Wireless Personal Communications
https://doi.org/10.1007/s11277-020-07567-w

Watermark Visibility Adjustable RVW Scheme for JPEG Images

D. R. Denslin Brabin[1] · **J. Raja Paul Perinbam**[2] · **D. Meganathan**[3]

© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In digital images, visible watermarks are embedded to convey the ownership information directly to the world so that copyright violations can be prevented. The removable visible watermarking (RVW) techniques allow the authorized user to remove the watermark from the watermarked image and restore the host image with permissible loss. Usually the visibility of the watermark can't be increased or decreased based on the application requirement. In most of the commercial communication, JPEG images are used over the internet because of its reduced size. In this paper a RVW scheme is proposed for JPEG images which allows the user to embed watermark in the host image with variable visibility levels. In this scheme, the watermark embedding is performed by modifying the frequency coefficients of host image during forward Discrete Cosine Transform phase of JPEG compression. Inverse operation is performed to remove the watermark and to recover the host image. Watermark key is used to enhance the security of watermarking scheme. Quality metrics of visible watermarking technique are confirmed through experiments.

Keywords Data hiding · DCT · JPEG · Removable visible watermarking

1 Introduction

Data hiding is a prominent area in information security which embeds secret data in digital media. It can be broadly categorized into steganography and watermarking. Steganography embeds secret information directly in digital media such as text, image, audio and video

✉ D. R. Denslin Brabin
denscse@gmail.com

J. Raja Paul Perinbam
rperinbam@yahoo.com

D. Meganathan
meganathan_phd@annauniv.edu

[1] Department of Computer Science and Engineering, Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

[2] Department of Electronics and Communication Engineering, Kings Engineering College, Chennai, India

[3] Department of Electronics Engineering, Anna University, Chennai, India

Published online: 19 June 2020

with the intention of secret communication. Watermarking embeds secret information, copyright information or ownership information directly in digital media with the intention of copyright protection. The secret data or watermark can also be in any format such as text, image, audio and video. Digital images are mostly affected by copyright violation because they can be easily copied and modified without any visible articrafts. So watermarking in digital images is always having a special part in watermarking domain. There are two categories of watermarking techniques for digital images: *invisible* and *visible*. The invisible watermarking techniques embed secret information or copyright information into a digital media in an undetectable manner. That means the watermark is secretly embedded in the host image that cannot be seen by any user through human visual system (HVS).

In contrast, the visible watermarking techniques embed copyright information or ownership information in a digital image which can be clearly seen by any user through HVS. It directly conveys the copyright information, but it cannot be removed by unauthorized users. The uses of watermarking in digital images are copyright protection, ownership identification, prevention of illegal use (includes copy, modification, personalization), integrity checking etc. Reversible data hiding (RDH) techniques allow the authorized users to reconstruct the host image to its original form after the removal of secret data or watermark. In RVW, the visible watermark that is embedded into a digital image can be removed and the host image can be recovered without distortion or with permissible distortion by any authorized users.

In commercial applications, valuable images are digitalized, compressed and then published over the Internet by many service providers and individuals. The most preferred image format in Internet is Joint Photographic Experts Group (JPEG) image format. JPEG compression yields fast transmission, less memory absorption, good image quality, easy downloading and uploading. There are lots of security risks to these images that vary from transmission errors to creating forged images. Most of these security problems can be solved by visible watermarking techniques.

Most of the existing watermarking techniques presented in Sect. 2 can embed visible watermarks in digital images, but the visibility or transparency of the watermark in the host image cannot be varied (it is fixed). In this paper, a watermark visibility adjustable RVW scheme is proposed for JPEG compressed images. The remaining parts of this paper are organized as follows. Sections 3 details about watermark embedding process and watermark removing process. Section 4 shows the experimental results and performance confirmation of the proposed RVW scheme. The conclusions and the suggestions for future work are conveyed in Sect. 5.

2 Literature Survey

Considerable quantity of research works were carried out on steganography and watermarking domain over the past few years. The steganography and watermarking techniques [1–8] embed secret data or watermarks in the original host images. In receiving side, after the removal of watermark, the host image is highly distorted that cannot be recovered to its original form. Some of the recent RDH and RVW schemes denoted below can embed watermark in the original host images and the host image can be recovered to its original form after the removal of the watermark.

Hu et al. [9] proposed a difference expansion based RDH scheme, in which the difference between the original image pixel and predicted image pixel is expanded to hide one

bit of secret data. In the extraction side, same predicted pixel is calculated to extract secret data and to recover the host image. The overflow and underflow pixels are identified by 2D location map. Secret information and location map are embedded in the host image. A capacity raising RDH scheme has been proposed by Lee et al. [10] based on the prediction of difference expansion. In this scheme, predictive pixel of a host image pixel is computed from its surrounding pixels. Generally the difference values between the host pixels and their corresponding predictive pixels are small. Large quantities of smaller difference values are expanded to hide secret data. The receiver can extract the embedded secret message and restore the original pixel according to predictive error. Leung et al. [11] proposed a block based RDH scheme that embeds secret data in a host image by modifying the prediction errors. Prediction error values of each block are computed based on the median value.

Qiu et al. [12] proposed a RDH scheme by extending the generalized integer transformation. In this method, the cover image is divided into blocks and the parameters like threshold and capacity parameter can be adaptively selected to embed more data into the smooth blocks with less distortion. Huang et al. [13] proposed a RDH scheme for JPEG images based on histogram modification. RDH in JPEG images is considerably more difficult than that in uncompressed images because there is less information redundancy in JPEG images. In this technique data embedding is performed based on the modification of DCT coefficients. Among the all quantized DCT coefficients, non zero AC coefficients are selected for data hiding. Secret data bits are embedded by histogram shifting. Reverse shifting is performed to reconstruct the original image.

In our previous work [14], we have proposed a block based RDH scheme for digital images. In that, optimal value for each 8×8 block is computed, and then the secret data is embedded on each block based on the difference between original pixel value and the optimal value. The hiding capacity is enhanced in the proposed scheme. Xie et al. [15] proposed a RDH method for JPEG images that improves the embedding capacity of existing methods. In this method, the secret data is embedded in the host image by doubling the selected frequency coefficients. The frequency coefficients are divided into two sets: one set comprises blocks containing no $(-3, +3, -4, +4)$ AC coefficients and the other set comprises all the remaining blocks. In the first set, secret data is embedded using Huang et al.'s method [13] and the other set uses extended method. A location map is used to distinguish the sets and this method gives better results when JPEG quality factor is low.

Yang et al. [16] proposed a reversible visible watermarking method which uses human visual system (HVS) characteristics to provide visible watermarking. To achieve reversibility, approximate version of the original image is generated and the difference between the original image and approximate image is computed. In this method, binary watermark images can be visibly embedded in a particular region of the host image. Tsai and Chang [17] proposed an approach that visibly hides a binary watermark image into a host image using pixel mapping function. Inverse function is used to remove watermark and to restore the host image. To provide additional authentication, an integer sequence is generated by random variables which is also added into the intermediate watermarks. Farrugia [18] proposed a RVW scheme suitable for lossy compressed images. The proposed mechanism embeds a visible watermark in a host compressed image. It also reversibly embeds the residual information packet required to restore the watermarked region, in the quantized transform coefficients.

Mehra et al. [19] proposed a RVW scheme that uses the complex mapping of pixels. Visible watermark embedding is based on a scaling factor derived by transforming the non-overlapping 8×8 block image into the appropriate DCT domain. Here host image pixel values are mapped according to watermark image using complex mapping function. The

reverse mapping function is used to remove the visible watermark and reconstructs the host image. The overflow/underflow pixels are identified using binary location map which creates payload overhead. Hsu et al. [20] proposed an RVW scheme for ownership protection in multimedia images which embeds a binary image watermark into gray-scale image by modifying the pixel values of the host image according to the pixel values of watermark image. Further a reversible invisible data hiding is used to hide the watermark information which can be used to invert the visible watermark losslessly in the receiving side.

Zhang et al. [21] proposed a RVW scheme for encrypted images. In that scheme, the original plaintext image is encrypted by bit-wise exclusive-or operation. Then the data-hider modifies a part of encrypted data corresponding to the black pixels of a binary watermark image to insert the visible watermark. A visible watermarking scheme for Block Truncation Coding (BTC) codes of images was proposed in [22]. Here the predicted version of the original image is obtained in the watermark region, and then watermark image is superposed into bi quantization levels of the BTC image in visible manner. After watermark removal, using the relationship of bi quantization levels of the BTC codes, the host image can be reconstructed. An improvement in reversible visible watermarking for BTC images was proposed by Mohammed et al. [23] which uses adaptive pixel circular shift operation to adjust the host image properties with watermark image properties.

Lossless visible watermarking based on DCT modification is proposed in [24]. In the proposed method, DCT coefficients of the watermark image are inserted into the DCT coefficients of the host image. Integer DCT is used for frequency transformation and reversible integer mapping is used for watermark embedding. Security is enhanced by using a random permutation. There exists overflow pixel values that are necessary to be embedded into the watermarked image for lossless recovery of the host image. Another watermarking scheme based on DCT is proposed in [25], that uses mathematical concept (Chinese Remainder Theorem) to embed watermark by modifying the DCT coefficients. Robustness of the scheme is increased by applying a voting strategy. This scheme provides better result against JPEG attack, but only binary watermark can be embedded in a host image. Recently, a RVW scheme for encryption domain is proposed by Yao et al. [26]. Prior to encryption, data inserting positions are dynamically selected using a perceptual model. Visible watermark is embedded in the data embedding positions by substitution method. The decrypted watermarked image contains watermark which can be perfectly viewed. After removing the embedded watermark, the original host image can also be perfectly regenerated.

Most of the existing RVW schemes perform watermarking in spatial domain and the visibility of the watermark cannot be adjusted based on the application requirement. In this paper, a frequency domain based removable visible watermarking scheme is proposed which allows the user to adjust the visibility or transparency of watermark in the host image. Watermark embedding is performed during forward DCT process of JPEG compression. Watermark removal and reconstruction of host image is performed during inverse DCT process of JPEG decompression.

3 Watermark Embedding and Removal

In this section, the process of embedding a watermark image in a host image and watermark removal are described. Watermark embedding is performed at forward DCT phase of JPEG compression. By modifying frequency coefficients of the host image with respect

to the frequency coefficients of watermark image, visible watermarking is performed. The general process of JPEG compression, embedding process and hiding the watermark key are explained below. The watermark can be removed from the watermarked image by using the corresponding reverse mapping and the secret key that gets generated during watermark embedding phase.

3.1 JPEG Compression

In JPEG compression, first the source image pixels are divided into number of blocks of size 8 × 8. Then the pixels in each block are transformed into frequency domain from spatial domain using Discrete Cosine Transform. The equation for forward DCT shown below transforms the image pixel P(x,y) of a block into frequency coefficients F(i,j).

$$F(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} P(x,y) * \cos\left[\frac{(2x+1)i\pi}{2N}\right] * \cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

where N = 8 for block size of 8 × 8; i = 1–8; j = 1–8.

F(0,0) is called DC coefficient and all other frequency coefficients are called as AC coefficients. The size is reduced by dividing each frequency coefficient by a particular threshold value. This process is called quantization. The threshold values are arranged as a table called quantization table. The compression quality factor of 50% is achieved by the default quantization table shown in Fig. 1. After quantization, DC coefficient is encoded using differential encoding and AC coefficients are encoded using Run length encoding. Finally it is Huffman coded and transmitted as a frame or stored as file.

3.2 Embedding Process

In the watermark embedding process, watermark image is embedded in the host image in a visible manner. For watermark embedding, the DCT coefficients of the host image are adjusted according to the DCT coefficients of the watermark image. Always the watermark image should be smaller than the host image and should be on same format as the host image. According to JPEG compression, the original host image is divided into 8 × 8 blocks and each block is converted from spatial domain to frequency domain using DCT. Similarly watermark image is also divided into blocks and DCT coefficients are computed. Then the Area of Watermarking (AOW) is identified in the host image. The selected area

Fig. 1 JPEG default quantization table

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

or region in the host image used for watermark embedding is called as AOW. DCT coefficients of each block in the selected area are processed as follow. Let A be the first DCT block in the selected area of host image and B be the first DCT block of the watermark image.

$$A(i,j) = A(i,j)/2 \tag{2}$$

$$B(i,j) = B(i,j)/2 \tag{3}$$

$$C(i,j) = A(i,j) + B(i,j). \tag{4}$$

For i = 1–8 and j = 1–8.

$$C(1,\ 1) = B(1,\ 1). \tag{5}$$

The watermark visibility can be varied using Eqs. (2) and (3). The division operations are optional operation. If the user wants to reduce the visibility of host image, he can use the division operation in Eq. (2). Otherwise the host image AC coefficients are kept as it is. Similarly if the user wants to reduce the visibility of watermark image, he can divide all the AC coefficients of block B by 2 as in Eq. (3). Otherwise the watermark image AC coefficients are kept as it is. So this division operation gives flexibility to the users to adjust the visibility or transparency of the watermark. Possible combination of this division operation in watermark embedding is shown in Table 1.

The division by 2 operations creates round off problem. For example, if the AC coefficient is 8, division by 2 yields 4. But if it is 11, the integer division by 2 again yields 5. This creates a round off problem. This will not produce any perceptual problem after watermark removal in the receiving side. This round off may create small variation in the pixel value during dequantization. So in the receiving end after watermark removal, the recovered host image pixel values are not exactly same as the JPEG decompressed pixel values. Therefore the proposed RVW scheme will not produce exact lossless recovery of host image. Instead, it will produce nearly lossless recovery of host image with permissible distortion.

After division operation, AC coefficients of block A is added with corresponding AC coefficients of block B and stored in block C. DC coefficient of block C is assigned as DC coefficient of block B. Then the block A in the host image is replaced by block C. These operations are performed for all blocks of the selected area in the host image to complete the watermark embedding process. Finally the host image is quantized and entropy encoded according to JPEG compression to construct the JPEG compressed watermarked image.

The proposed algorithm can be explained with an example. Figure 2 shows the modifications occurring in an example DCT coefficients block of size 8×8. A sample DCT

Table 1 Division operation in watermark embedding

Sl. no.	Host image	Watermark image	Remark
1	No division	No division	Visibility of both images are not changed
2	No division	Division	Visibility of watermark image is half reduced
3	Division	No division	Visibility of host image is half reduced
4	Division	Division	Visibility of both images are half reduced

754	−56	−26	34	−2	12	11	19
44	−179	25	13	6	−6	−12	18
−146	70	47	6	1	11	8	21
44	92	18	34	−26	−9	−15	7
53	−24	−29	13	−34	1	−1	14
25	67	−16	16	−25	−5	−5	−2
−15	−14	−28	45	−8	2	0	8
3	−19	44	13	−10	2	−1	−2

(a) DCT Block of host image

316	−86	11	32	−2	4	−8	8
−118	51	102	−43	35	1	2	5
68	−11	−64	−11	−28	−18	3	−6
−35	−20	−23	29	1	5	−21	10
−26	6	−22	15	−20	11	12	−5
−25	11	3	4	−14	17	−7	−4
−5	19	−6	−10	28	−34	7	5
17	−25	7	15	−32	35	−9	−1

(b) DCT block of Watermark image

377	−28	−13	17	−1	6	6	10
22	−90	13	7	3	−3	−6	9
−73	35	24	3	1	6	4	11
22	46	9	17	−13	−5	−8	4
27	−12	−15	7	−17	1	−1	7
13	34	−8	8	−13	−3	−3	−1
−8	−7	−14	23	−4	1	0	4
2	−10	22	7	−5	1	−1	−1

(c) Half reduced DCT Block of host image

316	−114	−2	49	−3	10	−2	18
−96	−39	115	−36	38	−2	−4	14
−5	24	−40	−8	−27	−12	7	5
−13	26	−14	46	−12	0	−29	14
1	−6	−37	22	−37	12	11	2
−12	45	−5	12	−27	14	−10	−5
−13	12	−20	13	24	−33	7	9
19	−35	29	22	−37	36	−10	−2

(d) DCT block of watermarked image

Fig. 2 Modification of DCT coefficients in an example block

block of a host image is shown in Fig. 2a. Figure 2b shows a sample 8 × 8 DCT block of a watermark image. Let the visibility of the host image is half reduced. Therefore integer division is performed on each coefficients of host image by 2 to produce the half reduced DCT of the host image as shown in Fig. 2c. The DC coefficient of the host image in Fig. 2c is directly replaced by the DC coefficient of watermark image block and AC coefficients of Fig. 2c is added with corresponding AC coefficient of Fig. 2b to construct the DCT block of watermarked image as shown in Fig. 2d.

The DC coefficient of each original host image block in AOW is quantized using default JPEG quantization table value 16 and combined as secret key which is called as watermarking key K. Let a_1 be the DC coefficient value of block 1, a_2 be the DC coefficient value of block 2 etc. Hence the watermarking key K is in the form of

$$K = b_1 \,||\, b_2 \,||\, b_3 \,||\, \cdots \,||\, b_N \tag{6}$$

where N = Number of blocks in the watermarking area AOW,

$$b_i = Round\left(\frac{a_i}{16}\right).$$

Flow chart for the proposed watermark embedding process is shown in Fig. 3. Let the host or cover image is I and the watermark image is W. Both I and W are separated into 8 × 8 blocks and forward DCT is applied. The area of watermarking is selected in the cover image. DC coefficient of each block of AOW is extracted as secret key. Frequency coefficient of I in AOW is modified according to the frequency coefficients of W. Then quantization is performed using JPEG quantization table. In the quantized DCT block of I, secret key is hidden using the reversible invisible data hiding scheme proposed in Sect. 3.3. Finally entropy encoding is performed to get the JPEG compressed

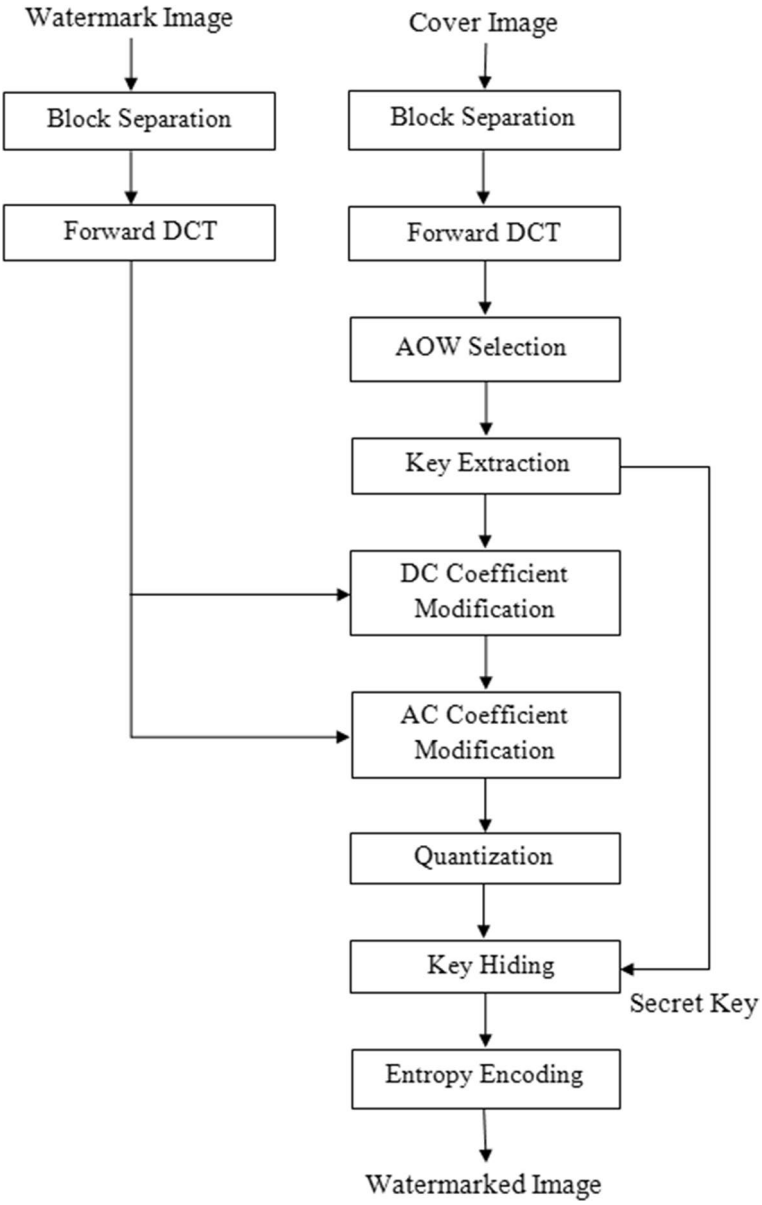

Fig. 3 Flow chart of the proposed watermark embedding scheme

watermarked image. When the resultant image is decompressed, the watermark is clearly visible in the JPEG image.

3.3 Hiding Watermark Key

The watermark key K can be hidden invisibly in the blocks of the image where visible watermarking is performed. That is the AOW in the host image I can be used to hide the key K also. K is an array consisting of Quantized DC coefficients of all the blocks in the watermarking area which is shown in Eq. (5). If it is desirable to have high security the watermark key can be XORed with user's private key before hiding in the image. Otherwise the key K can be directly hidden in the host image.

The first value b_1 is selected and converted into 6 digit binary number. Then split the 6 digit binary number into 2 halves: first half consists of 3 Most Significant Bits (MSB) and second half consists of 3 Least Significant Bits (LSB). Then convert the 2 halves into decimal numbers. Select a quantized DCT block in the host image. In the quantized DCT block, higher frequency coefficients are zero and lower frequency coefficients are nonzero values. The nonzero coefficients are run length encoded. First two zero coefficients are replaced by 2 decimal numbers of the key. Figure 4 shows the Zig-Zag scanning of a sample quantized block for entropy encoding. The zeros shown in bold letters are replaced by the 2 digits of the key (Integer form of b_{11} and b_{12} for the block b_1) of the particular block.

$$b_1 = b_{11} \,||\, b_{12} \tag{7}$$

where

$$b_{11} = MSB_3\,(b_1)$$
$$b_{12} = LSB_3\,(b_1).$$

3.4 Watermark Removal

The watermark can be removed from the watermarked image by using the corresponding reverse mapping during JPEG decompression. Watermark image and watermark key are needed to remove the watermark from the watermarked image and to restore the host

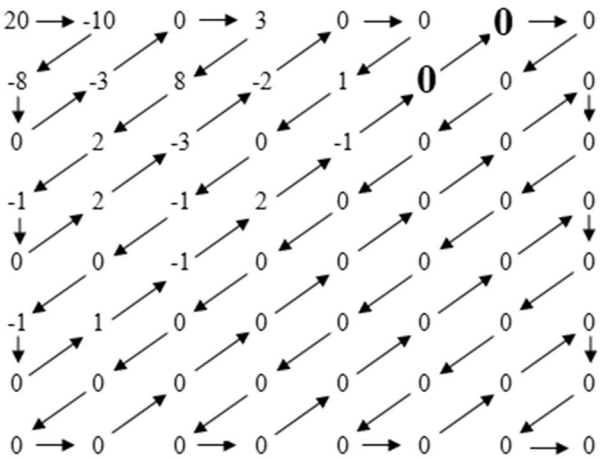

Fig. 4 Zig-Zag scanning

image. According to JPEG decompression procedure, the watermarked image is entropy decoded to produce quantized DCT coefficients. Then the AOW is identified and watermark removal is performed as follow.

1. Let the first block in AOW is C.
2. Watermarking key of the block is extracted using following steps
    a. The 2 elements that lies between non-zero coefficients and zero coefficients are separated as watermark key elements and replaced by zeros.
    b. The first key element is converted into 3 bits binary and second element is converted into 3 bit binary.
    c. Then the two binary numbers are concatenated to form a 6 bits binary number.
    d. The 6 bits number is converted into decimal form, which is the watermark key k_1 of the block A (It represents the DC coefficient of the original host image).
3. The DC coefficient of the block C is directly replaced by watermarking key k_1 of block.
4. Then dequantization is performed on the block.
5. Meanwhile the first block of the watermark image is converted into frequency domain using forward DCT.
6. After dequantization, the AC coefficients of the block are first subtracted by corresponding AC coefficients of the watermark image block.
7. Then it is multiplied by 2. (This multiplication operation is performed as optional operation against the division operation performed according to Table 1).

This process is repeated for all the blocks in AOW of the watermarked image. Finally, inverse DCT is performed to obtain the original host image. The reverse process of Eqs. (2)–(4) is performed for watermark removal. The operations performed in Eqs. (8) and (10) are optional operations. If the visibility of the host image and/or watermark image is changed according to Table 1, then these operations are performed.

$$B(i,j) = B(i,j)/2 \tag{8}$$

$$A(i,j) = C(i,j) - B(i,j) \tag{9}$$

$$A(i,j) = A(i,j) * 2. \tag{10}$$

For i = 1–8 and j = 1–8.

$$A(1,\ 1) = k_1. \tag{11}$$

4 Results and Discussion

The proposed RVW technique is implemented in MATLAB and tested with several monochrome and color images to quantitatively measure the effectiveness of the scheme. In watermarking techniques, quality of watermarked image and watermark visibility or transparency are the important metrics to be considered. To measure the image

quality, the Peak Signal-to-Noise Ratio (PSNR) value is often used. The unit of PSNR is decibel (dB).

$$PSNR = 10 * \log_{10}\left(\frac{255^2}{MSE}\right) \tag{12}$$

where 255 represents the maximum pixel value and MSE is the mean square error between the original image and the watermarked image.

$$MSE = \frac{1}{H * W}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}\left[I(x,y) - \bar{I}(x,y)\right]^2 \tag{13}$$

where I is the host image and $\bar{I}$ is the watermarked image, H and W represents the height and width of the image respectively. As there is no direct tool to measure the watermark visibility, it can be observed by human visual system through the resultant watermarked images. Four sample 24 bit color images of size 512×512 chosen are Lena, Barbara, Airplane and House images. The watermark sample image of different sizes 256×256, 128×128 and 64×64 is considered for watermark embedding.

The sample watermarked images with different watermark visibility are shown in Fig. 5. The perceptual variation in the visibility of the watermark can be directly observed from the resultant watermarked images through human visual system. In the first watermarked image, visibility of the watermark image is not reduced, which means the visibility of the watermark image is completely exposed. In the second watermarked image, visibility of the watermark image is half reduced. And in both cases visibility of the host image is half reduced. The visibility of the watermark can be adjusted as shown in the resultant watermarked image which is the important feature of the proposed scheme. Other visibility or transparency adjustments as mentioned in Table 1 are also performed as per the application requirement.

The comparison of image quality between the original host image and watermarked image for different sizes of watermark are shown in Table 2 and Fig. 6. JPEG compression itself reduces the image quality into approximately 35 dB PSNR with standard quantization table (quality factor of 50). Image quality degradation after watermarking is very less when compared with image quality degradation in JPEG compression. It is nearly 10 dB. In the receiving end, after watermark removal, the host image can be approximately recovered from the watermarked image. That is image quality of the recovered host image is approximately same as the quality of JPEG decompressed image.

The proposed scheme can be used for grayscale images also. Four sample 8-bit grayscale images Barbara, Boat, Baboon and Airplane are chosen to demonstrate the watermark visibility and image quality. The watermark of size 128×128 is embedded into the chosen images that are shown Fig. 7. The PSNR values after JPEG compression and after watermarking are shown in Table 3. The good image quality and high watermark visibility of the proposed technique can be observed through the results.

The comparison of image quality between the proposed scheme and other compression based RVW schemes are shown in Table 4. For this comparison, watermark size of 128×128 and JPEG compression with quality factor 50 is used. On the other hand, the proposed scheme is compared with existing schemes that didn't use compression. According to this comparison, the PSNR value is measured only for the AOW of the watermarked image with respect to the AOW of the original host image. Then the

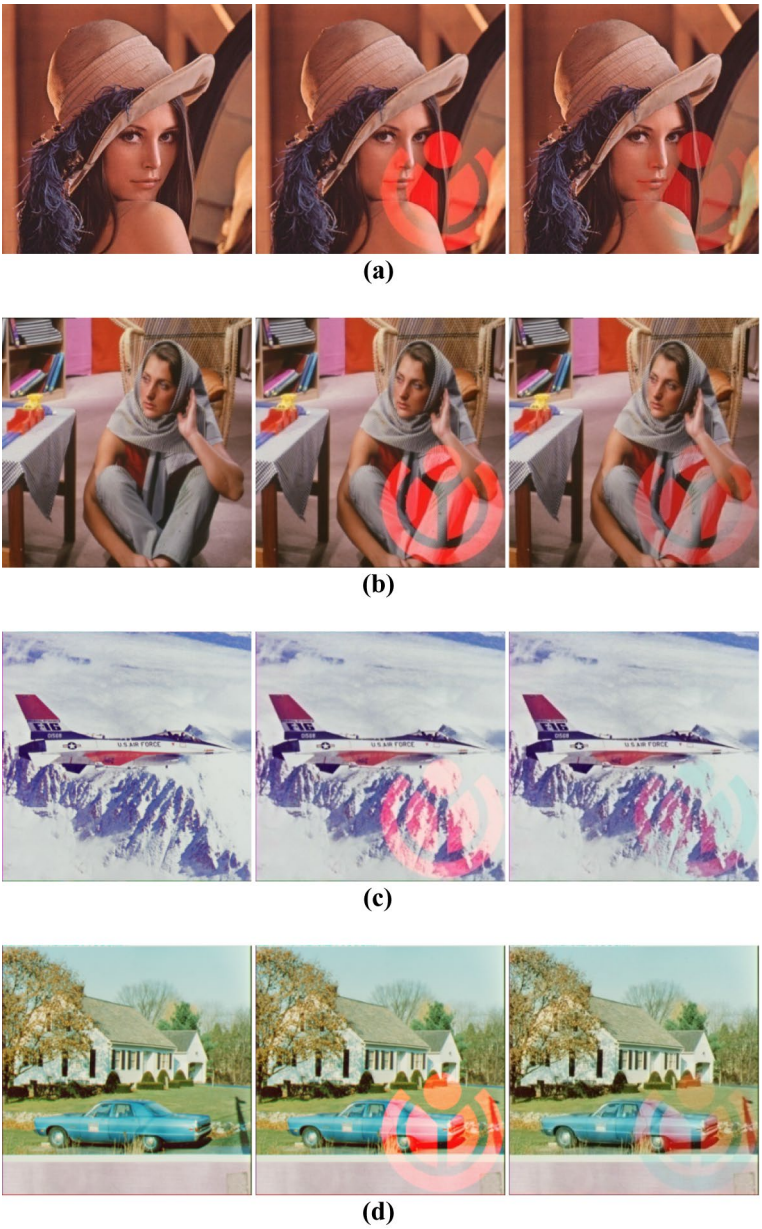

Fig. 5 Original image and watermarked images with full watermark visibility and half watermark visibility for **a** Lena, **b** Barbara, **c** Airplane, **d** House Images. (Color figure online)

measured PSNR values for different images are compared with existing schemes that represent the PSNR value of the AOW of watermarked images. This type of performance comparison for Lena, Airplane and Baboon with watermark size of 128×128 is shown in Table 5. For this comparison, JPEG compression with quality factor 100

Table 2 Image quality comparison for color images

Sl. no.	Image	PSNR after JPEG compression	Watermark size	PSNR of watermarked image with full watermark visibility	PSNR of watermarked image with half watermark visibility
1	Lena	36.70	256×256	18.45	22.32
			128×128	24.06	27.12
			64×64	32.56	35.80
2	Barbara	32.12	256×256	15.98	18.04
			128×128	20.26	23.38
			64×64	26.59	29.89
3	Airplane	38.09	256×256	19.98	23.57
			128×128	24.51	28.71
			64×64	30.89	35.45
4	House	35.42	256×256	17.31	19.22
			128×128	22.44	24.84
			64×64	28.94	31.95

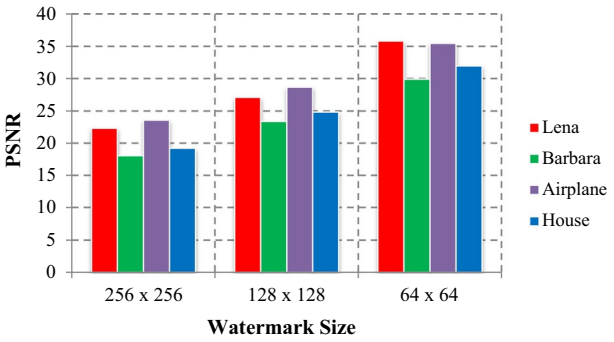

Fig. 6 Watermark size versus PSNR

Fig. 7 Watermarked images for **a** Barbara, **b** Boat, **c** Baboon and **d** Airplane grayscale images

is used. The results show that the proposed algorithm has high image quality than the existing schemes in the literature.

Table 3 Image quality comparison for grayscale images

Sl. no.	Image	PSNR after JPEG compression	PSNR after watermarking
1	Barbara	32.95	25.73
2	Boat	35.49	24.38
3	Baboon	30.50	25.43
4	Airplane	37.76	27.86

Table 4 Image quality comparison with compression based RVW schemes

Sl. no.	Image	PSNR (dB)		
		Yang et al. scheme [22]	Mohammad et al. scheme [23]	Proposed scheme
1	Lena	24.05	24.91	26.37
2	Baboon	24.12	24.52	25.43
3	Airplane	23.55	25.08	27.86
4	Barbara	23.68	24.22	25.73

Table 5 Image quality comparison with RVW schemes that didn't use compression

Sl. no.	Reference scheme	PSNR (dB)		
		Lena	Airplane	Baboon
1	Taha et al. scheme [7]	–	39.41	30.01
2	Hsu et al. scheme [20]	37.17	37.17	37.17
3	Lin et al. scheme [24]	38.47	38.28	–
4	Shiu et al. scheme [25]	33.73	33.76	34.87
5	Yao et al. scheme [26]	35.93	–	36.56
6	Proposed scheme	40.57	42.11	38.10

5 Conclusion

A JPEG image based RVW scheme is proposed in this paper. The watermarking scheme in JPEG is important because many commercial applications use JPEG compressed images. Different sizes of watermarks can be embedded in different region of host image using this scheme. Experimental results confirm that the proposed scheme has high watermark visibility and good host image quality. Another advantage of the proposed technique is that the visibility of the watermark can be adjusted based on the user requirement. One who has the watermark and secret key can only remove the watermark and recover the host JPEG image in its original state. Thus it enhances the security. This method can be extended to video compression standards like MPEG and H.264.

References

1. Sarkar, A., Madhow, U., & Manjunath, B. S. (2010). Matrix embedding with pseudorandom coefficient selection and error correction for robust and secure steganography. *IEEE Transaction on Information Forensics and Security, 5*(2), 225–239.
2. Hong, W., & Chen, T. S. (2012). A novel data embedding method using adaptive pixel pair matching. *IEEE Transactions on Information Forensic and Security, 7*(1), 176–184.
3. Tsai, M. J., Liu, J., Yin, J. S., & Yuadi, I. (2014). A visible wavelet watermarking technique based on exploiting the contrast sensitivity function and noise reduction of human vision system. *Multimedia Tools and Applications, 72,* 1311–1340.
4. Guo, L., Ni, J., & Shi, Y. Q. (2014). Uniform embedding for efficient JPEG steganography. *IEEE Transactions on Information Forensics and Security, 9*(5), 814–825.
5. Zong, T., Xiang, Y., Natgunanathan, I., Guo, S., Zhou, W., & Beliakov, G. (2015). Robust histogram shape-based method for image watermarking. *IEEE Transaction on Circuits and Systems for Video Technology, 25*(5), 717–729.
6. Agarwal, H., Sen, D., Raman, B., & Kankanhalli, M. (2016). Visible watermarking based on importance and just noticeable distortion of image regions. *Multimedia Tools and Applications, 75,* 7605–7629.
7. Taha, T. B., Ngadiran, R., & Ehkan, P. (2018). Adaptive image watermarking algorithm based on an efficient perceptual mapping model. *IEEE Access, 6,* 66254–66267.
8. Noor, R., Khan, A., & Sarfaraz, A. (2019). High performance and energy efficient image watermarking for video using a mobile device. *Wireless Personal Communications, 104,* 1535–1551.
9. Hu, Y., Lee, H. K., & Li, J. (2009). DE- based reversible data hiding with improved overflow location map. *IEEE Transaction on Circuits and Systems for Video Technology, 19*(2), 250–260.
10. Lee, C. F., Chen, H. L., & Tso, H. K. (2010). Embedding capacity raising in reversible data hiding based on prediction of difference expansion. *Journal of Systems and Software, 83,* 1864–1872.
11. Leung, H. Y., Cheng, L. M., Liu, F., & Fu, Q. K. (2013). Adaptive reversible data hiding based on block median preservation and modification of prediction errors. *Journal of Systems and Software, 86,* 2204–2219.
12. Qiu, Y., Qian, Z., & Yu, L. (2016). Adaptive reversible data hiding by extending the generalized integer transformation. *IEEE Signal Processing Letters, 23*(1), 130–134.
13. Huang, F., Qu, X., Kim, H. J., & Huang, J. (2016). Reversible data hiding in JPEG images. *IEEE Transaction on Circuits and Systems for Video Technology, 26*(9), 1610–1621.
14. Brabin, D. R. D., Perinbam, J. R. P., & Meganathan, D. (2017). A block based reversible data hiding scheme for digital images using optimal value computation. *Wireless Personal Communications, 94*(4), 2583–2596.
15. Xie, X., Lin, C., & Chang, C. (2019). A reversible data hiding scheme for JPEG images by doubling small quantized AC coefficients. *Multimedia Tools and Applications, 78,* 11443–11462.
16. Yang, Y., Sun, X., Yang, H., Li, C. T., & Xiao, R. (2009). A contrast-sensitive reversible visible image watermarking technique. *IEEE Transactions on Circuits and Systems for Video Technology, 19*(5), 656–667.
17. Tsai, H. M., & Chang, L. W. (2010). Secure reversible visible image watermarking with authentication. *Signal Processing: Image Communication, 25,* 10–17.
18. Farrugia, R. A. (2010). A reversible visible watermarking scheme for compressed images. In *Proceedings of fifteenth IEEE Mediterranean electrotechnical conference* (pp. 212–217).
19. Mehra, N., & Shandilya, M. (2013). Imprecise reversible visible watermarking. *CSIT, 1*(4), 355–365.
20. Hsu, F. H., Wu, M. H., Yang, C. H., & Wang, S. J. (2014). Visible watermarking with reversibility of multimedia images for ownership declarations. *Journal of Supercomputing, 70*(1), 247–268.
21. Zhang, X., Wang, Z., Yu, J,. & Qian Z. (2015). Reversible visible watermark embedded in encrypted domain. In *Proceedings of IEEE international conference on signal and information processing* (pp. 826–830).
22. Yang, H., & Yin, J. (2015). A secure removable visible watermarking for BTC compressed images. *Multimedia Tools and Applications, 74,* 1725–1739.
23. Mohammad, N., Sun, X., Yang, H., Yin, J., Yang, G., & Jiang, M. (2017). Lossless visible watermarking based on adaptive circular shift operation for BTC-compressed images. *Multimedia Tools and Applications, 76*(11), 13301–13313.
24. Lin, Y., Yang, C., & Tsai, J. (2018). More secure lossless visible watermarking by DCT. *Multimedia Tools and Applications, 77,* 8579–8601.
25. Shiu, P. F., Lin, C. C., Jan, J. K., & Chang, Y. F. (2018). A DCT-based robust watermarking scheme surviving JPEG compression with voting strategy. *Journal of Network Intelligence, 3*(4), 259–277.

26. Yao, Y., Zhang, W., Wang, H., Zhou, H., & Yu, N. (2019). Content-adaptive reversible visible watermarking in encrypted images. *Signal Processing, 164,* 386–401.

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

D. R. Denslin Brabin received B.E. and M.E. degrees in Computer Science and Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India in 2002 and 2004 respectively. He received Ph.D. from Anna University, Chennai, India in the year 2018. He is now working as Senior Assistant Professor in the Department of Computer Science and Engineering, Madanapalle Institute of Technology and Science, Andhra Pradesh, India. He has 16 years of teaching experience. He has published 15 research papers in International Journals. His current research interests include Network Security and Image Processing.

J. Raja Paul Perinbam received B.E. degree in Electrical Engineering and M.Sc. (Eng.) in Applied Electronics both from the University of Madras, India and Ph.D. from Indian Institute of Technology Madras, India in the years 1970, 1973 and 1984 respectively. He worked as a professor in the College of Engineering, Anna University, Chennai, India from 1975 to 2008. During that period he was also associated with the Department of Media Sciences, Anna University, as the head of the department and was instrumental in setting up audio and video studios. He has carried out a number consultancy projects for many small scale industries in Chennai in the area of embedded systems and power electronics. More than 10 research scholars have completed their Ph.D. degrees under his guidance. He has published about 60 research papers in different Journals and Conferences of International repute. His current area of research interest includes Data communication, VLSI Design and Embedded Systems.

D. Meganathan graduated from PSG Tech, Coimbatore, India and received doctorate degree from Anna University, Chennai, India. He works as Assistant professor in the department of Electronics Engineering, MIT Campus, Anna University since 2003. His areas of interest include VLSI, Analog VLSI, Devices and Network on Chip Design. He has published more than 50 numbers of papers in peer reviewed journals and conference proceedings. He is a member of professional bodies like IE and IETE.