

A new approach for colored watermarking image into gray scale image using wavelet fusion

Alaa Fkirin¹ Gamal Attiya¹ · Ayman El-Sayed¹

Received: 7 March 2017/Accepted: 28 July 2017/Published online: 1 August 2017 © Springer Science+Business Media, LLC 2017

Abstract With the quick growth of technologies and great spread of the Internet, many challenges face data hiding. Nevertheless, significant data may be protected by burring it in an image as a watermark. This paper shows an efficient data hiding watermarking approach for color image by using singular value decomposition (SVD), multi-level discrete wavelet transform (DWT) and wavelet fusion. The main idea in this work is to separate the color image into its basic components (three channels); red, green, and blue. Then, fuse every channel with an image which is gray scale and integrate the three fused images into one gray scale fused image. Finally, the fused image is burred into a cover gray scale image to produce the watermarked image by using DWT and SVD. The proposed approach evaluation is done by using several images and different hacking on the transmitted image. The experimental results show that the marked images which are generated by the proposed approach are tolerant to versatile attacks such as Gaussian, blur, wrap, and cropping. Above all, the extracted watermark images are recognized even when the watermarked images suffered from attacks.

Keywords Image watermarking \cdot Wavelet fusion \cdot SVD \cdot DWT \cdot Data hiding

Alaa Fkirin eng.alaa.fkirin@el-eng.menofia.edu.eg

> Gamal Attiya gamal_mahrouce@yahoo.com

Ayman El-Sayed ayman.elsayed@el-eng.menofia.edu.eg

¹ Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

1 Introduction

In recent years, digital image watermarking is used widely to solve ownership issues and verify the authenticity issue of text, image, audio or video. Researchers have proposed a lot of effective techniques aiming to secure information, and copyright protection authentication (Wang et al. 2012). One can define watermarking as process of hiding data, which can be logo, signature, image, sound, label or text, into multimedia object (text, image, audio or video). The embedded object will be later extracted by the other side to achieve the intended purpose such as securing information, authentication of an object and checking ownership (AL-Mansoori and Kunhu 2012).

Watermarking techniques could be categorized into two essential groups that are in spatial domain or in frequency domain. In spatial domain, watermark is embedded directly into pixels of original image by changing pixel values themselves. Least significant bits (LSB) is the simplest technique of all spatial domain techniques, LSB is based on modifying the least significant bits of the original image by watermarking (Ali et al. 2014). Generally, most spatial domain techniques are easy to implement. Unfortunately, spatial domain techniques are not robust to attacks (Ali et al. 2014).

In frequency domain, embedding process is done by transforming representation of spatial domain into frequency domain then modifying its frequency coefficients to embed the watermark. There are a lot of transform domain watermarking methods such as Discrete Fourier Transforms (DFT) (Lu et al. 2010), Discrete Cosine Transforms (DCT) (Phadikar et al. 2011), SVD (Mohammad et al. 2008), and DWT (Ouhsain and Hamza 2009). Frequency domain techniques are better than most of spatial domain techniques in terms of resisting attacks, but require higher computational cost (Ali et al. 2014).

This paper presents an efficient digital image watermarking technique for color image hiding. The proposed approach embeds a color image into a gray scale image by using DWT, SVD and wavelet fusion. Image wavelet fusion is known as the process of combining two or more images to improve the quality and reduce redundancy (James and Dasarathy 2014). The main idea is to split the color image into three basic components (red, green, blue), then fuse every channel with a gray scale image, and integrate the three fused images to construct watermark image by using fusion. Finally, a stego-image is constructed by embedding the watermark into a gray scale cover image by using DWT and SVD. The stego-image then sent via Internet. The transmitted image will appear to attacker as a completely gray scale image.

The rest of this paper is organized as the following arrangement, Sect. 2 briefly discusses the problem of data hiding while Sect. 3 shows the previous related work to solve the problem. Section 4 presents the principles of watermarking and some details for the DWT, SVD and Wavelet Fusion algorithms. Section 5 presents the proposed approach embedding and extracting process. Section 6 introduces the image quality measures and presents the experimental results. Finally, the paper conclusions are shown in Sect. 7.

2 Problem statement

Today, many secret data are being transmitted on the Internet. However, most of secret important messages may get high risks while being transmitted over many public communication channels. The problem now is how to achieve safe secret communication of critical messages.

Some researchers show that a private message can be easily encrypted into some cipher text using a cryptographic technique like data encryption standard (DES) before sending out through the communication channel, to appear meaningless and hence guarantee safe secret communication. Nevertheless, the appearance of secret information as cipher texts readily attract the hackers' attention. Under such circumstances, if the message is attacked and decrypted by unwanted parity, the data will no longer be secured. In addition, even though chances for the hackers to perform decryption of ciphertexts is weak because of the cryptographic system strong security, at least the upset hackers can destroy the ciphertexts easily and spoil the transmission process.

To easily fix this problem, various kinds of plaintexts like images, audios, videos, etc., are used as a cover to hide the existence of the secret message from the attacker. Although there are multitude plaintext media, images are known to be the most commonly used as they are widely ubiquitous and readily found on the Internet. Also, the higher distortion tolerance degree that images have over other diverse kinds of plaintexts provides them with a very large hiding capacity.

3 Related work

Abdallah et al. (2007a) proposed a robust simple image watermarking technique which embed a watermark in transform domain using the fast Hadamard transform (FHT), DWT and SVD. The applied technique makes improvements in the data embedding system efficiently. As it improves the watermark imperceptibility and resist against several attacks. Abdallah et al. (2007b) proposed a tensor video watermarking scheme which is based on SVD technique. The main idea is to embed a watermark image into the stable coefficients of video frames. That can be applied by modifying singular values (SVs) of high order tensors which belongs to intra-frames video. The proposed method performance shows good robustness and surviving against various attacks such as frame averaging, frame dropping and geometric attacks.

Hemdan et al. (2013a) proposed a hybrid image watermarking technique that is based on fusing two gray scale images using wavelet fusion. Their experimental results demonstrate that wavelet fusion is really an efficient algorithm. Hemdan et al. (2013b) proposed a robust efficient hybrid watermarking technique which is based on wavelet fusing to two gray scale images using three-level DWT and wavelet fusion. Their proposed algorithm increases the embedded information capacity without affecting the original image perceptual scene, and is robust against severe attacks like Gaussian noise, filtering and cropping attacks.

Agarwal et al. (2014) proposed an optimized watermarking embedding and extracting technique which is based on DWT and SVD. The LL3 sub-band SVs coefficients of the cover image are modified by using of watermark SVs. Experimental results declare that the proposed technique guarantee high PSNR values, good visual quality after attack and high robustness against some image processing operations.

Mohananthini and Yamuna (2015) proposed a scheme which is based on fusing the two watermarks into single watermark then embed it into the cover original image using the discrete wavelet transforms. The experimental results declare that this proposed algorithm give the watermarked image good visual quality and is survival to a lot of image attacks like: Gaussian noise, salt and pepper noise, speckle noise, cropping, median filtering, and rotation.

Narula et al. (2015) proposed two watermarking approaches DWT and DWT–SVD which are applied to ensure image content security and watermark robustness. After that they applied both watermarking approaches and compared values of peak signal to noise ratio (PSNR). Experimental results show that the hybrid DWT–SVD is much better than DWT approach alone. It is shown that after applying the two watermarking approaches, the quality of the watermarked image degrades significantly when using DWT approach watermark embedding in comparison to DWT–SVD.

Naidu et al. (2016) proposed a DWT–SVD watermarking method that aims to embedding a single watermark image that can be exactly as large as the cover image. It is proved that modifying the cover image SVs of DWT domain provides highly robustness against several common attacks. Another beneficial point of DWT–SVD algorithm is high PSNR and high correlation coefficient of the watermarked image compared to the results of using only DWT.

4 Preliminaries

4.1 Principles of image watermarking

Generally, image-watermarking scheme has two main phases; embedding process, and extraction process, as shown in Fig. 1. In embedding process, the insertion of watermark into original image is done using an algorithm that produces watermarked image. This watermarked image is then transmitted to the other side via communication channel. It may pass safely or be exposed to an attack. In extraction process, the other side receives the watermarked image and uses that chosen algorithm to separate the watermark and original images. Without attack, the extracted watermark is often the same as the watermark before sending. However, with attack, without a robust algorithm, the extracted watermark will be ruined.

The image watermarking algorithm should fulfill the following requirements which must integrate with each other in addition to trade-offs in order to produce a powerful watermarking algorithm (Singh 2011):

- (1) *Robustness* the watermark shouldn't be affected or removed by an unauthorized party. Therefore, it should be very resilient against common signal processing manipulations like cropping, filtering, or compression.
- (2) Imperceptibility the watermark shouldn't degrade the quality of the original image and it shouldn't be observed by human naked eye.
- (3) *Capacity* maximum number of bits which can be buried in the original image.
- (4) Security watermark should be only detected by the authorized party.



Fig. 1 General framework of digital image watermarking. a Without attack, b with attack

4.2 Discrete wavelet transform

Discrete wavelet transform (DWT) is widely used in the field of signal processing. It can be used in removal of noise in audio as well as compression of image, audio and video. One dimensional DWT or one level DWT decomposes the image into 4 bands denoted by lower resolution image approximation (LL), horizontal (HL), vertical (LH) and diagonal (HH) as shown in Fig. 2a (Hemdan et al. 2013a; Mohamed 2010). Multi-level DWT is done by applying previous decomposition again on a band. The image can be decomposed onto N level wavelet transformation, as shown in Fig. 2b (Bhatnagar and Raman 2009).

4.3 Singular value decomposition

Singular value decomposition (SVD) is a mathematical technique that is based on linear algebra theorem which shows that the rectangular matrix 'A' can be decomposed into three matrices (Hemdan et al. 2013b): U (Orthogonal matrix), S (Diagonal matrix) and V (Transpose of an orthogonal matrix). The theorem can be presented usually as:

$$A = USV^T.$$
 (1)

4.4 Wavelet fusion

4.4.1 Definition

Image fusion is defined as the process that can combine two or more images into a single image which is called Fused Image. This is shown in Fig. 3. The fused image keeps most

Fig. 2 Discrete wavelet transform (DWT). a One level DWT, b Multi level DWT





Fig. 3 Fusion of two images

important features of the original cover image. Image fusion is a vital technique used in many applications such as computer vision, microscopic imaging, robotics and remote sensing (Hemdan et al. 2013b).

Image fusion's common form of transform is the wavelet transform fusion (Hill et al. 2002). First, two images are transformed into wavelet transforms. Then, the transformed images are combined in transform domain by using a defined fusion rule. At last images transformed back to spatial domain to give the resultant fused image. Mathematically wavelet transform fusion can be defined by considering wavelet transforms W of two registered input images $I_1(x, y)$ and $I_2(x, y)$ together with fusion rule \emptyset . After that, inverse wavelet transform ω^{-1} is computed, and fused image I(x, y) is reconstructed. This process is shown in Fig. 4 and expressed by Eq. (2) (Hill et al. 2002).

$$I(x,y) = \omega^{-1}(\emptyset(\omega(I_1(x,y))), \omega(I_2(x,y)))$$
(2)

4.4.2 Why to choose wavelet fusion?

The proposed approach applies multi-level wavelet decomposition for both the cover and watermark image. When images apply wavelet decomposition, their components are separated directly into bands which have approximately equal bandwidth. This idea is like retina of human eye when it splits any image into its components. So, it is expected to use discrete wavelet transform as it makes the independent processing of resulting components much like human eye. For that reason, using of wavelet decompositions for fusion of images is very popular. Fusion is known as the process of combining information (Kundur and Hatzinakos 1997).



Fig. 4 Fusion of wavelet transforms of two images

5 Proposed approach

In this section, color image watermarking approach is proposed. It is based on SVD, DWT and wavelet fusion techniques. The major goal of this proposal is to embed a colored watermark image into a gray scale image without perceptual degradation of colored watermark image taking into account robustness against common attacks. The proposed watermarking approach consists of two main phases; embedding phase and extraction phase.

5.1 Embedding process

Figure 5 illustrates the embedding process of the proposed algorithm. It works as follows:

- 1. Analyze/split colored watermark image into three channels; red, green, and blue.
- 2. Fuse every channel of colored image into the same gray scale image separately using wavelet fusion. This produces 'Fused Image1' for red channel, 'Fused Image2' for green channel and 'Fused Image3' for blue channel.
- 3. Fuse 'Fused Image1' and 'Fused Image2' using wavelet fusion to produce 'Fused mixed1'.



Fig. 5 Embedding process of the proposed approach

- 4. Fuse 'Fused mixed1' and 'Fused Image3' using wavelet fusion to produce 'Total Fused Watermark' that will be embedded onto an original gray scale image.
- 5. Apply one-level DWT to 'Original Image' as well as 'Total Fused Watermark'.
- 6. Apply SVD to A matrix of the resultant 'Total Fused Watermark'

$$A = U_1 S_1 V_1^T \tag{3}$$

7. Apply SVD to resultant 'Original Image' matrix B according to equation:

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

 Add SVs of Matrix B 'Original Image' to SVs of Matrix A 'Total Fused Watermark' according to equation

$$D = S + k * S_1 \tag{5}$$

where, k is a gain factor that controls the watermark strength.

9. Apply SVD to the new altered D matrix resultant from step 8 as:

$$S_w = U_w D V_w^T \tag{6}$$

10. Obtain resultant image A_w By using altered matrix:

$$A_w = U S_w V^T \tag{7}$$

11. Apply one-level inverse DWT (IDWT) to resultant image A_w To produce the 'Watermarked Image', which is gray scale image.

5.2 Extraction process

Figure 6 illustrates the extraction process of the proposed algorithm. It works as follows:

- 1. Apply one-level DWT to 'Extracted Watermarked Image' to produce 'Extracted Resultant Image'.
- 2. Apply SVD to 'Extracted Resultant Image' A_w^* matrix according to equation:

$$A_{w}^{*} = U^{*} S_{w}^{*} V^{*T}$$
(8)

3. Compute matrix D^* according to equation:

$$D^* = U_w S^*_w V^T_w \tag{9}$$

4. Obtain 'Extracted Total Fused Watermark' W* according to the equation.

$$W^* = \frac{D^* - S}{k} \tag{10}$$

- 5. Apply IDWT (inverse DWT) to construct the 'Extracted Total Fused Watermark'
- 6. Apply Anti-fusion on the resultant 'Extracted Total Fused Watermark' to produce 'Extracted Fused mixed1' and 'Extracted Fused Image3'.
- 7. Apply Anti-fusion to 'Extracted Fused mixed1' to produce 'Extracted Fused Image1' and 'Extracted Fused Image2'.
- Apply Anti-fusion to 'Extracted Fused Image1', 'Extracted Fused Image2' and 'Extracted Fused Image3' to produce the extracted channels (red, green, blue) respectively.
- 9. Combine the three extracted channels to obtain 'Extracted Colored Image'.



Fig. 6 Extraction process of the proposed approach

Note that * is a mark of probable corruption resultant from attacks.

6 Experimental results and discussion

The proposed algorithm is coded in MATLAB [®] R2015a environment and implemented on a PC which has 8 GB RAM and core i5 processor.

6.1 Quality metrics

In this paper, PSNR, Correlation (Cr) and mean square error (MSE) are chosen as quality measure factors (Avcibas et al. 2002, 2003)

6.1.1 Peak signal to noise ratio

Watermarked image quality can be measured by using peak signal to noise ratio (PSNR). In the ideal case, the PSNR should be infinite (AL-Mansoori and Kunhu 2012). In fact, this can't be accomplished with watermarked image. So, the larger PSNR the better. The PSNR is defined as:

$$PSNR = 10log_{10} \left(\frac{max * max}{MSE}\right)$$
(11)

where max = 255 for grey scale image.

6.1.2 Mean square error

Mean square error (MSE) is a standard quality measurement. In ideal case, the MSE must be zero(Mohamed and El Mohandes 2012; Planitz and Maeder 2005). In fact, this is can't be reached with watermarked image. So, the smaller the value of MSE, the better the quality is. MSE is defined as:

$$MSE = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{ORG(i,j) - WM(i,j)}{m \times n}$$
(12)

where, 'ORG' is original image, 'WM' is watermarked image and m & n are the original image width and height respectively.

6.1.3 Correlation coefficient

Correlation coefficient (Cr) is used in measuring closeness between original image and watermarked image. In ideal case, Cr should equal 1(Avcibas et al. 2003; Hemdan et al. 2013b). In real, this can't be achieved so the value of Cr near one. The Cr is defined as:





$$C_{r} = \frac{\sum_{m} \sum_{n} (Xi - X')(Yi - Y')}{\sqrt{\left(\sum_{m} \sum_{n} (Xi - X')^{2}\right) \left(\sum_{m} \sum_{n} (Yi - Y')^{2}\right)}}$$
(13)

where, X' is original image average value and Y' is watermarked image average value.

Note that, PSNR, MSE and Cr are calculated for gray scale image. For color image, the calculation of each parameter may be done by taking the average value of corresponding parameter of the colored image three channels because each channel is considered as a gray scale image.

| Gain factor | PSNR for color in | nage with and w | ithout attack | | | |
|-------------|-------------------|-----------------|---------------|--------|----------|--------|
| | Without attack | Gaussian | Blur | Wrap | Cropping | |
| | | | | | 50% | 75% |
| 0.1 | Infinity | 1.4542 | 3.2478 | 2.0634 | 1.4226 | 1.4257 |
| 0.2 | Infinity | 1.4558 | 4.9228 | 2.1633 | 1.4368 | 1.4366 |
| 0.3 | Infinity | 1.4567 | 6.2397 | 2.2543 | 1.4453 | 1.4438 |
| 0.4 | Infinity | 1.4567 | 7.2606 | 2.3379 | 1.4506 | 1.4485 |
| 0.5 | Infinity | 1.4567 | 8.0715 | 2.4155 | 1.4541 | 1.4512 |
| 0.6 | Infinity | 1.4567 | 8.7348 | 2.4930 | 1.4567 | 1.4531 |
| 0.7 | Infinity | 1.4567 | 9.2940 | 2.5624 | 1.4589 | 1.4544 |
| 0.8 | Infinity | 1.4567 | 9.7694 | 2.6235 | 1.4609 | 1.4553 |
| 0.9 | Infinity | 1.4567 | 10.1810 | 2.6773 | 1.4627 | 1.4560 |
| 1 | Infinity | 1.4567 | 10.5417 | 2.7257 | 1.4645 | 1.4566 |

Table 1 Results for first quarter (Ll) at various gain factor

Table 2 Results for second quarter (LH) at various gain factor

| Gain factor | PSNR for color in | nage with and | without attack | | | |
|-------------|-------------------|---------------|----------------|---------|----------|---------|
| | Without attack | Gaussian | Blur | Wrap | Cropping | |
| | | | | | 50% | 75% |
| 0.1 | Infinity | 9.1258 | 9.5913 | 12.9723 | 10.5532 | 9.3787 |
| 0.2 | Infinity | 10.6126 | 11.2315 | 16.1264 | 13.3271 | 10.9091 |
| 0.3 | Infinity | 11.5879 | 12.3607 | 18.1082 | 15.2771 | 11.9490 |
| 0.4 | Infinity | 12.3536 | 13.2529 | 19.4998 | 16.7817 | 12.7849 |
| 0.5 | Infinity | 12.9964 | 13.9889 | 20.5637 | 17.9796 | 13.4952 |
| 0.6 | Infinity | 13.5516 | 14.6134 | 21.4048 | 18.9578 | 14.1109 |
| 0.7 | Infinity | 14.0372 | 15.1487 | 22.0901 | 19.7794 | 14.6500 |
| 0.8 | Infinity | 14.4685 | 15.6153 | 22.6579 | 20.4788 | 15.1296 |
| 0.9 | Infinity | 14.8539 | 16.0233 | 23.1372 | 21.0797 | 15.5584 |
| 1 | Infinity | 15.2016 | 16.3829 | 23.5486 | 21.6031 | 15.9421 |

| Gain factor | PSNR for color in | nage with and v | without attack | | | |
|-------------|-------------------|-----------------|----------------|---------|----------|---------|
| | Without attack | Gaussian | Blur | Wrap | Cropping | |
| | | | | | 50% | 75% |
| 0.1 | Infinity | 8.5364 | 8.9077 | 10.0377 | 10.2521 | 8.8249 |
| 0.2 | Infinity | 9.9702 | 10.5697 | 14.0109 | 12.9812 | 10.4974 |
| 0.3 | Infinity | 10.9137 | 11.6657 | 16.7379 | 14.8200 | 11.6014 |
| 0.4 | Infinity | 11.6277 | 12.5129 | 18.6322 | 16.2243 | 12.4671 |
| 0.5 | Infinity | 12.2221 | 13.2082 | 19.8897 | 17.3567 | 13.1892 |
| 0.6 | Infinity | 12.7348 | 13.7861 | 20.7061 | 18.2985 | 13.8028 |
| 0.7 | Infinity | 13.1855 | 14.2722 | 21.2267 | 19.0907 | 14.3289 |
| 0.8 | Infinity | 13.5812 | 14.6910 | 21.5535 | 19.7707 | 14.7925 |
| 0.9 | Infinity | 13.9283 | 15.0580 | 21.7579 | 20.3588 | 15.2013 |
| 1 | Infinity | 14.2375 | 15.3818 | 21.8843 | 20.8715 | 15.5693 |

Table 3 Results for third quarter (HL) at various gain factor

Table 4 Results for fourth quarter (HH) at various gain factor

| Gain factor | PSNR for color in | nage with and | without attack | | | |
|-------------|-------------------|---------------|----------------|---------|----------|---------|
| | Without attack | Gaussian | Blur | Wrap | Cropping | |
| | | | | | 50% | 75% |
| 0.1 | Infinity | 10.8045 | 10.9804 | 16.3009 | 13.9870 | 11.0712 |
| 0.2 | Infinity | 12.8442 | 13.0756 | 20.7089 | 17.9863 | 13.2913 |
| 0.3 | Infinity | 14.2620 | 14.5265 | 22.9977 | 20.6015 | 14.8646 |
| 0.4 | Infinity | 15.3797 | 15.6633 | 24.3728 | 22.4773 | 16.1067 |
| 0.5 | Infinity | 16.2974 | 16.5911 | 25.2710 | 23.9092 | 17.1066 |
| 0.6 | Infinity | 17.0589 | 17.3560 | 25.8913 | 25.0487 | 17.9447 |
| 0.7 | Infinity | 17.7109 | 18.0129 | 26.3400 | 25.9833 | 18.6667 |
| 0.8 | Infinity | 18.2812 | 18.5845 | 26.6760 | 26.7676 | 19.2952 |
| 0.9 | Infinity | 18.7825 | 19.0845 | 26.9376 | 27.4397 | 19.8467 |
| 1 | Infinity | 19.2273 | 19.5288 | 27.1443 | 28.0183 | 20.3318 |

| Table 5 | Results | for | best | Case |
|-----------|---------|------|------|------|
| (sub-band | l HH wi | th g | ain | |
| factor = | 1) | | | |

| | MSE | PSNR | Cr |
|----------------|---------|----------|--------|
| Without attack | 0 | Infinity | 1 |
| Gaussian | 41.1456 | 19.2275 | 0.9219 |
| Blur | 40.2732 | 19.5288 | 0.9265 |
| Wrap | 22.1651 | 27.1443 | 0.9859 |
| Cropping 50% | 28.6422 | 28.0183 | 0.9886 |
| Cropping 75% | 39.6652 | 20.3318 | 0.9374 |
| | | | |

Table 6 Test images

Case Gray scale image with its name in MATLAB Color watermark image with its name in MATLAB



В

A



С

D

Е



uag.



coins.png





board.tif



autumn.tif



coloredChips.png



concordaerial.png



fabric.png

| \$ |
|-----------|
| le |
| Lab |
| Ľ |
| s II |
| image |
| for |
| 1 |
| Ш |
| factor |
| gain |
| with |
| ΗH |
| (sub-band |
| case |
| best |
| for |
| Results |
| 1 |
| able |

| Table ['] | 7 Resul | ts for bes | st cas | e (sub-ban | d HH wit | h gain fac | stor $= 1$) f | or image | s in Tabl | e 6 | | | | | | | | |
|--------------------|---------|------------|--------|------------|----------|------------|----------------|----------|-----------|---------|---------|--------|----------|---------|--------|---------|---------|--------|
| Cases | With n | o attack | | Gaussiar | _ | | Blur | | | Wrap | | | Cropping | | | | | |
| | MSE | PSNR | C | MSE | PSNR | Cr | MSE | PSNR | Cr | MSE | PSNR | Cr | 50% | | | 75% | | |
| | | | | | | | | | | | | | MSE | PSNR | Cr | MSE | PSNR | Cr |
| А | 0 | Infinity | - | 79.9026 | 15.4822 | 0.7310 | 79.1438 | 15.6294 | 0.7379 | 63.4243 | 19.2873 | 0.8706 | 58.8958 | 22.2817 | 0.9323 | 72.4404 | 18.6295 | 0.8524 |
| в | 0 | Infinity | - | 63.7023 | 17.7546 | 0.9106 | 62.2523 | 18.0513 | 0.9158 | 36.3661 | 23.3144 | 0.9726 | 46.7114 | 23.9768 | 0.9762 | 59.9034 | 19.8296 | 0.9413 |
| C | 0 | Infinity | - | 71.6360 | 19.6657 | 0.8927 | 68.2189 | 20.4544 | 0.9086 | 18.9489 | 31.9096 | 0.9927 | 39.7178 | 27.5323 | 0.9802 | 60.2280 | 23.2231 | 0.9488 |
| D | 0 | Infinity | 1 | 77.8928 | 18.5934 | 0.6822 | 75.8797 | 19.0404 | 0.7029 | 39.4189 | 27.0392 | 0.9340 | 38.5687 | 27.9962 | 0.9468 | 65.9987 | 21.9608 | 0.8186 |
| щ | 0 | Infinity | - | 92.1187 | 16.4462 | 0.7098 | 90.6826 | 16.8125 | 0.7262 | 69.9691 | 21.4120 | 0.8798 | 60.9132 | 24.3807 | 0.9353 | 81.7715 | 20.0511 | 0.8458 |
| | | | ĺ | | | | | | | | | | | | | | | |

6.2 Experimental results

In this section, several experiments are carried out to evaluate performance of the proposed watermarking approach. Here, the proposed approach is tested on variety of reference test images (different original and watermark images) and different attacks.

6.2.1 First case

The first test is carried out by using "elephant.jpg" image as the original/cover image and "bg_global_logo.jpg" image as color watermark image, as shown in Fig. 7. The purpose is to determine the best quarter (LL, LH, HL or HH) to embed the watermark and to find the proper gain factor. Indeed, to test robustness of the proposed watermarking approach several kinds of common attacks have been used. Four types of attacks have been applied on watermarked image including: Gaussian noise, blurring filtering, wrap and cropping (50 and 75%).Both watermarked image and its attacked version are taken in account to calculate robustness of watermarking. Tables 1, 2, 3, and 4 show PSNR for color image with and without attack for the sub-bands LL, LH, HL and HH respectively, at various gain factor from 0.1 to 1. These results show that, with no attack PSNR equals infinity. This means that extracted image after attack is identical to the watermark image before attack. Also, it is obvious from the results that PSNR increases as gain factor increases. From these results, embedding a color watermark image into a gray scale image in HH sub-band



Fig. 8 Proposed embedding algorithm for images in Fig. 7

achieves best results compared to results from other bands. This deduction proves that, the best quarter for embedding a color watermark image into a gray scale image is the fourth quarter (HH) with gain factor equal to 1. Table 5 shows MSE, PSNR, and Cr at best case, sub-band HH with gain factor 1.



Fig. 9 Proposed extraction algorithm for images in Fig. 7

Fig. 10 Extracted color image



| Level | PSNR for color in | nage with and w | ithout attack | | | |
|-------|-------------------|-----------------|---------------|---------|----------|---------|
| | Without attack | Gaussian | Blur | Wrap | Cropping | |
| | | | | | 50% | 75% |
| 1 | Infinity | 19.2275 | 19.5288 | 27.1443 | 28.0183 | 20.3318 |
| 2 | Infinity | 21.8606 | 22.0355 | 28.9460 | 30.7397 | 23.1762 |
| 3 | Infinity | 28.4985 | 28.6600 | 34.0963 | 37.5943 | 30.0615 |
| 4 | Infinity | 33.0333 | 33.1359 | 37.8827 | 41.7287 | 34.1651 |
| 5 | Infinity | 39.8040 | 40.0347 | 43.6855 | 47.5301 | 41.5112 |
| 6 | Infinity | 43.9664 | 43.9664 | 45.9154 | 50.4765 | 45.2023 |

Table 8 Results of multilevel DWT for HH and gain factor = 1



Fig. 11 Quality improvement of extracted image

6.2.2 Other cases

Evaluation of proposed watermarking approach is done with several color watermark images and gray images which play the role of host/cover image. Test images are selected from MATLAB image database. Table 6 shows test images used with their names in MATLAB. In addition, four types of attacks have been applied to the watermarked image including: Gaussian noise, blurring filtering, wrap and cropping. Table 7 shows experimental results for different images considering sub-band HH with gain factor =1. It shows MSE, PSNR, and Cr with and without attack.

6.2.3 Limitations of one level DWT

Although proposed watermark approach is robust against attacks, the quality of the extracted image after attack is low. Figure 8, shows the various stages of embedding process in HH sub-band while Fig. 9, shows the various stages of extraction process. Figure 10, shows extracted color image after Gaussian noise attack. It is clear from Fig. 10, that the extracted image quality is low. The extracted image reveals some details of original image (elephant image). This problem appears also with all other types of test cases in Table 7

| 1 | |
|----------------------------|--|
| nd HH with gain factor = 1 | |
| -baı | |
| sub | |
| 6 considering | |
| ble | |
| Tal | |
| images of | |
| for | |
| evel | |
| oth] | |
| nd (| |
| evel a | |
| st l(| |
| between 1 | |
| Comparison | |
| PSNR | |
| 6 0 | |
| Table | |

| Cases | With no at | tack | Gaussian | | Blur | | Wrap | | Cropping | | | |
|------------------|------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| | 6th level | 1st level | 6th level | 1st level | 6th level | 1st level | 6th level | 1st level | 50% | | 75% | |
| | | | | | | | | | 6th level | 1st level | 6th level | 1st level |
| Case under study | Infinity | Infinity | 43.9664 | 19.2275 | 43.9664 | 19.5288 | 45.9154 | 27.1443 | 50.4765 | 28.0183 | 45.2023 | 20.3318 |
| A | Infinity | Infinity | 43.9519 | 15.4822 | 44.1758 | 15.6294 | 47.1950 | 19.2873 | 48.9340 | 22.2817 | 46.5739 | 18.6295 |
| В | Infinity | Infinity | 45.0733 | 17.7546 | 45.0733 | 18.0513 | 53.8104 | 23.3144 | 55.4008 | 23.9768 | 46.7152 | 19.8296 |
| C | Infinity | Infinity | 44.6848 | 19.6657 | 45.0603 | 20.4544 | 50.5543 | 31.9096 | 53.1916 | 27.5323 | 48.7371 | 23.2231 |
| D | Infinity | Infinity | 45.8833 | 18.5934 | 45.8833 | 19.0404 | 50.6361 | 27.0392 | 52.5023 | 27.9962 | 48.4068 | 21.9608 |
| Е | Infinity | Infinity | 45.1421 | 16.4462 | 45.4467 | 16.8125 | 48.7711 | 21.4120 | 51.5102 | 24.3807 | 46.9051 | 20.0511 |
| | | | | | | | | | | | | |

6.2.4 Suggested solution

To solve the low-quality problem of the extracted image, the proposed approach is modified by using multi-level DWT instead of using one level DWT. The problem now is to determine which level of the DWT is the best for embedding process. Table 8 shows PSNR of color image for first 6 levels of multilevel DWT considering the fourth quarter (HH) and gain factor =1. This test is done on test images shown in Fig. 7, where, "elephant.jpg" image is used as the original/cover image and "bg_global_logo.jpg" image is used as a colored watermark image. From Table 8, level 6 DWT achieves best PSNR value.

Figure 11, shows quality improvement of extracted image. It shows the extracted image when using level 6 of multilevel DWT and extracted image when using level 1 DWT.

Table 9 shows a comparative study between the PSNR of color image when applying 1 level DWT and applying 6 level DWT on test images of Table 6. The results indicate that applying 6th level DWT is better than applying 1st level DWT.

7 Conclusion

In this paper, a new efficient color image watermarking approach for data hiding by using SVD, multi- DWT and wavelet fusion is developed, discussed, and tested. The suitable quarter of DWT and suitable gain factor are first selected. Then, many tests are done using the best HH quarter with gain factor 1 with and without attack. Another improvement has been achieved in the proposed watermarking approach by applying 6th level DWT to overcome the problem of revealing some details of original image in the extracted image. The simulation results demonstrate that watermarked images generated by proposed watermarking approach are tolerant to versatile attacks such as Gaussian, blur, wrap, and cropping. The experimental results prove that using multi-level DWT improves colored watermark image quality after extraction. In addition, experimental results show that using the 6th level DWT is more robust against severe attacks.

Acknowledgements Funding was provided by Academy of Scientific Research and Technology.

References

- Abdallah, E.E., Hamza, A.B., Bhattacharya, P.: Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms. J. Electron. Imaging 16, 1–9 (2007). doi:10.1117/1.2764466
- Abdallah, E.E., Hamza, A.B., Bhattacharya, P.: MPEG video watermarking using tensor singular value decomposition. In: Proceeding of Image Analysis and Recognition, pp. 772–783 (2007b)
- Agarwal, C., Mishra, A., Sharma, A., Bedi, P.: Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. Expert Syst. Appl. 41, 7858–7867 (2014). doi:10.1016/j.eswa.2014.06.011
- AL-Mansoori, S., Kunhu, A.: Robust watermarking technique based on DCT to protect the ownership of DubaiSat-1 images against attacks. Int. J. Comput. Sci. Netw. Secur. (IJCSNS) 12, 1–9 (2012)
- Ali, M., Ahn, C.W., Pant, M.: A robust image watermarking technique using SVD and differential evolution in DCT domain. Int. J. Light Electron. Opt. 125, 428–434 (2014). doi:10.1016/j.ijleo.2013.06.082
- Avcıbas, I., Memon, N., Sankur, B.: Steganalysis using image quality metrics. IEEE Trans. Image Process. 12, 221–229 (2003)
- Avcıbas, I., Sankur, B., Sayood, K.: Statistical evaluation of image quality measures. J. Electron. Imaging 11, 206–223 (2002). doi:10.1117/1.1455011

- Bhatnagar, G., Raman, B.: A new robust reference watermarking scheme based on DWT–SVD. Comput. Stand. Interfaces 31, 1002–1013 (2009). doi:10.1016/j.csi.2008.09.031
- Hemdan, E.E.D., El Fishawy, N., Attiya, G., El-Samie, F.A.: Hybrid digital image watermarking technique for data hiding. In: Proceeding of 30th National Radio Science Conference (NRSC 2013), pp. 220–227 (2013a)
- Hemdan, E.E.D., El Fishawy, N., Attiya, G., El-Samie, F.A.: An efficient image watermarking approach based on wavelet fusion and singular value decomposition in wavelet domain. In: Proceeding of 3rd International Conference on Advanced Control Circuits And Systems (ACCS'013) (2013b)
- Hill, P., Canagarajah, N., Bull, D.: Image fusion using complex wavelets. In: Proceeding of the 13th British Machine Vision Conference (BMVC), pp. 487–496 (2002)
- James, A.P., Dasarathy, B.V.: Medical image fusion: a survey of the state of the art. Inf. Fusion 19, 4–19 (2014)
- Kundur, D., Hatzinakos, D.: A robust digital image watermarking method using wavelet-based fusion. In: Proceeding of International Conference on Image Processing, pp. 544–547 (1997)
- Lu, W., Lu, H., Chung, F.-L.: Feature based robust watermarking using image normalization. Comput. Electr. Eng. 36, 2–18 (2010). doi:10.1016/j.compeleceng.2009.04.002
- Mohamed, M.A.: Choosing the best digital watermarking techniques for still images. Mediterr. J. Comput. Netw. 6, 101–107 (2010)
- Mohamed, M.A., El Mohandes, A.M.: Hybrid DCT-DWT watermarking and IDEA encryption of internet contents. Int. J. Comput. Sci. Issues (IJCSI) 9, 394–401 (2012)
- Mohammad, A.A., Alhaj, A., Shaltaf, S.: An improved SVD-based watermarking scheme for protecting rightful ownership. Signal Process. 88, 2158–2180 (2008). doi:10.1016/j.sigpro.2008.02.015
- Mohananthini, N., Yamuna, G.: Image fusion process for multiple watermarking schemes against attacks. J. Netw. Commun. Emerg. Technol. (JNCET) 1, 1–8 (2015)
- Naidu, A.R., Akhila, K., Mounica, G., Sony, J.: Analysis of robust DWT–SVD domain based digital image watermarking technique. Int. J. Appl. Sci. Eng. Manag. 5, 94–97 (2016)
- Narula, N., Sethi, D., Bhattacharya, P.P.: Comparative analysis of DWT and DWT–SVD watermarking techniques in RGB images. Int. J. Signal Process. Image Process. Pattern Recognit. 8, 339–348 (2015)
- Ouhsain, M., Hamza, A.: Ben: image watermarking scheme using nonnegative matrix factorization and wavelet transform. Expert Syst. Appl. 36, 2123–2129 (2009). doi:10.1016/j.eswa.2007.12.046
- Phadikar, A., Maity, S.P., Verma, B.: Region based QIM digital watermarking scheme for image database in DCT domain. Comput. Electr. Eng. 37, 339–355 (2011). doi:10.1016/j.compeleceng.2011.02.002
- Planitz, B., Maeder, A.: Medical image watermarking: a study on image degradation. In: Society Workshop on Digital Image (2005)
- Singh, V.: Digital watermarking: a tutorial. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. (JSAT), 10–21 (2011)
- Wang, X., Qin, Q., Cheng, Y.: Design and implementation of digital image watermark based on FPGA. In: Recent Advances in Computer Science and Information Engineering, pp. 223–229. Springer Berlin Heidelberg (2012)