Int J Syst Assur Eng Manag
https://doi.org/10.1007/s13198-022-01732-z

ORIGINAL ARTICLE

Robust and secure watermarking method through BEMD, SVD and Arnold transform in wavelet domain

Laxmanika Singh[1] · Pradeep Kumar Singh[2] · Jagpreet Sidhu[1]

Received: 13 July 2021 / Revised: 1 February 2022 / Accepted: 26 June 2022

Abstract In this paper, an enhanced watermarking technique through discrete wavelet transform (DWT), singular value decomposition (SVD) and Bi- dimensional empirical mode decomposition (BEMD) is presented. During the embedding process, the first level of DWT has applied to decompose an original image into distinct sub-bands (LL, LH, HH, HL). Further, BEMD decomposition is applied to divide sub-bands of DWT according to the robust and least fragile bands. SVD is employed to compute the singular coefficient on a certain band for an embedding process. The proposed technique is implemented with haar wavelet. Further, an inverse process of IDWT, ISVD and IBEMD is applied to this method to get the watermarked image. Moreover, watermark images can be extracted by the extraction process. BEMD is used to get the multiple range representation in the form IMFs. Also, it is used to improve the visual quality of an image. Moreover, the fusion of SVD, DWT and arnold transform is employed to increase the security, robustness and imperceptibility of an image against various attack. Finally, the subjective measure is used to assess the visual quality of the watermarked image. The proposed method provides better imperceptibility, security and robustness against numerous geometrical and non- geometrical attacks such as salt & pepper, Gaussian attack, JPEG compression, median filter, shearing.

Keywords Image watermarking · DWT · Arnold transform · Encryption · BEMD · Watermarking

✉ Pradeep Kumar Singh
pradeep_84cs@yahoo.com

Laxmanika Singh
laxmanika.singh81@gmail.com

Jagpreet Sidhu
jagpreet.pu@gmail.com

1 Department of Computer Science and Engineering, Jaypee University of Information Technology, Solan, HP, India

2 Department of Computer Science, KIET Group of Institutions, Delhi-NCR, Ghaziabad, U.P, India

1 Introduction

Digital Document dissemination through open chain used information technology has proved an essential and cost-friendly system for diffusion and spreading of digital data files. Watermarking methods can be divided into four categories based on the type of data to be watermarked: text watermarking, image watermarking, audio watermarking, and video watermarking. However, because images have a higher data embedding capacity, the current research focuses on watermarking with images as the cover media. There are some challenging issues of malicious attacks such as prohibiting copyright violation, proprietary identification and fake identity (Singh 2017). Some researchers have established that security and safety issues can be solved by digital image watermarking. Digital watermarking is a strong solution for multimedia copyright protection and content authentication. There are two types of image watermarking techniques: 'spatial domain' and 'transform domain' techniques. The spatial domain techniques are straight forward in terms of computation. The essential spatial domain techniques are LSB replacements, correlation-based, and spread-spectrum. The watermark data is directly incorporated in the host signal's pixel values, bit stream, or code values in spatial domain watermarking (cover media). The spatial domain approaches, on the other hand, are less resistant to signal processing attacks (Liu et al. 2018). The data is embedded using transform domain techniques like discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) by modulating the coefficients of a transform. Although transform domain watermarking approaches are computationally complex, they provide increased robustness of watermark data.

In this paper, the SVD technique for encoding the watermark is employed and this technique is applied in almost popular image processing applications such as image compression, image watermarking etc. (Kamble et al. 2012). The following two characteristics of an effective watermarking algorithm are imperceptibility (the difference between the watermarked image and the original image cannot be distinguished by human eyes) and robustness (unauthorised individuals or groups cannot remove the watermark from the embedded data). The robustness of a watermarking method defines its ability to alter throughout transmission and storage, both deliberate (malicious attacks) and inadvertent (compression, noise, filtering, and rotation, etc.). (Wang et al. 2009).The remaining paper is structured in the following ways: the related work is given in Sect. 2. Section 3 defines the major contribution of the work. Section 4 describes the elaboration of offered technique. The process of embedding and extraction process is discussed in Sect. 5. An experimental outcome of the work is described in Sect. 6. Section 7 represents the conclusion and future work.

2 Related work

In this section, the prospective researchers are stated some significant contribution which is presented below:

In Wang et al. (2009), digital image watermarking with DCT, SVD and DWT founded on Arnold map is presented. Thus, DCT, SVD and DWT are used for better imperceptibility and robustness. This technique preserves a lot of memory space. A digital image watermarking algorithm based on DWT along with SVD is provided in Li et al. (2011). Therefore, a binary image was used as a watermark. Moreover, the proposed method has good robustness against different geometric attacks and frequency domain attacks. A robust image watermarking through SVD, DWT and Arnold map is presented in Kamble et al. (2012). Therefore, copyright protection and security can be preserved by SVD and Arnold map of the algorithm respectively. The result shows that the good quality of an image can be achieved by the proposed method. In Ye and Wong (2012), an effective chaotic image encryption procedure based on a generalized arnold map is developed. In this paper, this method is formulated with dual phases i.e. substitution and distribution. Traditional frequent position substitution is applied in the substitution phase. Moreover, this section is persistent and effective encryption through an enormous keyspace and great key sensitivity. An image encoding algorithm based on SVD and arnold transform in the fractional domain is proposed in Chen et al. (2013). In this paper, FrFT is used to transform the original image in a fractional domain and disintegrated by three sections through SVD. Moreover, all these three sections are secured by the arnold transform.

In Zhang et al. (2016), a digital watermarking scheme using SVD, DWT, DCT as well as arnold transform is proposed. Therefore, arnold transform is employed to increase the security of the watermark. Moreover, this proposed method can be protracted to the videotape, audible and colorize the image. The experimental result presented good robustness and a high level of security. An image embedding technique using multi-resolution singular value decomposition (MSVD), DWT and Arnold transform in fractional domain presented in Vaish and Kumar (2017). Therefore, multi-resolution singular value decomposition, Discrete Wavelet Transform and Arnold transform in FrFT is applied on a color image. Further, each component of RGB is encoded individually through DWT, MSVD and arnold transform. An outcome of this technique is high robustness and robustness and increased level of security. In Liu et al. (2018), an image watermarking scheme through logistic and RSA algorithm is used for robustness and secured of the obscure data. The experimental result presents good robustness and imperceptibility.

An image watermarking using SPIHT in the wavelet domain is presented in Kumar et al. 2020a. DCT and SVD are used high-energy compaction properties. Therefore, the SPHIT technique is used for compressed bit string and provides exact rate control and Arnold transform is used for better confidentiality. The outcome of the suggested method is robust and imperceptible in contradiction of various attacks. In Kumar et al. (2020b), multiple image watermarking is employed by the combination RDWT, NSCT, SPHIT and SVD is offered. Therefore, shift variance and higher directionality assets are achieved by the NSCT. Moreover, compression on the watermark image is obtained by the SPHIT. The outcome shows high robustness and security against the different attacks. An improved blind image watermarking using BEMD and arnold transform in circular embedding is proposed in Wang et al. (2020). Therefore, arnold transform is employed to scramble to the watermark image and it is used to enhance the security of the algorithm. Moreover, BEMD technique is utilized for the decomposition of the host image to achieve the IMFs and residue. The outcome of the paper demonstrates higher imperceptibility and robustness.

Table 1 highlights the comparison of different techniques with respect to technique used, factors, result and main remark of the technique.

Table 1 Comparison of various techniques of the watermarking schemes

Technique used	Factors	Results	Remarks
DWT, DCT, SVD and arnold transform (Wang et al. 2009)	Imperceptibility, Robustness and good speed	Performance better than other existing method in terms of robustness and speed	Saves lots of memory space Good speed
DWT-SVD (Li et al. 2011)	Robustness, good visibility	Better visibility and good objectivity	Good to resist geometric attacks and frequency domain attacks
Chaotic image encryption, Arnold transform (Ye and Wong 2012)	Security	Guarantees of security image communication	Suitable for secure image communication
Fractional fourier transform, SVD, Arnold transform, Encryption (Chen et al. 2013)	Quality of recovered image, digital information processing	Better quality of recovered image	Has potential application value in both optics And digital information processing
DCT, DWT, SVD and arnold transform (Zhang et al. 2016)	Robustness, Security, Imperceptibility	Better robustness and high security	Less serious false positive rate Better invisibility Ensure the confidentiality of copyright protection Multiresolution Singular Value
Decomposition, DWT, FrFT, Arnold transform, encryption (Vaish and Kumar 2017)	Robustness, Security	Maintain the level of security and robustness	Secure the data without revealing the original information
DWT,SVD, Logistic, RSA (Liu et al. 2018)	Robustness, copyright protection, Imperceptibility	Performance better than other existing method in terms of robustness and imperceptibility	Less encryption time Large data embedding capacity
DWT, SVD, DCT, SPHIT, Arnold (Kumar et al. 2020a)	Robustness, Imperceptibility	Better robustness, imperceptible and good security	Achieved secure against various attack
RDWT, SPHIT, SVD, Arnold transform, non-sub sampled contourlet transform (Kumar et al. 2020b)	Robustness, security and imperceptibility	Performance better than other existing method in terms of robustness and security	Achieved high capacity and high security
BEMD, Arnold transform (Wang et al. 2020)	Robustness, Imperceptibility	Better robustness and high imperceptibility	Circular embedding is used

Table 2 PSNR, SSIM, NC, NPCR and UACI values achieved of proposed method at different gain factor

Gain factor	PSNR (in dB)	SSIM	NC	NPCR	UACI
0.01	42.47	1.0000	0.9522	0.9959	0.3465
0.08	42.15	0.9999	0.9964	0.9965	0.3470
0.09	41.07	0.9998	0.9961	0.9970	0.3461
0.1	40.81	0.9997	0.9972	0.9968	0.3446
0.3	38.69	0.9881	0.9981	0.9980	0.3453
0.5	38.35	0.9579	0.9999	0.9960	0.3469

Table 3 PSNR, SSIM, NC, NPCR and UACI values achieved for distinct image from proposed method

Images	PSNR (in dB)	SSIM	NC	NPCR	UACI
Barbara	41.13	0.9991	0.9962	0.9963	0.3767
Baboon	43.28	0.9988	0.9935	0.9960	0.4847
Lena	43.79	0.9965	0.9981	0.9951	0.3468
Cameraman	44.06	0.9954	0.9992	0.9946	0.4598
Boat	42.36	0.9921	0.9931	0.9961	0.4789

3 Major contribution of work

In such paper, we offered a robust image watermarking method relying on SVD, DWT, BEMD and arnold techniques. The process for embedding and extraction is computed in terms of robustness, security and imperceptibility.

(i) For a better trade-off between imperceptibility and robustness requirements, a combination of SVD, BEMD and DWT is applied, and high NC values are obtained using the popular transform domain and arnold transform.
(ii) For better confidentiality, watermark image is scrambled by arnold transform. This is hard to recover watermark for attackers even after extraction. BEMD technique is used to decompose the watermarking image to enhance the quality of an image and get a better frequency factor for the host image.
(iii) Our watermarking method reduces bandwidth consumption, and the hidden watermark allows for quick data storage and retrieval.
(iv) Our results (Tables 1, 2, 3 and 5) clearly demonstrate that the proposed method embeds the watermarking imperceptibility and recovers the hidden watermark that is nearly identical to the original.
(v) Numerous experimental tests are used to evaluate the performance of this method. Further, the NC and PSNR values are found to be superior to those observed in other similar techniques (Singh 2017; Zhang et al. 2016; Kumar et al. 2020a).
(vi) Refer Table 9, the visual quality of the watermarked image is evaluated using a subjective method.

4 Terminology

A strong watermarking process through BEMD, Arnold transform, DWT and SVD is introduced. The cover image is decomposing through DWT. Also, the watermarking image can be separated by BEMD and SVD and arnold transform on watermark image. Hence, a brief explanation of this method is described in the following sections:

4.1 Discrete wavelet transform (DWT)

DWT has been very useful implement for image processing, compression and analysis. The basic idea of DWT, is decomposed into multi-frequency and different spaces. DWT has been employed to disintegrate the image into 4 frequency bands: LL band, HL band, LH band and HH band. The low-frequency band is used for the image's energy. The rest three-band describes the peripheral details of the corresponding direction and has some energy (Li et al. 2011). Therefore, good capacity (huge amount of information hiding) cannot be achieved by DWT because of the shift variance (Ansari et al. 2016).

4.2 Arnold transform

Arnold transform is often introduced as cat face transform. Cat face transform is a scrambling method that can be used to encrypt and decrypt images. Arnold transform is applied and it can change the configuration of gray values by changing the coordinates pixels in a digital image.

Arnold scrambling is only applied to pixels, but it can be expanded to entire image blocks. The robustness and security of an image can be increased if the scrambling is done on both pixels and blocks. Arnold's pixel scrambling effect can be used on any image of any size. However, to apply Arnold scrambling to an image which is divided into blocks, the image size must be in the order of M × M. If the image's size is not M × M, it can be made M × M by padding the image with zeros. Arnold transform is used as a scrambling step in which the number of iterations is used as a key.

Image of N × N matrix and scrambled the image pixel by the formula (Li et al. 2011):

$$\begin{pmatrix} a1 \\ b1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \; mod \; n \tag{1}$$

where (a, b) = location coordinates of the cover image pixels.

(a1, b1) = location coordinates of image pixel that after transform.

4.3 Singular value decomposition (SVD)

Assume that the input image can be represented by matrix B as well as X × X represents the square matrix for this image with ranking r (r ≤ X). The SVD of matrix B is expressed by

$$B = UDV^T \tag{2}$$

where matrix B defines the matrix X × X, the U and V represent the orthogonal matrix (Chung et al. 2007). Singular values of B represent the diagonal matrix D. Matrix D's main diagonal has singular values D1 ≥ D2 ≥ D3 ≥ .... Dn ≥ 0 that are in declining order. However, these singularities have been achieved by getting the square root mean of the eigen values of ZZT and ZTZ. The U and V are not unique matrix where the singular value is unique. The relation can be defined as:

$$Z = UDV^T \tag{3}$$

Now

$$ZZ^T = UDV^T\left(UDV^T\right)^T = US^2U^T \tag{4}$$

$$Z^TZ = \left(UDV^T\right)^T\left(UDV^T\right) = VS^2V^T \tag{5}$$

If matrix B becomes real then the values of U and V also real and singular values always become real numbers. There is an essential role for SVD in image watermarking, and scalability is the main factor. (Singh 2017).

4.4 Bi-dimensional empirical mode decomposition (BEMD)

Haung et al. introduced the basic concept of BEMD (Deng et al. 2011). This technique allows the determination of non-linear and unbound data. The main principal of such a method is that it is used to divide an absolute signal into distinct frequency properties, called IMFs (intrinsic mode functions) and the highest frequency component is called residue (r) (Deng et al. 2011).

$$BEMD = \text{residue (r)} + IMFs_i \tag{6}$$

where i defines IMF's index number.

5 Proposed algorithm

The proposed method is based on DWT, arnold transform, BEMD and SVD. The proposed method is applied to improve security and robustness without devaluing the visual quality against different attacks. In our experiment, the cover image size of 512 × 512 and watermark image of size just half of the cover image i.e. 256 × 256 are applied for testing. In our experiment, the considerable distortion between the cover and watermarked image is measured using the Peak Signal to Noise Ratio (PSNR), Normalized correlation (NC), number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) and the Structure Similarity Index (SSIM).

Here, the Arnold transform is used to encrypt the watermark by allowing a private key of 32 bit to achieve the imperceptibility and security of the watermark image. To maintain the highest level of security, a key is used during insertion, and the same key must be given to the receiver in order to extract the watermark or cover image. On the other hand, the same private key is used for the decryption process to retrieve the watermark. The watermarking embedding and extraction process is demonstrated in Figs. 1 and 2 respectively.

Explanation of Fig. 1

1. Apply 2-level DWT transform on cover image to decompose it into the sub-bands and select LL1 sub bands.
2. Apply BEMD to selected sub band and then apply SVD to residue of BEMD to obtain corresponding three matrices U_y, S_y, V_y.

$$S = U_y S_y V_y^T$$

3. Apply SVD method into matrix U_y, S_y, V_y to get singular value on the diagonal vector (s).
4. Apply the Arnold transform the watermark image I_w with secret key to scramble the pixels of an image.
5. Apply BEMD on the scrambled watermark image to get the residue and apply SVD applied to compute the singular coefficient and it becomes the matrix U_w, S_w and V_w. The reconstruct the image of the matrix U, S_w and V.
6. Apply the embedding process with the equation:

$$S_{mark} = S_y + \alpha \times S_w \tag{7}$$

7. Perform inverse of ISVD, IBEMD and IDWT process on I_w image to get watermarked image.

Explanation of Fig. 2

1. Apply 2- level DWT to decompose the grayscale watermarked image (I_w) into four sub bands.
2. Apply BEMD on the LL sub band and decomposed into IMF_1, IMF_2, IMF_3 and residue R_w.
3. Apply SVD on R_w to get the coefficients of matrix U, S_w and V.
4. After that reconstruct the image from the U_w, S_w and V_w matrices.

$$S_{wt} = U_w \times S_w \times V_w; \tag{8}$$

5. Then extract the watermark image from S_{wt}.

$$S_{wrec=}\left(S_w - S_y\right)/\alpha; \quad (9)$$

6. Apply inverse of SVD, BEMD and Arnold transform same as embedding method.
7. Recovered watermark image is obtained.

This algorithm stages are given below:

5.1 Embedding steps

The watermarking process is described as follows:

Start:
Step 1:Variable statement
α : gain factor (efficiency factor)
SVD and DWT : methods based on transformation domain
Wavelet filter: Haar
LL1, LH1, HL1 and HH1 : DWT sub bands for original image
U_y, S_y, V_y : SVD coefficients for cover image
U_y and V_y^T: Orthonormal matrices for D
S_y: Diagonal matrix for D
I_1: watermarked image
S_w^K: Modified value of S_y
Smodi: Modified DWT coefficient
Step 2: Read the image
I ← Baboon.jpg
I_w ← Cameraman.jpg
Step3: Perform 2nd level DWT on the sub-image LL into LL1, LH1, HL1 and HH1.
[LL1, LH1, HL1, HH1]← DWT (I, Haar);
Step4: Apply BEMD on LL1 band of DWT to get the IMFs and residue (r).
B ← BEMD (LL1);
Step5: Apply Arnold transform on watermark image I_w with secret key to scramble the pixels of an image.
A← Arnold (I_w);
Step6: Apply BEMD on scrambled watermark image to get the residue
B1← BEMD(A);
Step7: Compute the singular coefficient of residue of BEMD
If (SVD on B)then
$U_y S_y V_y^T$ ← SVD(B)
Endif;
If (SVD on Iw) then
$U_w S_w V_w^T$ ← SVD(Iw)
Endif;
Step8: Compute the singular coefficient of residue of BEMD on scrambled watermark image
If (SVD on B1)then
$U_y S_y V_y^T$ ← SVD(B1)
Endif;
Step9: Image watermarking embedding
For α ← 0.01 :0.5
Smark= $S_y + \alpha \times S_w$;
End;
Step10: Obtain watermarked image
Inverse of SVD(SVD_{LL})= U_y(new $S_{w)}$ V_y^T;
LL_R= IBEMD (SVD_{LL}, IMF_1, IMF_2, IMF_3)
apply inverse of DWT to LL_R, LH1, HL1 and HH1with modified coefficient
X= idwt2 (LL_R, LH_1, HL_1, HH_1,"Haar", S_x)
End;

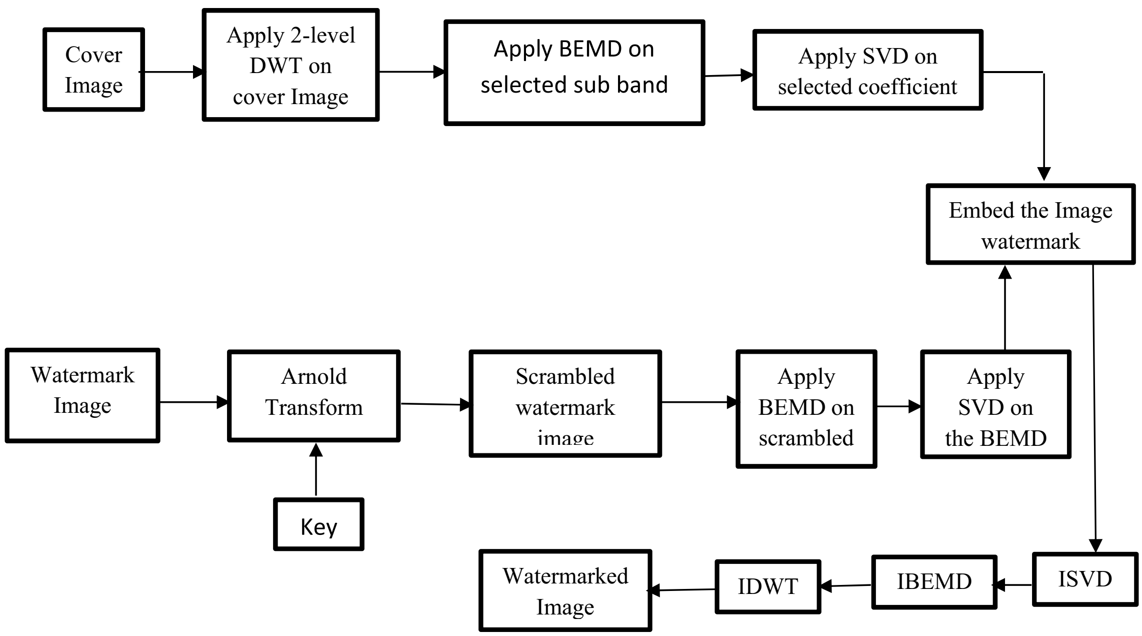

Fig. 1 Block diagram of watermarking embedding process

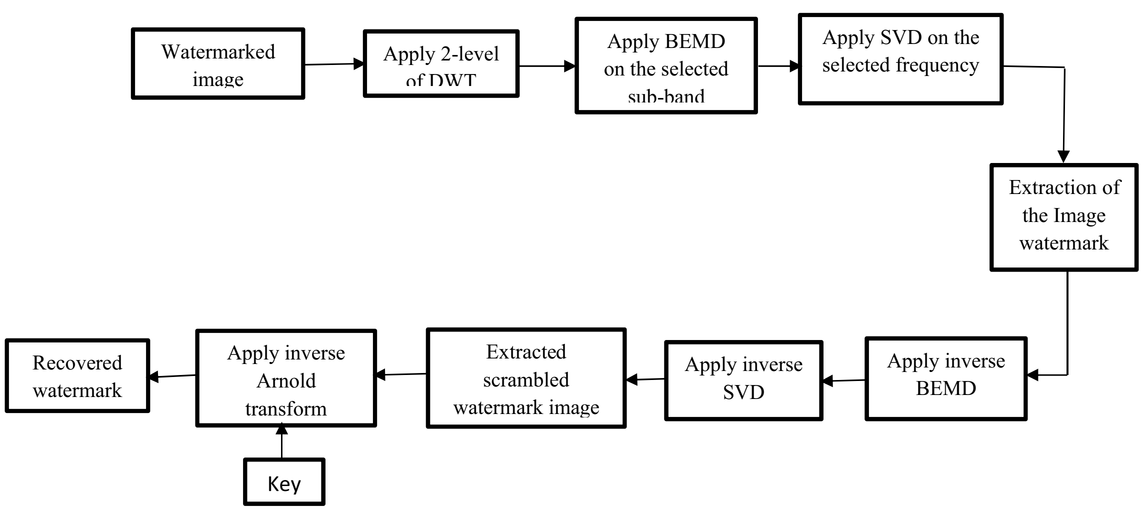

Fig. 2 Block diagram of watermarking extraction method

5.2 Recovery steps

The inverse of embedding process is an extraction method for image watermarking. The extraction algorithm for image watermarking is described as follows:

The following steps are explaining the extraction of watermark:

Start:

Step1: Variable declaration

α : gain factor (efficiency factor)

LL_2, HL_2, LH_2, HH_2: sub-bands for watermarked image

Uw, Sw, Vw: SVD coefficients for watermarked image

Step2: Apply DWT on watermarked image I_w

[LL2, HL2, LH2, HH2]←DWT (I_w, Haar)

Step3: The I_w image decomposed with BEMD method into IMF1, IMF2, IMF3 and residue R_w.

Pw← BEMD(LL2);

Step4: Extract the watermark image from S_{wt} and compute singular value for Pw.

S_{wt}= Uw×Sw×Vw;

Sw← SVD(Pw);

Step5: Retrieved the embedded watermark

Swrec= (Sw-sy)/α;

//the process is observed using the reverse of SVD, BEMD, arnold transform and DWT on the extracted component to retrieve the watermark image.

6 Experimental results and analysis

In the article, the size of the cover image is 512×512 and the size of the watermark image is 256×256 is taken. MATLAB R2018a is used for the implementation. There are five gray level images like Barbara, baboon, cameraman, Lena and boat which are utilised for the testing purpose. In this process, peak-signal noise ratio (PSNR), Similarity Index Measure (SSIM) and Normalized correlation (NC), are applied for the testing. Furthermore, the performance of this technique is implemented through the use of two critical parameters, namely the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI). UACI is used to calculate the mean difference between encrypted and actual images. Here, 'Haar' wavelet is used for better resolution. Figure 3 represents the original images and watermark image that is used in experimental results.

There are many aspects to measure the performance of watermarking techniques: Robustness and imperceptibility. The PSNR computes the peak signal to noise ratio in decibels between two images. The ratio is used as a quality measurement between the original image and a compressed

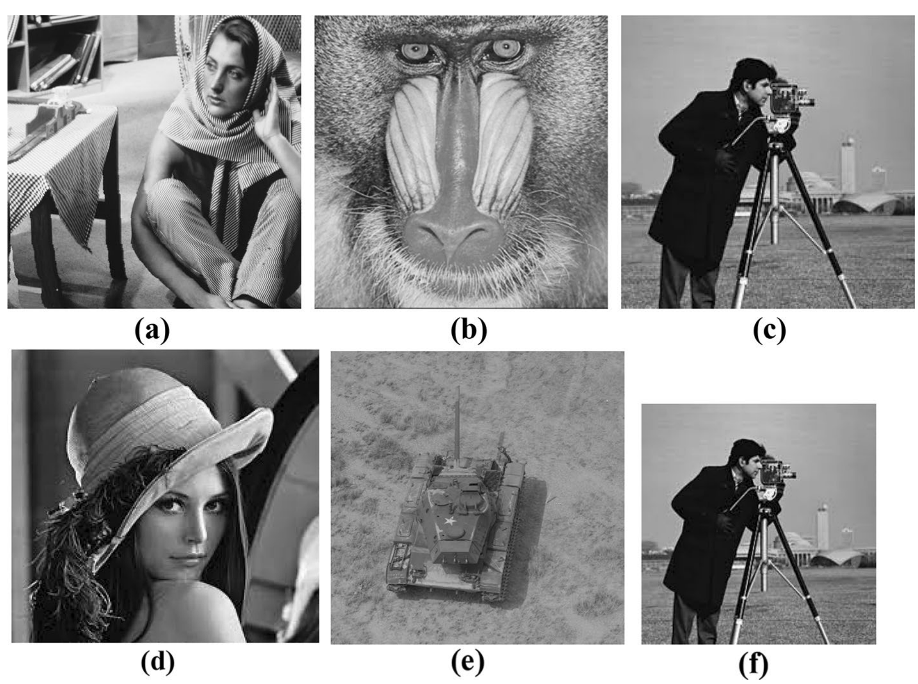

Fig. 3 The original host image of **a** Barbara **b** Baboon **c** Cameraman **d** Lena **e** Boat **f** the watermark image

Table 4 Description and MATLAB command for different attacks

Attacks	Description	MATLAB command
Salt and pepper	Salt & pepper is a type of impulse noise which can be seen on image	noise_salt&pepper = imnoise(image,'salt&pepper',.01);
	This noise can be caused by sharp and sudden disturbance in the image	where, noise density = .01
Gaussian noise	To reduce the image visual quality, adds a noise signal to an image in order to deliberately corrupt the image	noise_gaussian = imnoise(image,'gaussian',.01); where, noise density = 0.01
JPEG compression	JPEG compression image is created when the watermarked image is not in the JPEG format. The attacker can resave the as a JPEG using a lower quality factor	noise_JPEG = imnoise(image,'JPEG file path,'Quality',10); where, noise density = 10
Median filter	Aims to reduce the presence of noise in an image and improve the visual quality of an image	noise_medianfilter = medfilt2(image, [3 3]); where, noise density = 3 × 3
Shearing	Shearing is an attack that slants the image shape. The watermarked image is directly affected by shearing transform	noise_shearing = imnoise(image,'Shear Attack x-axis','FontSize', x = 0.4,y = 0.4); on x–y axis

Table 5 The value of PSNR and NC achieved under various attacks

Attacks	Noise density	PSNR (in dB)	NC
Salt & pepper	0.001	44.76	0.9979
	0.003	43.23	0.9921
	0.005	42.39	0.9880
	0.01	41.29	0.9998
	0.1	40.13	0.9877
Gaussian attack	0.001	43.34	0.9956
	0.003	42.67	0.9875
	0.005	41.34	0.9596
	0.01	40.12	0.9519
JPEG compression	10	42.45	0.9977
	30	40.11	0.9819
	60	40.18	0.9801
Median Filter	3 × 3	39.01	0.9978
	4 × 4	40.34	0.9832
Shearing	0.4 × 0.4	39.82	0.9701

image. When the PSNR value is higher, the quality of an image will be better. PSNR is calculated using this equation

$$\text{PSNR} = 10\log\frac{(255)^2}{\text{MSE}} \tag{10}$$

Here, mean square error (MSE) is measured using this equation:

$$\text{MSE} = \frac{1}{m*n}\sum_{x=1}^{m}\sum_{y=1}^{n}\left(O_{xy} - W_{xy}\right) \tag{11}$$

where Oxy represents the pixels of the cover image of dimension x × y and pixel of watermarked image is represented by Wxy of dimension x × y. Normalized correlation is used to find the dissimilarities and similarities between the original and extracted watermark (s) images. NC value is acceptable between 0 and 1.

$$NC = \frac{\sum_{k=1}^{X}\sum_{l=1}^{Y}\left(Q_{original\ kl} \times Q_{recovered\ kl}\right)}{\sum_{k=1}^{X}\sum_{l=1}^{Y}Q_{original\ kl}^{2}} \tag{12}$$

where $Q_{originalkl}$= pixel of the original watermark, $Q_{recoveredkl}$ = pixel of the extracted watermark. The Structural similarity index (SSIM) is a method for measuring the similarity between cover image and watermark image. The SSIM value lies between 0 to 1.

$$\text{SSIM (a, b)} = \text{p (a, b) q (a, b) r (a, b)} \tag{13}$$

where $p(a,b) = \frac{2\mu_a\mu_b + C_1}{\mu_a^2 + \mu_b^2 + C_1}$

$$q(a,b) = \frac{2\sigma_a\sigma_b + C_2}{\sigma_a^2 + \sigma_b^2 + C_2}$$

$$r(a,b) = \frac{\sigma_{ab} + C_3}{\sigma_a\sigma_b + C_3}$$

where The variables p (a, b), q (a, b) and r (a, b) are known as luminance, contrast and structure comparison functions respectively. Further C1, C2 and C3 are constants with positive values.

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. Let us consider 'Im1' and 'Im2' be two cipher text images. The pixel value at grid (m, n) in 'Im1' and 'Im2' are given as Im1 (a, b) and Im2 (a, b).

$$NPCR = \sum_{a,b}\frac{T(a,b)}{R} \times 100\% \tag{14}$$

Table 6 Comparative NC values with existing technique

Attacks	Noise density	NC (Singh 2017)	NC (Kumar et al. 2020a)	Proposed method
Salt & pepper	0.001	0.9938	0.9969	0.9979
	0.01	0.9961	0.9424	0.9998
	0.1	NA	0.7005	0.9877
Gaussian noise	0.001	0.9591	0.9874	0.9956
	0.005	NA	0.9219	0.9596
	0.01	0.6297	0.8569	0.9519
JPEG compression	10	0.9913	0.9969	0.9977
Scaling attacks	(×0.5)	NA	0.5563	0.8193
Scaling attacks	(1.1)	0.7251	NA	0.7989

Table 7 Comparative NC values with other existing values

Attacks	Noise density	NC (Kumar et al. 2020a)	NC (Zhang et al. 2016)	NC of proposed method
Median Filter	3×3	NA	0.9949	0.9978
JPEG compression	10	0.9969	0.9965	0.9977

Table 8 Comparing PSNR values with other techniques

Image	PSNR (Kumar et al. 2020a)	PSNR (Singh 2017)	PSNR of proposed method
Barbara	32.82	26.86	41.13
Boat	30.13	NA	42.36
Lena	30.00	31.06	43.79

Table 9 Measuring watermarked image visual quality using subjective evaluation under distinct gain factor (Singh and Singh 2021)

Gain factor	Visual quality of watermarked image
0.001	Excellent visual quality
0.01	Very good visual quality
0.05	Good visual quality
0.1	Acceptable visual quality
0.2	Poor visual quality
0.5	Very poor visual quality

Table10 NC value achieved from distinct attacked watermark image and recovered image

Attacks	Attacked image	Obtained NC value	Recovered watermark image
Salt and pepper (0.001)		0.9979	
Salt and pepper (0.1)		0.9877	
Gaussian attack (0.001)		0.9956	
Gaussian attack (0.01)		0.9519	
Median Filter (3×3)		0.9978	
JPEG (60)		0.9801	
Shearing		0.9701	

where ‘R’ = total number of pixels in cipher text and T (a,b) is defined as

$$T(a,b) = \begin{cases} 0, & if\ I_{m1}(a,b) = I_{m2}(a,b) \\ 1, & if\ I_{m1}(a,b) \neq I_{m2}(a,b) \end{cases} \quad (15)$$

$$UACI = \sum_{a,b} \frac{|I_{m1}(a,b) - I_{m2}(a,b)|}{T \times R} \times 100\% \quad (16)$$

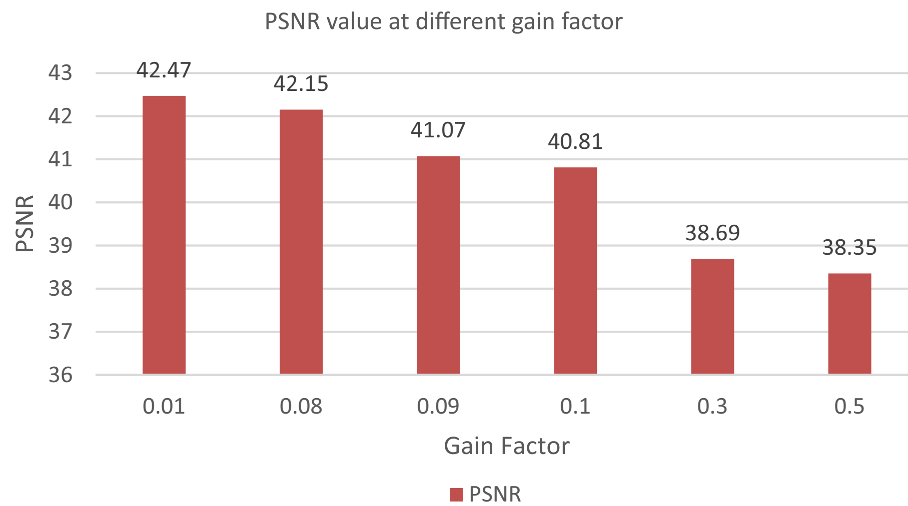

Fig. 4 Pictorial illustration for the PSNR value under distinct gain factor

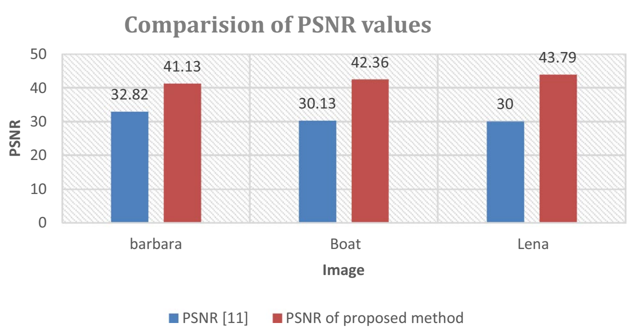

Fig. 5 Pictorial illustration for the comparison of PSNR value for the proposed method and PSNR algorithm [11]

where 'T' = maximum supported pixel value compatible to format of cipher text image.

The outcomes of these techniques are explained in Tables 2, 3, 4, 5, 6, 7, 8 and 10. In Table 2, the value of PSNR and NC are evaluated at distinct gain factors (GF) for the baboon image. As shown in Table 2, the acceptable PSNR and NC values are 42.47 (GF = 0.01) and 0.9999 (GF = 0.5) respectively. Usually, there are PSNR and NC values which are dependent on each other. The NC value increases and the PSNR value decreases at the same time (Singh et al. 2020). The max values of SSIM, NPCR and UACI are 1.000, 0.9980 and 0.3470 respectively in Table 2. Table 3 shows the PSNR and NC values calculated for six different images at GF = 0.01.

As reported in Table 3, the best values of PSNR and NC are 44.06 and 0.9992 for the cameraman respectively. The maximum values of SSIM, NPCR and UACI are 0.9991, 0.9963 and 0.4847 respectively for different images in Table 3. All the values are calculated on same gain factor (GF = 0.01).

Image processing attacks induce synchronization errors between the original and the extracted watermark during the detection process. Table 4 describes the properties and MATLAB command of an attack.

The values of PSNR and NC are possibly satisfactory. Table 5 demonstrates the value of PSNR and NC for various kinds of attacks for the baboon image. According to Table 5, PSNR and NC values are larger than 39.01 and 0.9519 respectively (more often). As reported in Table 5, the proposed technique has good robustness against attacks and the maximum value of PSNR is 44.76 (GF = 0.001) for salt & pepper and the maximum NC value is 0.9998 for salt & pepper (GF = 0.01).

Additionally, the value of NC and PSNR is related to other comparable stated techniques (Singh 2017; Zhang et al. 2016; Kumar et al. 2020a) as shown in Tables 6, 7 and 8. As reported by Table 6, the highest value of NC value is attained as 0.9998 for salt & pepper. However, the value of the NC achieved with the Kumar et al. (2020a) method is 0.9424 for similar attack. From Table 7, NC values are opposed to other techniques described (Zhang et al. 2016; Kumar et al. 2020a). From Table 8, the proposed method has enhanced performance (PSNR values) compared to other reported techniques (Singh 2017; Kumar et al. 2020a).

According to Table 9, it is concluded that the visual quality of the watermarked images is acceptable except for the gain factor = 0.5 from the subjective measure.

According to Table 10, the value of NC and recovered watermark are obtained from different attacks.

Figure 4 represents a pictorial representation of the PSNR value at a different gain factor for greyscale image baboon. Figure 5 demonstrates the assessment of PSNR values between the suggested technique and the exiting technique (Kumar et al. 2020a) for greyscale image Barbara, Boat and Lena.

Figure 6 demonstrates the performance of SSIM, NPCR and UACI at distinct gain factors. Figure 7 shows the value of SSIM, NPCR and UACI for different images.

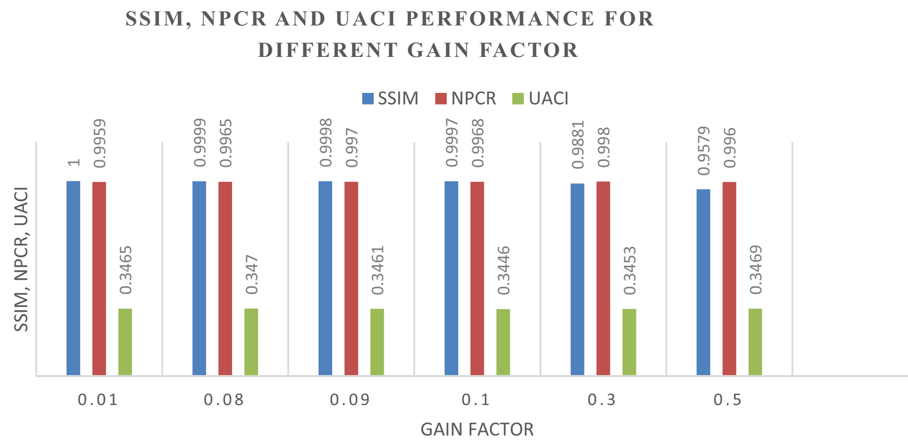

Fig. 6 SSIM, NPCR and UACI Performance for different gain factor

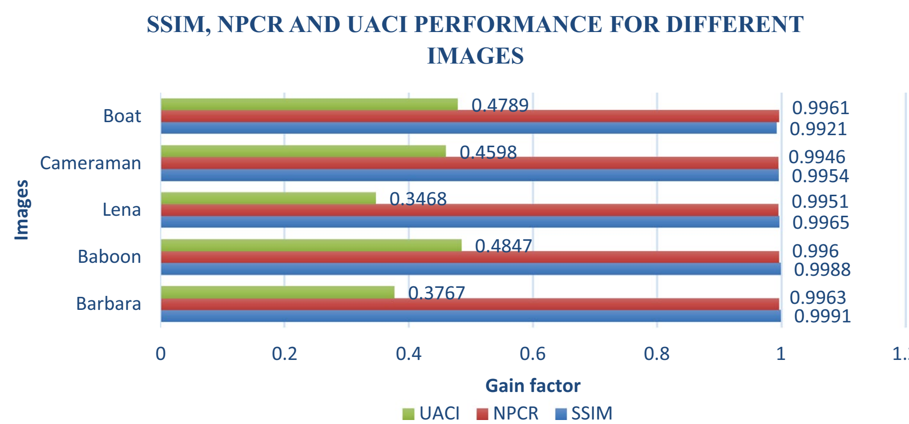

Fig. 7 SSIM, NPCR and UPCI performance for different images

7 Conclusion and future scope

An improved robust and secure watermarking algorithm based on DWT, BEMD, SVD and arnold transform is presented. The main key points of the proposed method can be observed in such a way: (1) DWT is utilised to increase the resolution of an image and reduce the size of an image without losing the quality of the image. Therefore, visual quality and robustness can be achieved by the combination of DWT and SVD. (2) BEMD is used to divide the least fragile and robust frequency bands to get the best frequency coefficients for the input image. (3) The Arnold transform is used to scramble the pixels of an image and to improve the algorithm's security. Through discussion, the proposed method's outcome represents good robustness, imperceptibility and security against various attacks, and it establishes excellent execution to other similar methods. Furthermore, the suggested applications find potential applications in medical image analysis, remote sensing, image enhancement and classification and texture segmentation.

As per future perspective, we would like to further compute the performance of underlying audio, video and multiple watermarking with some transform methods.

Author contributions All authors contributed for the manuscript.

Funding There is no funding support to carry out this research work.

Declarations

Conflict of interest There is no conflict of interest.

Research involving human participants and/or animals informed consent This research work carried out in this manuscript does not include the involvement of human/animal in any form nor it is related to human/animal medical data.

References

Ansari IA, Pant M, Ahn CW (2016) PSO optimized and secured watermarking scheme based on DWT and SVD. In: Fifth international conference on soft computing for problem solving, Springer, pp 411–424.

Chen L, Zhao D, Ge F (2013) Image encryption based on singular value decomposition and Arnold transform in fractional domain. Opt Commun 291:98–103

Chung KL, Yang WN, Huang YH, Wu ST, Hsu YC (2007) On SVD-based watermarking algorithm. Appl Math Comput 188(1):54–57

Deng MH, Yang F, Wang RT (2011) Robust watermarking algorithm based on bi-dimensional empirical mode decomposition. Mater Res 204:627–631

Kamble S, Maheshkar V, Agarwal S, Srivastava VK (2012) DWT-SVD based robust image watermarking using Arnold map. Int J Inform Technol Knowl Manag 5(1):101–105

Kumar C, Singh AK, Kumar P (2020) Improved wavelet-based image watermarking through SPIHT. Multimed Tools Appl 79(15):11069–11082

Kumar C, Singh AK, Kumar P, Singh R, Singh S (2020) SPIHT-based multiple image watermarking in NSCT domain. Concurr Comput Practce Exp 32(1):e4912

Li Y, Gou W, Li B (2011) A new digital watermark algorithm based on the DWT and SVD. In: International symposium on distributed computing and applications to business, engineering and science, pp 207–210.

Liu Y, Tang S, Liu R, Zhang L, Ma Z (2018) Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Syst Appl 97:95–105

Singh AK (2017) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimed Tools Appl 76(6):8881–900

Singh L, Singh PK (2021) Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain. Multimed Tools Appl 2:1–26

Singh L, Singh AK, Singh PK (2020) a robust image watermarking through bi-empirical mode decomposition and discrete wavelet domain. ICETIT 2019. Springer, Heidelberg, pp 1041–1054

Vaish A, Kumar M (2017) Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. Optik 145:273–283

Wang X, Hu K, Hu J, Du L, Ho AT, Qin H (2020) Robust and blind image watermarking via circular embedding and bidimensional empirical mode decomposition. Vis Comput 36(10):2201–2214

Wang B, Ding J, Wen Q, Liao X, Liu C (2009) An image watermarking algorithm based on DWT DCT and SVD. In: IEEE international conference on network infrastructure and digital content, pp 1034–1038.

Ye G, Wong KW (2012) An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn 69(4):2079–87

Zhang Z, Wang C, Zhou X (2016) Image watermarking scheme based on Arnold transform and DWT-DCT-SVD, In: IEEE 13th international conference on signal processing (ICSP), pp 805–810