques: a survey. *Multimed Tools and Appl.* **79**, 15901–15921 (2020)
5. M. Begum, M.S. Uddin, Digital image watermarking techniques: a review. *Information* **11**, 110 (2020)
6. M. Miller, I. Cox, J. Linnartz, T. Kalker, "A review of watermarking principles and practices", IEEE International Conference on image processing. 461–485 (1999)
7. H. Kayarka, S. Sanyal, A survey on various data hiding techniques and their comparative analysis. *ACTA Technica Corviniensis.* **5**(3), 35–40 (2012)
8. A. Dixit, R. Dixit, A review on digital image watermarking techniques. *Int. J. Image Graph. Signal Process* **9**, 56 (2017)
9. S. Kumar, B.K. Singh, M. Yadav, A recent survey on multimedia and database watermarking. *Multimed. Tools Appl.* **79**, 20149–20197 (2020)
10. V. Singh, "Digital Watermarking: A Tutorial", *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*. 10–21 (2011)
11. S. Lee, S. Jung, A survey of watermarking techniques applied to multimedia. *IEEE Trans. Industr. Electron.* **1**, 272–277 (2001)
12. Z. hang, H. Wang, C. Zhou, (2017) A robust image watermarking scheme based on SVD in the Spatial Domain. **9**, 45
13. R. Liu, T. tan, "An SVD-Based Watermarking Scheme for protecting rightful ownership", *IEEE Trans. on multimedia.* **4** (1), (2002)
14. HN. Huang, DF. Chen, CC. Lin, "Improving SVD-based image watermarking via block-by-block optimization on singular values", *J Image Video Proc.* **25** (2015)
15. R. Ghazy, N. El-Fishawy, M. Hadhoud, M. Dessouky, F. El-Samie, Block-by-block SVD-based image watermarking scheme. *Natl. Radio Sci. Conf.* **1**(9), 13–15 (2007)
16. Z. Wang, A.-C. Bovik, Modern image quality assessment. *Synthesis Lectures on Image, Video, and Multimed Process.* **2**(1), 1–156 (2006)
17. Z. Wang, A.-C. Bovik, (2002) Why is Image Quality Assessment So Difficult?", *Proceeding of the IEEE International Conference on Acoustics, Speech, & Signal Processing (ICASSP)*. (4), 3313–3316
18. E. Hemdan, N. El-Fishawy, G. Attiya, F. El-Samie, "Hybrid Digital Image Watermarking Technique for Data Hiding", *Proceedings of the 27th National Radio Science Conference.* 220–227 (2013)
19. A. F. Eldaashy, M. I. Dessouky, S. Al-Dalil, F. E. Abd El-Samie, "Block-By-Block SVD Image Watermarking with Variable Block Sizes", *CIIT Digital image processing.* **5**(12), (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.