Journal of Engineering Science and Technology
Vol. 14, No. 4 (2019) 1924 - 1939
© School of Engineering, Taylor's University

A SECURED AND ROBUST IMAGE WATERMARKING BASED ON PIXEL PERMUTATION, WAVELET TRANSFORM AND SINGULAR VALUE DECOMPOSITION

RANJEET KUMAR SINGH*, DILIP KUMAR SHAW

Department of computer applications, National Institute of Technology Jamshedpur, India
*Corresponding Author: 2014rsca002@gmail.com

Abstract

This paper proposed blind reversible digital image based watermarking technique to combined Singular Value Decomposition (SVD) with Discrete Wavelet Transformation (DWT), to improve data security, robustness and capacity. In this approach, two watermarks are embedded into two different sub-bands of the original image. Initially, we decomposed the original image into four sub-bands using DWT, and again DWT is used on *LL* sub-band till the third level. Pixel permutation is used to encrypt the QR Code, then encrypt QR code, and logo images are embedded in the third level of *LL* in *LL*3 and *HL*3. After subjecting the watermarked image to various attacks like cropping, rotation, sharpen, adding noise, contrast adjustment and filtering etc., we recovered inserted watermark image from cover image and compared the quality of the recovered watermark by the correlation coefficient. Robustness of the proposed algorithm is comparatively better than some of the previously proposed methods. Various graphs and tables show results in the paper.

Keywords: Correlation coefficient, DWT, QR Code, SVD.

1. Introduction

In recent years, usage of digital media has increased enormously. An important usage of digital media is the transmission of data and information itself over the internet. The transmission of a huge quantity of data over the internet through several hierarchies may well produce illegals and unauthorised digital media, and thus it is very difficult to identify and protect the ownership of the digital media. Digital watermarking introduced as a solution to this problem. Digital watermarking is a mechanism for hiding information into digital content, i.e. image, audio and video, etc. It is used primarily for data authentication purpose, i.e., honour ship proving, digital data verification, copyright protection etc. There are two main operations in watermarking procedure one is information (watermark) hiding, and other is watermark detection and recovery. There are two main approaches are used for digital watermarking one is spatial domain and other is frequency domain. Least Significant Bit (LSB) is an example of a spatial domain and Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) are the example of frequency domain digital watermarking approach.

2. Related Work

In this section, we express some important existing watermarking scheme based on DWT, DCT and SVD approach. There are many techniques are available on DWT and SVD based watermarking approach. Chang et al. [1] presented a watermarking technique, which is based on SVD. Singular Value decomposition preserves both one-way and non-symmetric properties of the image. This property of SVD provides various sizes of transformation and security. In this technique, both *S* and *U* components of SVD are explored for embedding the watermark information and maintain the more robustness.

Fan et al. [2] due to SVD approach provides robustness and invisibility property, in which, it introduced two notes on the SVD scheme. (1) Changing the coefficients in column vector will cause not as much of visible distortion than that on the row vector, for *U* component of SVD. Similarly, (2) changing the coefficients in column vector will cause fewer visible distortions than that on the row vector, for the *V* component of SVD. By these two notes, they have shown that invisibility and robustness of the watermark can be increased.

Watermarking is not only used for authentication, but it is also used for data security. Security is usually provided by using any encryption mechanism. Liu and Tan [3] proposed a scheme, which provides both robustness and security even without using an encryption scheme. The watermark is embedded into the SVD domain of the original image. SVD uses a non-fixed orthogonal basis, and it is a one-way non-symmetrical decomposition. These properties of SVD are used to improve the security and robustness of the scheme.

Watermarking approach can be blind and non-blind. Golea et al. [4] introduced the blind watermarking technique. This paper introduced an algorithm on which, watermark is embedded into the SVD transform of the RGB colour image. By this method, without using any extra information like matrices, which contains the information about the watermark, the watermark can be embedded and extracted. Techniques like this are called blind watermarking techniques.

Watermarking techniques also divided into Fragile and semi-fragile. Sun et al. [5] shown a semi-fragile watermarking technique based on block SVD. The binary

watermark image of pseudo-random permutation is embedded into the biggest singular value of the host image by quantisation process. To achieve more robustness and invisibility property, a lot of combined approach of DWT and SVD watermarking scheme is available. Abdallah et al. [6] proposed a watermarking scheme, in which, the DWT is a hierarchical four-channel filtering operation. Based on this scheme and with the help of Fast Hadamard Transform (FHT). FHT is applied to the small blocks computed from the four DWT sub-bands. The method is as follows: initially, DWT is applied to obtain the four sub-bands, and then those sub-bands are divided into different blocks. Then FHT is applied to each block, and finally, SVD is applied on the watermark and embedded in the transformed blocks.

SVD and DWT can be combined to get more effectiveness for the watermarking technique. Lai and Tsai [7] proposed a watermarking technique based on SVD and DWT. In this method, the watermark is embedded into singular values of the cover image rather than on the wavelet coefficients. By this way, this method fully utilises the respective feature of spatial-frequency localisation of DWT and SVD.

Khorasani and Sheikholeslami [8] presented a watermarking technique based on SVD and DWT. In this method, security is achieved by DWT. It is robust to various types of attacks since each sub-band includes the watermark in this method.

Ghaderi et al. [9] proposed another DWT and SVD based approach. This paper explained a watermarking technique based on SVD and DWT along with CPPN and a new proposed algorithm NEAT. Compositional Pattern Producing Network (CPPN) is used to make the representation of watermark to be very compact. NeuroEvolution Augmenting Topologies (NEAT) is used to develop a CPPN structure for producing a suitable watermark image. Watermarking process is as follows: (1) Decompose the host image with 2D-DWT at 5-level. (2) Apply SVD on *LH*3 to LH5 sub-bands of a horizontal image. (3) Embed the watermark by modifying the singular values of the original image. The extraction process is, (1) the embedded coefficients of CPPN NEAT are extracted from the watermarked image. (2) By using the extracted values and Gaussian functions, the watermark is rendered by CPPN. This method is robust against the attacks like average and median filtering, JPEG compression, rotation, contrast adjustment, noise addition, resizing, scaling and cropping and this method satisfies capacity, transparency, robustness and extraction key. Anita and Parmar [10] introduced a watermarking method based on SVD, DWT and fuzzy logic, which is robust against the attacks like salt and pepper and poison attacks.

For enhancing the security level of a digital content, chaotic system is widely used. In a chaotic system pixel, permutation-based encryption is used. Moniruzzaman et al. [11] discussed a watermarking technique based on DWT, SVD and chaotic system. According to this method, SVD and DWT are applied separately on the three colour planes of the original image and on the watermark. The chaotic technique is used for security of watermark by scrambling the watermark. On embedding, the watermark is embedded on the three colour planes of the cover image separately and on extraction, the watermark is extracted from those three colour planes, and an average of them is taken. This method is robust against attacks like cropping, filtering, rotation, JPEG compression and noise attacks.

A combined approach of DCT and DWT is the main current transform domain algorithm. Mainly DCT is used to selecting the low-frequency information of host image. As long as this information is not lost or loses only a little, then the host image can be renewed well, and another property is providing a compression mechanism. Deb

et al. [12] explained that by using this property of DCT and scalability property of DWT, a hybrid technique for image watermarking. It is performed based on these two techniques along with the low frequency watermarking with weighted correction. Weighted correction is used for imperceptibility. Watermark is embedded in the low-frequency band of each DCT block of selected DWT sub-bands. The extraction procedure is the reverse of that of embedding. It is robust to various attacks like JPEG compression, sharpening, cropping, and contrast adjustment and so on.

Akter and Ullah [13] discussed a hybrid technique for image watermarking based on DCT and DWT. It is performed by 2-level, 3-level and 4-level DWT algorithm followed by respective DCT on the host image. The embedding algorithm proposed in this paper is the New Embedding Algorithm (NEA).

Meng et al. [14] introduced a joint DWT-DCT transform technique for image watermarking, which utilises a) the visual characteristics of low-frequency sub-band of DWT and b) the ability of DCT technique to remove the correlation between DWT coefficients. Watermarking is made robust by embedding the watermark into spatial middle-frequency sub-bands of DWT and then to low-frequency coefficients of DCT. It is robust to the attacks like noise jamming, filtering, cutting and JPEG compression.

In the above description, DWT and SVD play an important role in watermarking. Now this paper presents a dual and multiple watermarking schemes for multilevel security. This paper explains the multi-watermark hiding scheme. The main advantage of this scheme is if any way hacker or faker knows one of the watermarks, but in this tedious situation, one of the watermarks is remaining. The second advantage of this paper is the capacity of hiding data in the original image is good; after hiding two different watermark image the quality of the watermarked image is good. This paper used SVD to optimise the DWT based scheme. The main advantage of this paper is multi-level security that means at first watermark is encrypted then embedding.

3. Proposed Method

This paper presents a dual watermark scheme based on DWT and SVD. Firstly, host image is divided into *LL, LH, HH* and *HL* sub-band by using DWT then *LL* sub-band is divided up to 3rd level. Encrypted QR Code and the logo image are two watermarks are taken to embedded into the *LL*3 and *HL*3 sub-band. During the watermark insertion process, SVD is applied to *LL*3, and *HL*3 sub-band and singular values are selected to embedding the watermark. Watermark encryption, embedding and recovery process is explained in sub-section. The advantage of this algorithm is providing multilevel security and authentication system. Here two watermarks are used for authentication purpose. If one watermark is hacked, the other watermark remains, thus providing another level of authentication. The second advantage of this algorithm is one watermark is encrypted form for providing the more security purpose of the watermark.

3.1. Encryption procedure

The image encryption procedure and algorithm is given below, and the graphical representation of this algorithm is shown in Fig. 1.

Step 1: Select an image for encryption.

Step 2: Apply DWT for original image, to decompose into 4 sub bands.

Step 3: Select *LL*1 sub band and find the dimension. [rows, columns, numberOfColorBands] = size (rgbImage).

Step 4: Set the order to scramble using randperm function.

Step 5: Extract the individual red, green, and blue colour channels of *LL*1.

Step 6: Scramble the redChannel, green channel and blue-channel according to the randperm function.

Step 7: Recombine separate colour channels into a single, true colour RGB.

Step 8: Display the scrambled *LL*1 sub-band, and select *LH*1 sub-band.

Step 9: Repeat step 6 to step 8 and display the scrambled *LH*1 sub-band.

Step 10: Similarly do the above step, and we find scrambled *HL*1 sub-band, scrambled HH1 sub-band.

Step 11: Combining the scrambled *LL*1 sub-band, scrambled *LH*1 sub-band, scrambled *HL*1 sub-band and scrambled HH1 sub-band by using inverse DWT.

Scrambled-image = idwt2 (Scrambled *LL*1 sub-band, Scrambled *LH*1 sub the band, scrambled *HL*1 sub-band, scrambled *HH*1 sub-band, 'haar');

Step 12: Get the scrambled image.

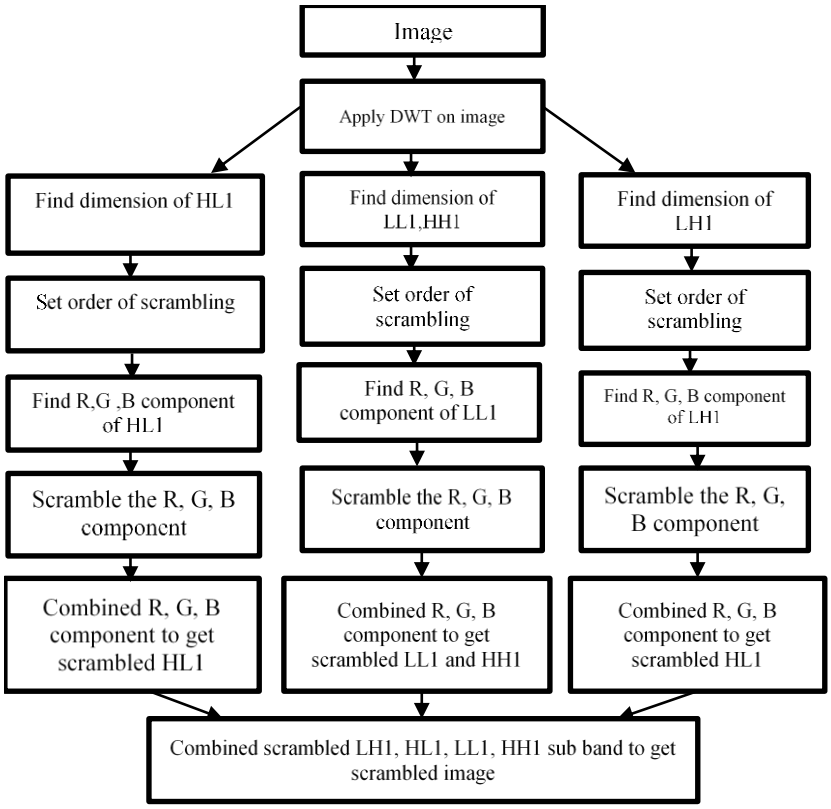

Fig. 1. Encryption process.

3.2. Decryption procedure

The image decryption procedure and algorithm are given below, and the graphical representation of this algorithm is shown in Fig. 2.

Step 1: Select the scrambled image.

Step 2: Apply DWT on scrambled image.

[Scrambled *LL*1 sub-band, Scrambled *LH*1 sub-band, scrambled *HL*1 sub Band, scrambled *HH*1 sub band] = dwt2 (scrambled image,'haar').

Step 3: Chose scrambled *LL*1 sub-band and converted its RGB colour component.

Step 4: Set the reverse of scrambled function.

Step 5: Unscramble the red channel, green channel and blue-channel according to the reverse of randperm function.

Step 6: Recombine separate colour channels into a single, true colour RGB.

Step 7: Get unscrambled *LL*1 sub-band.

Step 8: Select scrambled *LH*1 sub-band and converted it RGB colour component.

Step 9: Repeat step 4 to 6.

Step 10: Similarly chose scrambled *HL*1 sub-band, scrambled *HH*1 sub-band and repeat step 4 to 6.

Step 11: Combining the unscrambled *LL*1 sub-band, unscrambled *LH*1 sub-band, unscrambled *HL*1 sub-band and unscrambled *HH*1 sub-band by using Inverse DWT.

Scrambled-Image = idwt2 (unscrambled *LL*1 sub band, unscrambled *LH*1 sub band, unscrambled *HL*1 sub band, unscrambled *HH*1 sub band, 'haar').

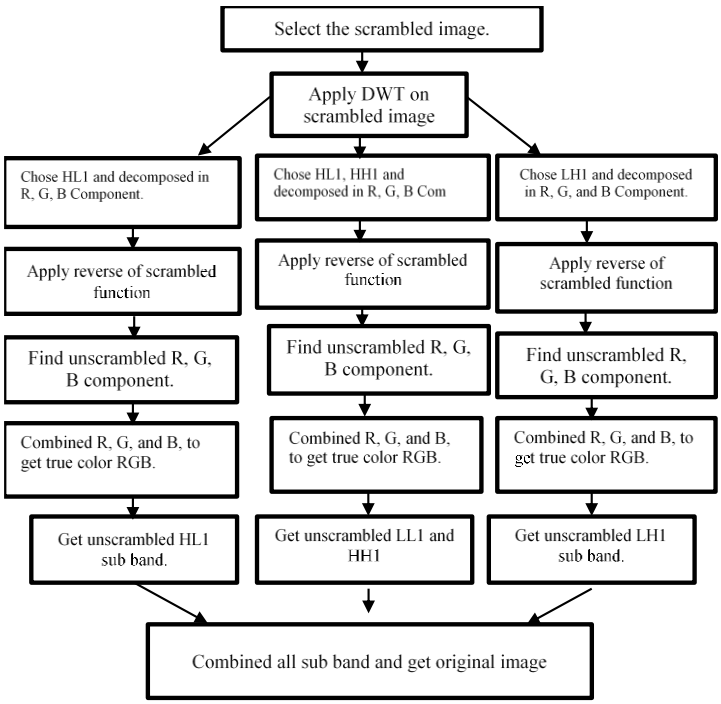

Fig. 2. Decryption process.

3.3. Embedding algorithm

In Fig. 3, we show the watermark embedding process. The embedding process is divided into 16 steps. The requirement for the embedding process is: all the watermark and the original images must be of the same dimension, let us say M×N Then, the process can be briefly described as follows:

Step 1: Apply DWT on the original image; the original image is decomposed into 4 sub-bands:

$[LL1, LH1, HL1, HH1] = dwt2(original\ Image)$.

Step 2: Apply DWT for *LL1* sub-band:

$[LL2, LH2, HL2, HH2] = dwt2(LL1)$

Step 3: Apply DWT for *LL*2 sub-band, to decompose into four sub-bands:

$$[LL3, H3, HL3, HH3] = dwt2(LL2)$$

Step 4: Apply SVD to *LL3* and *HL3* sub-bands.

$$Uh1\ Sh1\ \ Vh1 = SVS(LL3)$$

$$[Uh2\ Sh2\ Vh2] = SVD(HL3)$$

Step 5: A text is encoded by QR coding method, and it is treated as a watermark image. Then encrypt the QR code by given encryption techniques.

Step 6: Do steps 1-3 for encrypted QR code watermark image.

Step 7: Apply SVD to *LL*3 sub-band of the watermark:

$$[Uw1\ \ Sw1\ \ Vw1] = SVD(LL3)$$

Step 8: Embed the SVs of *LL*3 sub-band of the watermark image into that of the original image with a factor of α*:*

$$Sh = Sh1 + \alpha.Sw1$$

Step 9: By using the new *Sh* and *U* and *V* components of *LL*3 sub-band of the original image, recreate the *LL*3 sub-band:

$LL3_{modified} = Uh1 * Sh * Vh1^T$

Step 10: Do steps 1-3 for the logo image.

Step 11: Apply SVD to *HL*3 sub-band of the logo:

$$Ul1\ Sl1\ Vl1 = SVD(HL3)$$

Step 12: Embed the SVs of *HL*3 sub-band of the logo into that of the original image with a factor of α*:*

$Sh' = Sh2 + \alpha * Sl1$

Step 13: BY using the new Sh' and *U and V* components of *HL*3 sub-band of the original image recreate *HL3* sub-band:

$HL3_{modified} = Uh2 * Sh'\ * Vh2^T$

Step 14: By using the modified *LL*3 and *HH*3 sub-bands together with the old *LH*3 and *HH*3 sub-bands of the original image, take IDWT and treat the result as the modified *LL* sub-band for next level.

Step 15: By using the modified *LL* sub-band together with the remaining 3 sub-bands of 2nd level, recreate the modified *LL* sub-band for the final level by using IDWT.

Step 16: By using the modified *LL* sub-band together with the three other sub-bands of 1st level DWT of the original image, create the watermarked image by using IDWT.

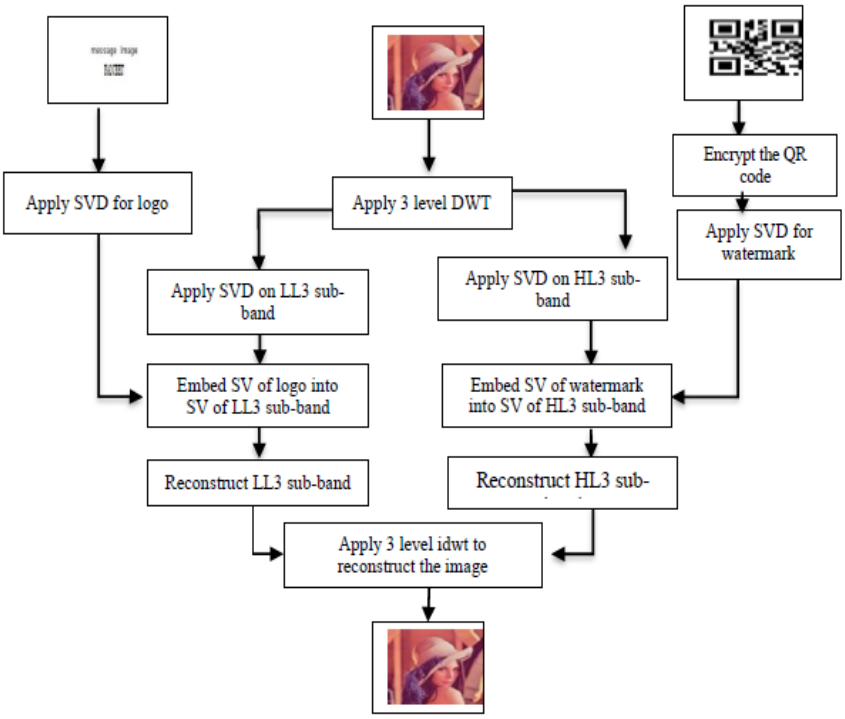

Fig. 3. Embedding process.

3.4. Extraction process

Watermark removal or extraction process is shown in Fig. 4. The extraction process is divided into 20 steps and is described as follows:

Step 1: Apply DWT for the watermarked image to decompose into four sub-bands:

$[LL1, LH1, HL1, HH1] = dwt2(Watermarked\ Image)$.

Step 2: Apply DWT for *LL*1 sub-band to decompose into four sub-bands:

$[LL2, LH2, HL2, HH2] = dwt2(LL1)$.

Step 3: Apply DWT for *LL*2 sub-band to decompose into four sub-bands:

$[LL3, LH3, HL3, HH3] = dwt2(LL2)$.

Step 4: Apply SVD to *LL*3 and *HL*3 sub-bands:

$[U_{wed1}\ S_{wed1}\ V_{wed1}\ ] = SVD(LL3)$.

$[U_{wed2}\ S_{wed2}\ V_{wed2}\ ] = SVD(HL3)$.

Step 5: Do steps 1-3 for the original image:

$[Uh1\ Sh1\ \ Vh1] = SVD(LL3)$.

Step 6: Apply SVD to *LL*3 sub-band of the original image.

Step 7: Do steps 1-3 for Encrypted QR code watermark image.

Step 8: Apply SVD to *LL*3 sub-band of watermark image:

$[Uw1 \;\; Sw1 \;\; Vw1] = SVD(LL3)$.

Step 9: Extract the SVs of *LL*3 sub-band of the watermark image from that of the watermarked image with a factor of α:

$$Swl' = (S_{wed1} - Sh1)/\alpha$$

Step 10: By using the new $Sw1'$ and *U and V* components of *LL*3 sub-band of the watermark image, recreate the *LL*3 sub-band:

$$LL3_{modified} = Uw1 * Sw1 * Vw1^T$$

Step 11: By using the modified *LL*3 sub-bands together with the remaining three sub-bands of the 3rd level of the watermark image, take IDWT and treat the result as the modified *LL* sub-band for the next level.

Step 12: By using the modified *LL* sub-band together with the remaining three sub-bands of 2nd level, recreate the modified *LL* sub-band for the final level by using IDWT.

Step 13: By using the modified *LL* sub-band together with the three other sub-bands of 1st level DWT of the watermark image, recreate the encrypted QR code watermark image by using IDWT then applying decryption procedure, we get the QR code.

Step 14: Redo steps 1-3 for the logo.

Step 15: Apply SVD to *HL*3 sub-band of the logo:

$[Ul1 \;\; Sl1 \;\; Vl1] = SVD(HL3)$.

Step 16: Apply SVD to *HL*3 sub-band of the original image:

$[Uh2 \;\; Sh2 \;\; Vh2]$=SVD (HL3).

Step 17: Extract the SVs of *HL*3 sub-band of the logo from that of the watermarked image with a factor of α*:*

$Sl1'$=(Swed1-Sh2)/α.

Step 18: BY using the new *Sl1* and *U and V* components of *HL*3 of the logo recreate the *HL*3 sub-band. By using the modified *HL*3 sub-bands together with the remaining sub-bands of the 3rd level of the watermark image, take IDWT and treat the result as the modified *LL* sub-band for the next level.

Step 20: By using the modified *LL* sub-band together with the remaining 3 sub-bands of 2nd level, recreate the modified *LL* sub-band for the final level by using IDWT:

$$HL3_{modified} = Ul1 * Sl1 * Vl1^T$$

Step 21: By using the modified *LL* sub-band together with the three others sub-bands of the 1st level of DWT, recreate the logo by using IDWT.

In the above experiment, authors take α = 0.10, because it gives the optimised result. The value of α less than 0.10 and greater than 0.10 not provide the optimal correlation coefficient between watermark and recover watermark and similarly in the case of peak signal to noise ratio.

However, in the case of α = 0.10, it gives the optimal correlation coefficient and peak signal to noise ratio also

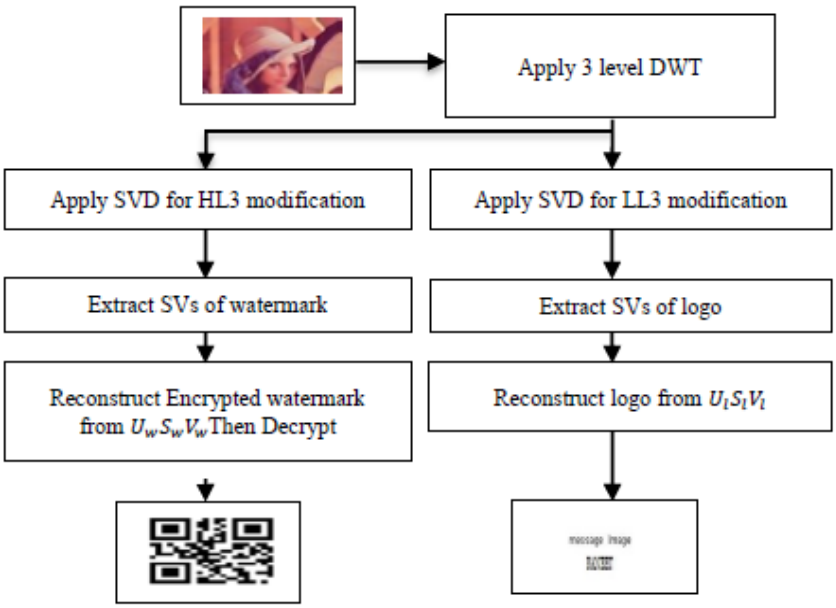

Fig. 4. Extraction process.

4. Result and Discussions

The proposed method is implemented in MATLAB software, and the results are tabulated below. For the experiments, we used to host images as "Lena", and watermark image as "Peugeot logo image" and a sample QR code with every image is of size 200×200 pixels, which are shown in Fig. 5.

(a) **(b)** **(c)**

Fig. 5. (a) Lena (host image), (b) Peugeot (watermark), (c) QR code(watermark).

We took CC values for comparing our results. CC (Correlation Coefficient) measures the similarity between two images. CC value can be calculated by using Eq. (1).

$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j) * w'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} w^2(i,j)} \quad (1)$$

where w and w' are original and extracted images respectively.

Initially, without any attacks, the obtained value of CC is 1 for original QR code and extracted QR code and original logo and extracted logo and after various

attacks like rotation, filtering, histogram equalisation, contrast adjustment, cropping, noise addition, transposing, etc. are done, and the results are tabulated in Tables 1 and 2 as a comparison with results of some other works.

Table 1. Comparison of robustness with [11, 15-17] for various attacks.

Attacks	[15]	[16]	[17]	[11]	Our (Logo)	Our (QR)
Median filter 3×3	0.7303	0.97832	0.6007	0.98727	0.9975	0.9983
Winner filter 5×5	0.7081	0.96146	0.4568	0.98316	0.9891	0.9942
Crop upper left corner (1/4)	0.6536	0.96728	0.9261	0.97559	0.9791	0.7275
Crop middle (1/4)	0.6147	0.91395	0.8973	0.95689	0.9788	0.5993
Crop lower right corner (1/4)	0.6458	0.95227	0.9247	0.97412	0.9966	0.8150
Rotate 15^0	0.6158	0.90317	0.9002	0.92139	0.9963	0.1988
Rotate 45^0	0.6027	0.89799	0.9000	0.91003	0.9786	0.0616
Gaussian noise (2%)	0.6821	0.99523	0.9658	0.99854	0.9827	0.3113

Table 2. Comparison of robustness with [18, 19] for attacks: Sharpen, cropping (1/4) area remaining and contrast adjustment.

Attacks (lena image)	[18]	[19]	Our
Sharpen	0.696	0.983	0.9987
Cropping (1/4) area remaining	0.900	0.466	0.7799
Contrast Adjustment	0.673	0.992	0.9860
Attacks (pepper image)	**[18]**	**[19]**	**Our**
Sharpen	0.712	0.969	0.9989
Cropping (1/4) area remaining	0.884	0.466	0.8668
Contrast Adjustment	0.737	0.973	0.9989
Attacks (plane image)	**[18]**	**[19]**	**Our**
Sharpen	0.746	0.990	0.9984
Cropping (1/4) area remaining	0.853	0.466	0.8477
Contrast Adjustment	0.758	0.997	0.9991

Makhloghi et al. [18] used DWT and SVD approach for watermarking. At first original image is divided into it's Red, Green and Blue component and each RGB Component is divided into four non-overlapping blocks. DWT is applied each non-overlapping block of RGB Component and chose *HL* and *LH* sub-band for SVD and found *S* component for watermarking. In this process, the computational complexity of the algorithm is increased due to a lot of block conversion. Because the original image is divided into its colour component, then each colour component is divided into four blocks. Due to this, the impact of rotation cropping and filtering is affected by the recovery process, and recover watermark is not good to the proposed method.

The proposed algorithm maintains the complexity of the algorithm without loss of authentication and security mechanism. In this paper, the authors used a third level DWT approach on the original image and then applied SVD on *LL*3 and *HL*3 for watermarking. Here the authors represent a dual watermark mechanism for multilevel security. Two watermarks are embedded in the original image without any loss of quality of the watermarked image. Quality

of recover watermark is good for different malicious attacks on watermarked image. Nguyen et al. [19] given a mechanism for more than one watermark embedding in the original image.

Here, authors used second level DWT and found out *HH*1 and *HH*2 sub-band for watermarking, and two watermark logos and QR Code is embedded in this sub-band. However, in our proposed algorithm, we used the third level of DWT for watermarking. Based on studies by Nguyen et al. [19], quality of the recovered watermark is better compared when cropping, sharping and contrast adjustment attacks are effected watermarked image. Table 1 represents the comparative result of Correlation Coefficient (CC) value of other existing DWT and SVD based methods [11, 15-17] to the new proposed method. The presented method specifies well robustness against a different type of attacks, i.e., cropping attack where $1/4^{th}$ pixels are removed from the upper left corner, lower right corner and middle, rotations, Median and winner filter of kernel size 3×3 and 5×5 and Gaussian noise of variance 2% etc., dominant the previous exiting method in CC values.

Tables 2 and 3 give CC value of watermark, i.e., the logo image and QR Code image using Lena as the cover image.

Tables 2 show the correlation coefficient between watermarks and recover the watermark image. Here watermark image is logo image. Similarly, Table 3 shows the correlation coefficient between watermarks and recovers the watermark image. Here watermark image is encrypted QR code image.

According to Makhloghi et al. [18], the results from Tables 2 and 3, which show that our proposed approach is more robust and Nguyen et al. [19] on sharpen attacks. Cropping (1/4) area remaining and contrast adjustment.

However, in the case of encrypted QR code as a watermark correlation coefficient is not comparatively good in the contrast adjustment and cropping (1/4) area remaining because the process to recovery encrypted QR code watermark then apply decryption mechanism to decrypt the watermark a lot of operation are performing on the image, therefore, so the pixel of the image are degraded.

Table 3. Comparison of robustness with [18, 19] for attacks: Sharpen, cropping (1/4) area remaining and contrast adjustment.

Attacks (lena image)	**[18]**	**[19]**	**Our**
Sharpen	0.696	(QR:0.988)	(QR:0.9990)
Cropping (1/4) area remaining	0.900	(QR:0.638)	(QR:0.0563)
Contrast adjustment	0.673	(QR:0.996)	(QR:0.8468)
Attacks (pepper image)	**[18]**	**[19]**	**Our (QR)**
Sharpen	0.712	(QR:0.982)	(QR:0.4902)
Cropping (1/4) area remaining	0.884	(QR:0.638)	(QR:0.0942)
Contrast adjustment	0.737	(QR:0.986)	(QR:0.4902)
Attacks (plane image)	**[18]**	**[19]**	**Our (QR)**
Sharpen	0.746	(QR:0.996)	(QR:0.9990)
Cropping (1/4) area remaining	0.853	(QR:0.638)	(QR:0.0270)
Contrast adjustment	0.758	(QR:0.998)	(QR:0.4857)

Table 4 represents the Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) between host image and watermarked image, logo image and recover logo image, Qr code and encrypted Qr code, Qr code and decrypted QR code, encrypted QR and recover QR code.

Figure 6 shows the correlation distributions of host image and watermarked image in horizontally, vertically and diagonally also and similarly Fig. 7 shows the correlation distributions of the watermark and recover watermark image in horizontally, vertically and diagonally.

Table 4. SNR, PSNR and MSE comparison.

Host image and watermarked image		
SNR	**PSNR**	**MSE**
22.5018	28.3329	95.4532
21.4349	28.2234	97.8913
21.4127	28.2100	98.1935
Logo image and recover logo image		
SNR	**PSNR**	**MSE**
26.5631	33.0025	32.5710
26.5631	33.0025	32.5710
26.5631	33.0025	32.5710
Qr code and encrypted QR code		
SNR	**PSNR**	**MSE**
6.2888	11.8809	4.2169e+003
6.2888	11.8809	4.2169e+003
6.2888	11.8809	4.2169e+003
Qr code and decrypted QR code		
SNR	**PSNR**	**MSE**
20.6175	26.2096	155.6410
20.6175	26.2096	155.6410
20.6175	26.2096	155.6410
Encrypted Qr and recover QR		
SNR	**PSNR**	**MSE**
6.3052	11.9371	4.1626e+003
6.3052	11.9371	4.1626e+003
6.3052	11.9371	4.1626e+003

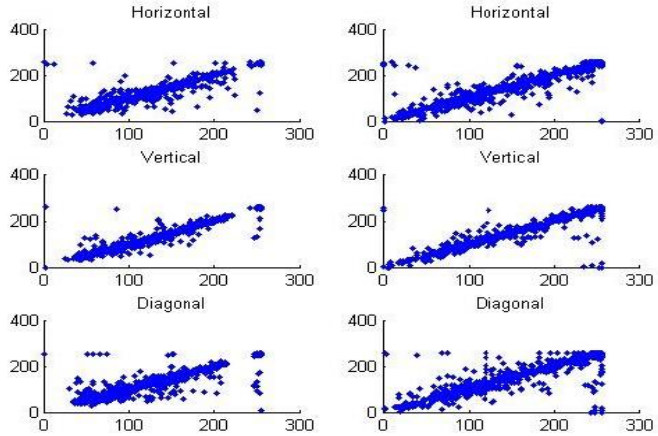

Fig. 6. Correlation distributions of host image and watermarked image.

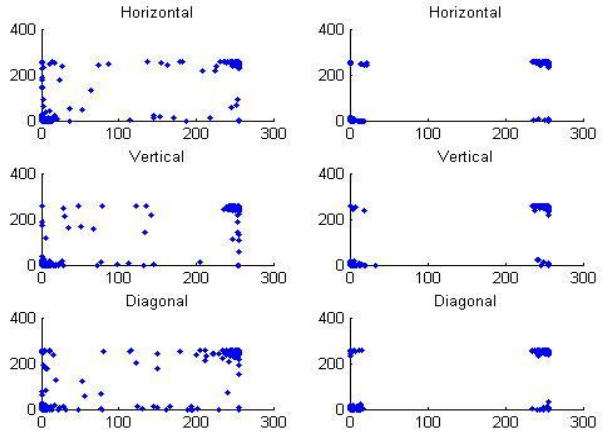

Fig. 7. Correlation distributions of watermark and recover watermark image.

5. Conclusion

In this paper, a dual watermark is embedded into an original image based on the combined approach of DWT and SVD. Where QR code watermark is embedded into *Ll*3 band, which is the third Level of *LL* Component and logo, is also embedded into *Hl*3 part of the third level of *LL*. Under the attack of cropping, rotation sharpens and adding noise the experimental result of a newly developed approach is improved in Robustness, and perceptibility compares to previously given approach.

Nomenclatures

HH	Both horizontally and vertically high pass
HL	Horizontally high-pass and vertically low-pass
LH	Vertically high-pass and horizontally low-pass
LL	Both horizontally and vertically low pass
S	Diagonal metric detail
U	Horizontal decomposition
V	Vertical decomposition

Abbreviation

CC	Correlation Coefficient
CPPN	Compositional Pattern Producing Network
DCT	Discrete Cosine Transform
DOF	Degree of Freedom
DWT	Discrete Wavelet Transform
FHT	Fast Hadamard Transform
NEA	New Embedding Algorithm
NEAT	Neuroevolution Augmenting Topologies
PSO	Particle Swarm Optimisation
QR Code	Quick Response Code
RGB	Red, Green, Blue
SVD	Singular Value Decomposition

References

1. Chang, C.-C.; Tsai, P.; and Lin, C.-C. (2005). SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, 26(10), 1577-1586.
2. Fan, M.-Q.; Wang, H.-X.; and Li, S.-K. (2008). Restudy on SVD-based watermarking scheme. *Applied Mathematics and Computation*, 203(2), 926-930.
3. Liu, R.; and Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 4(1), 121-128.
4. Golea, N.E.-H; Seghir, R.; and Benzid, R. (2010). A blind RGB colour image watermarking based on singular value decomposition. *Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*. Hammamet, Tunisia, 1-5.
5. Sun, R.; Sun, H.; and Yao, T. (2002). A SVD-and quantization based semi-fragile watermarking technique for image authentication (volume 2). *Proceedings of the 6th International Conference on Signal Processing*. Beijing, China, 1592-1595.
6. Abdallah, E.E.; Hamza, A.B.; and Bhattacharya, P. (2007). Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms. *Journal of Electronic Imaging*, 16(3), 033020-1-033020-9.
7. Lai, C.C.; and Tsai, C.C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement*, 59(11), 3060-3063.
8. Khorasani, M.K.; and Sheikholeslami, M.M. (2012). An DWT-SVD based digital image watermarking using a novel wavelet analysis function. *Proceedings of the Fourth International Conference on Computational Intelligence, Communication Systems and Networks.* Phuket, Thailand, 254-256.
9. Ghaderi, K.; Akhlghian, F.; and Moradi, P. (2012). A new digital image watermarking approach based on DWT-SVD and CPPN-NEAT. *Proceedings of the 2nd International eConference on Computer and Knowledge Engineering (ICCKE).* Mashhad, Iran, 12-17.
10. Anita; and Parmar, A. (2015). Image security using watermarking based on DWT-SVD and fuzzy logic. *Proceedings of the 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO).* Noida, India, 1-6.
11. Moniruzzaman, M.; Hawlader, M.A.K.; and Hossain, M.F. (2014). Robust RGB color image watermarking scheme based on DWT-SVD and chaotic system. *Proceedings of the 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. Dhaka, Bangladesh, 1-6.
12. Deb, K.; Al-Seraj, M.S.; Hoque, M.M.; and Sarkar, M.I.H. (2012). Combined DWT-DCT based digital image watermarking technique for copyright protection. *Proceedings of the 7th International Conference on Electrical and Computer Engineering.* Dhaka, Bangladesh, 4 pages.
13. Akter, A.; and Ullah, M.A. (2014). Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. *Proceedings of the International Conference on Informatics, Electronics and Vision (ICIEV).* Dhaka, Bangladesh, 6 pages.

14. Meng, Z.-Y.; Yu, P.-P.; and Yu, G.-Q. (2012). Copyright protection for digital image based on joint DWT-DCT transformation. *Proceedings of the International Conference on Wavelet Analysis and Pattern Recognition.* Xian, China, 11-14.
15. Liu, R.; and Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, 4(1), 121-128.
16. Liang, F.; and Wang, L. (2011). An improved wavelet-based color image watermark algorithm. *Journal of Computational Information Systems,* 7(6), 2013-2020.
17. Nasir, I.A.; and Abdurrman, A. (2013). A robust color image watermarking scheme based on image normalization. *Proceedings of the World Congress on Engineering (Volume 3).* London, United Kingdom, 6 pages.
18. Makhloghi, M.; Akhlaghian, F.; and Danyali, H. (2012). Robust blind DWT based digital image watermarking using singular value decomposition. *Proceedings of the 10th IEEE International Symposium on Signal Processing and Information Technology*. Luxor, Eqypt, 219-224.
19. Nguyen, T.H.; Duong, D.M.; and Duong, D.A. (2015). Robust and high capacity watermarking for image based on DWT-SVD. *Proceedings of the IEEE International Conference on Computing and Communication Technologies-Research, Innovation, and Vision for the Future (RIVF).* Can Tho, Vietnam, 83-88.