



Imprecise reversible visible watermarking

Neelesh Mehra · Madhu Shandilya

Received: 13 May 2013 / Accepted: 20 October 2013 / Published online: 17 December 2013
© CSI Publications 2013

Abstract Using the program visible digital, a perceptible watermark is added to an image to prevent illicit use of multimedia content and to provide copyright and copy protection for the author. There are numerous applications that require user authentication to make the original image content available. If the original image is recovered from the watermarked image successfully, then the scheme is said to be a reversible watermarking scheme. However, most of the reversible visible watermarking schemes found in the current literature do not preserve visual quality of image. In this investigation, we propose a novel reversible and visible watermarking method that is suitable for both grey and colour images. In our approach, we use the complex mapping of pixels via embedding combined with a scaling factor derived from the contrast-sensitive function of the original image. We then prove experimentally that our scheme is advantageous over the previous works in this field. Furthermore, we compare the performance of proposed work with other state-of-the-art under various parameters.

Keywords Reversible visible watermarking · Pixel mapping · Contrast sensitive function · Data hiding

Electronic supplementary material The online version of this article (doi:10.1007/s40012-013-0031-3) contains supplementary material, which is available to authorized users.

N. Mehra (✉)
Department of Electronics, SATI, Vidisha, India
e-mail: neeshmehra@gmail.com

M. Shandilya
Department of Electronics, MANIT, Bhopal, India
e-mail: madhu_shandilya@yahoo.co.in

1 Introduction

Digital image watermarking is a process that embeds a watermark into a digital image to form a watermarked image. The watermark in the watermarked image is classified as visible or invisible based on the human visual perception. Visible watermarks are used to declare the ownership of digital images, and provide copyright as well as copy protection in active way, thereby decreasing the unauthorised use of the original image. Conversely, invisible watermarks provide only copyright protection but are unable to provide copy protection as it does not impede the unauthorized access of copyrighted items. In general, there are three major requirements for visible watermarking [1–3].

- **Perceptibility:** The watermark must be easily identified to provide copyright information.
- **Transparency:** The watermark must not significantly obscure the image details over which it covers.
- **Robustness:** The original image should not be easily recovered from the watermarked image by an illicit user [3, 4].

The task of embedding a visible watermark involves a trade-off between its perceptibility and transparency. A law-abiding customer must have error-free access to the image content, mandating that a visible watermark be reversible in nature. Several reversible watermarking schemes [5–7] have been proposed for specific image types such as medical, military, and satellite, etc. Mintzer et al. [1] were the first to propose a reversible visible watermark model in which the watermarked image can be viewed for free and the original image can be reconstructed from the watermarked image at an additional cost. Mohanty et al. [2] proposed a visible watermarking technique in the discrete cosine transform (DCT) domain. Their scheme modifies each DCT coefficient by designated scaling and embedding factors. Watermarked

images employing this scheme, I_w , can be defined by $I_w = \alpha C + \beta W$, where C and W are the DCT coefficients of original image and watermark, respectively. The parameters α and β are determined by exploiting the texture sensitivity of the human visual model (HVS). Huang and Tang [8] proposed a visible watermarking scheme with a discrete wavelet transformation (DWT). The intensity of the watermark in different regions of the image varies depending on the underlying content of the image and human sensitivity to the spatial frequency. However, these two schemes are not reversible. Hu et al. [9] proposed a removable visible watermarking. The scheme uses a key to determine the unchanged coefficients, and the pixel-wise varying parameters are calculated from those unchanged coefficients. Thus, the user with the correct key in the receiver end can recalculate the parameters to remove the visible watermark from the watermarked image. However, the scheme cannot perfectly recover the original image due to a rounding error caused by wavelet transform. Another study [10] adopted removable visible watermarking schemes that allow authenticated users to automatically remove the embedded visible watermark. Nevertheless, these methods do not manage to recover the original image quality, and result in visually impaired images. Impaired images are unsuitable for military, legal and medical applications in which high-quality image recovery is mandatory. The reversible visible watermarking schemes presented in Refs. [11–14] were able to recover the original image quality. However, the embedded visible watermark with the method proposed in Ref. [12] significantly reduces the quality of the watermarked image, while the methods presented in Refs. [13, 14] require a copy of the original watermark to recover the original image. The quality of watermark image and recover watermark in [15] is not so good. Liu and Tsai [18] proposed a generic lossless visible watermarking scheme based on the compound mapping of pixels as a benchmark for reversible, visible watermarking; however, the original watermark is required to recover the original image, with which there may be some resolution issues because the recovery scheme estimates neighbouring pixels. In Xuan et al. [17] propose a distortionless data embedding technique based on integer wavelet transform and achieve good embedding capacity but the robustness of watermarked image is weak and the visual quality of watermarked image is not good enough. The proposed work is also based on the pixel mapping technique, but the watermark is applied using alternate pixels, i.e., the watermark is embedded without altering the four nearest neighbouring pixels, that are scaled by the average contrast-sensitive function [16] to yield the watermarked image and for the correct image estimation upon recovery. The proposed mechanism not only provide us flexibility for embedding large watermark (nearly equal to the size of original image) but also preserves visual quality, as will be demonstrated in a latter section.

The remainder of this paper is organised as follows: Sect. 2 presents the mathematical model of the complex mapping and proposed schemes, Sect. 3 presents the experimental results, and Sect. 4 summarises the concluding remarks.

2 Proposed scheme

In this section, the complex compound mapping is first described. The process is then demonstrated to be reversible, and finally the proposed algorithm based on the complex compound mapping is examined. The process of mapping can be defined as transforming one set of values into another by using some parameter. If different component values are mapped by different parameters then this type of mapping is called as complex compound mapping as demonstrated in Fig. 1. Here input is image and pixel values of image are mapped with certain parameter A, B and C. This nesting of compound maps can be repeated indefinitely to form a complex compound structure.

Under the experimental conditions, $P = \{p_1, p_2, \dots, p_m\}$ are a set of distinct values (pixels value of image) that are to be converted into another set of values defined as $Y = \{y_1,$

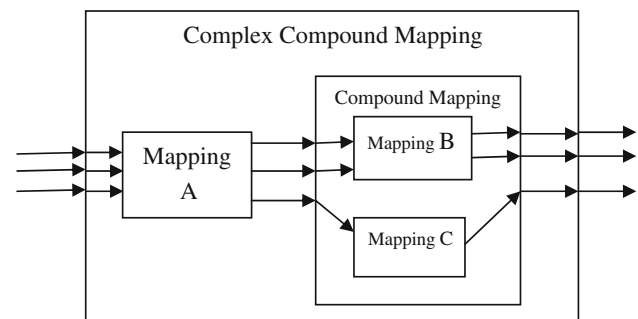


Fig. 1 Depiction of complex compound scheme

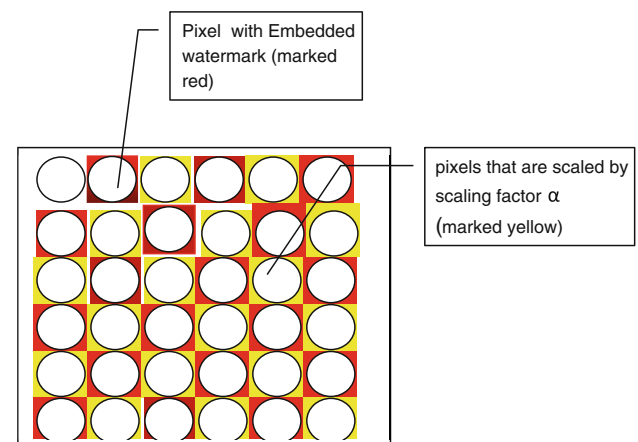


Fig. 2 Depiction of the watermark embedding and the altering of the four nearest neighbour pixels value

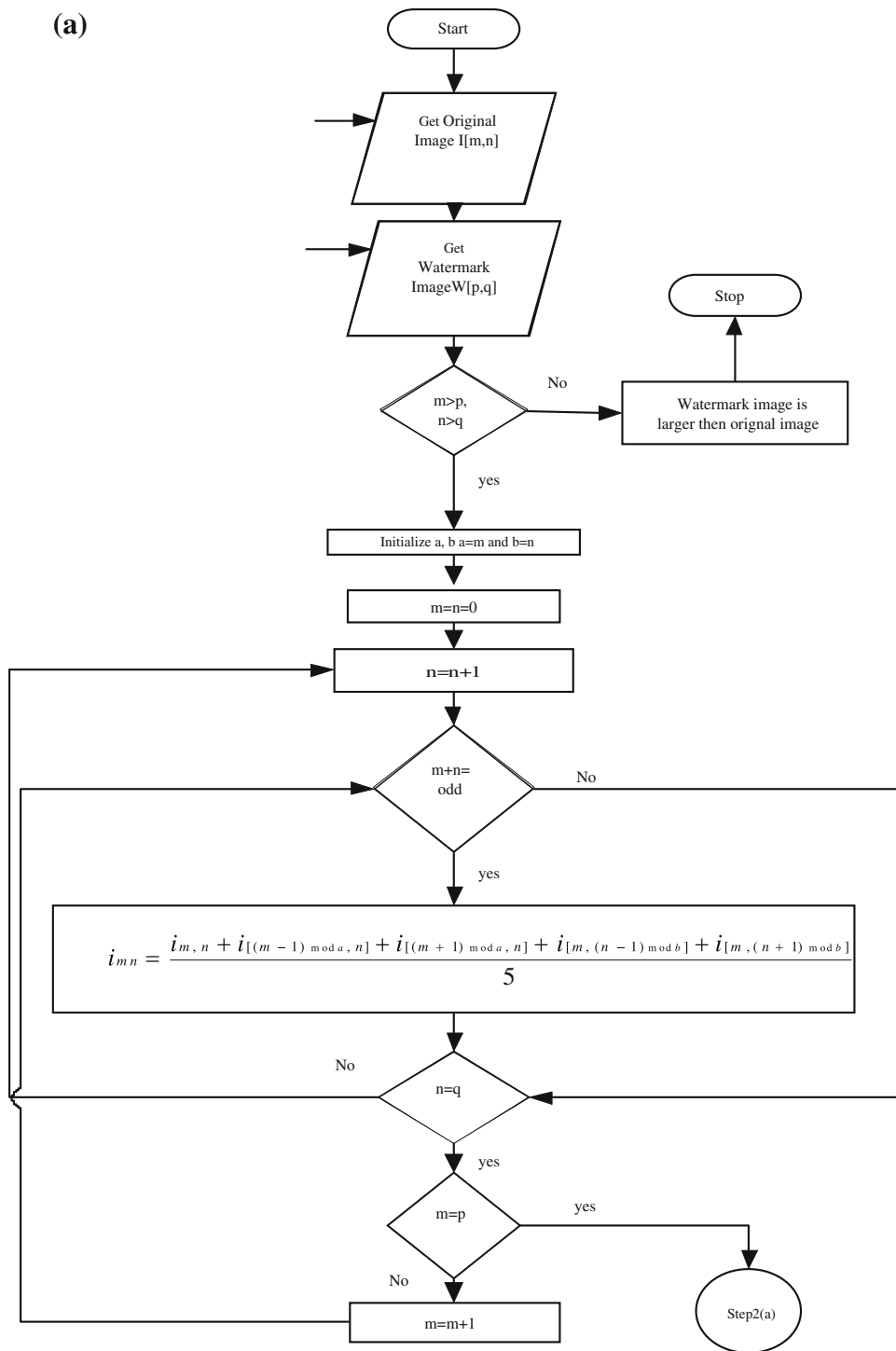


Fig. 3 Flow graph (a, b, c) demonstrating watermark embedding process

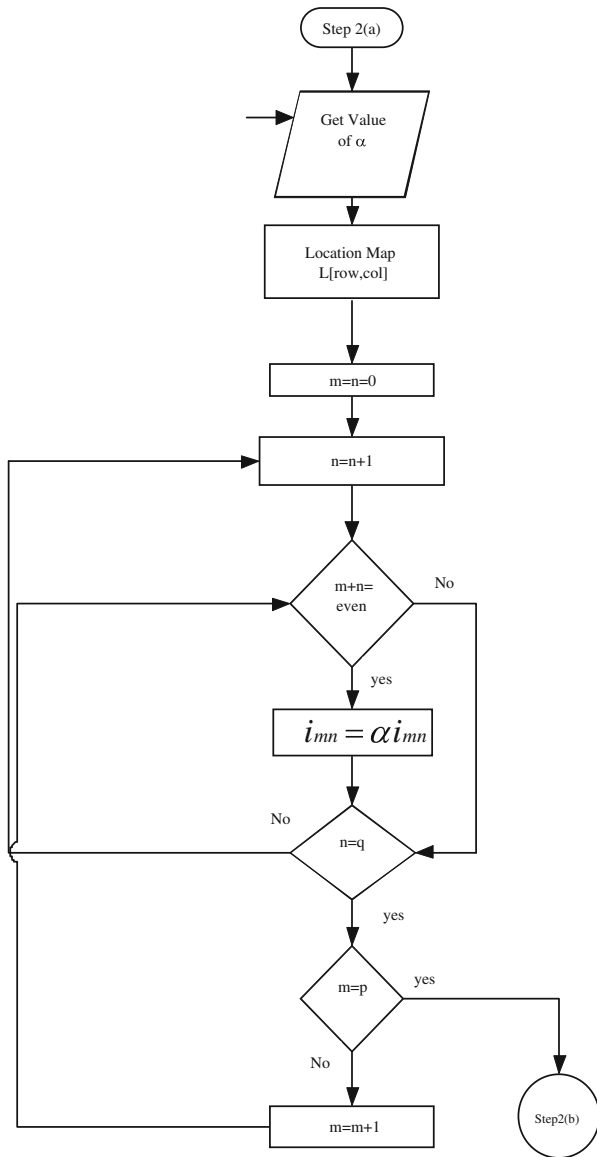
$y_2, \dots, y_m\}$. The respective mapping from p_m to m_i for all values of $m = 1, 2, 3, \dots, m$ is completely reversible. The complex compound mapping, f_x , is governed by the parameter x , such that $x = \{A, B, C\}$ and $A \neq B \neq C$. The whole process can be illustrated as follows:

Let q be the intermediate value such that

$$Q = f_A(P) \tag{1}$$

Leading to the circumstance that if $f_A(P) = Q$ then $f_a^{-1}(Q) = P$.

(b)



(c)

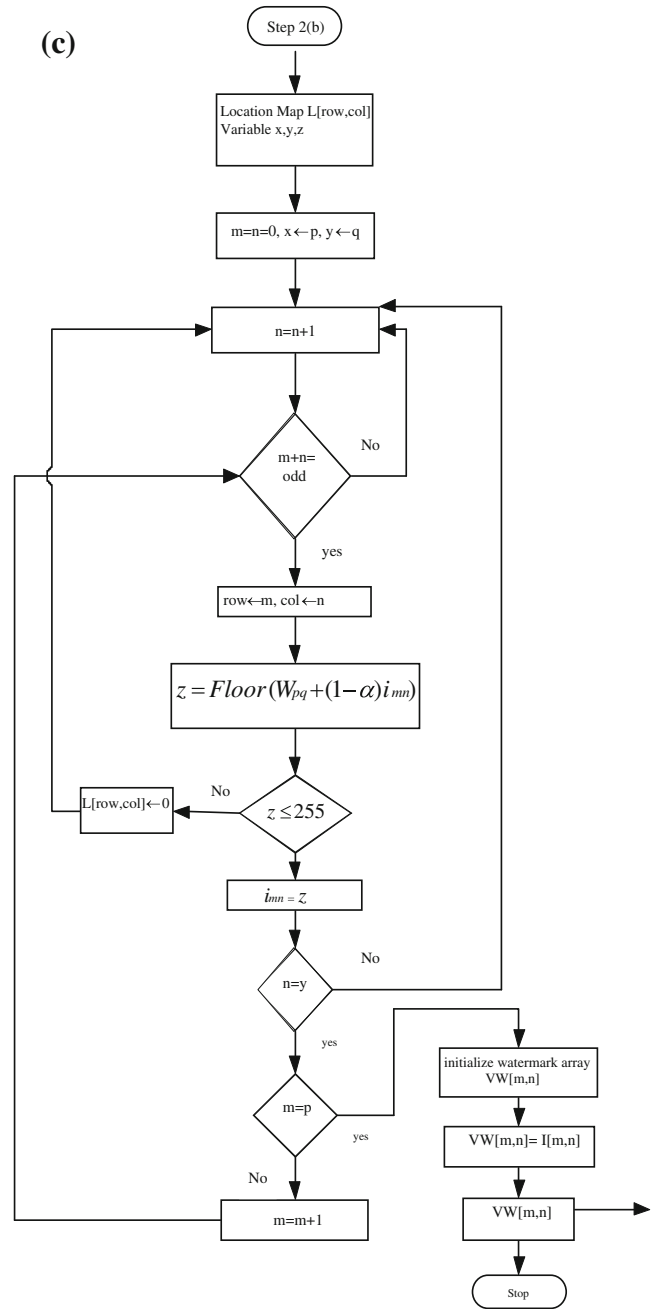


Fig. 3 continued

Now, the variable Q is defined as an intermediate set of values of q_m for $m = 1, 2, 3, \dots, m$, while Q_1 and Q_2 are two subsets of Q such that $Q_1 \cup Q_2 = Q$.

The variables Y_1 and Y_2 also form two subsets of Y such that $Y_1 \cup Y_2 = Y$. Additionally, Y_1 and Y_2 can be defined as:

$$Y_1 = f_B(Q_1) \text{ and } Y_2 = f_C(Q_2) \tag{2}$$

The definition of these two variable leads to:

$$Y = \{f_B(Q_1)\} \cup \{f_C(Q_2)\} \tag{3}$$

$$Y = \{f_B(f_A[P])\} \cup \{f_C(f_A[P])\} \tag{4}$$

This mapping is reversible if we can derive the value of all P from Y using the following equation:

$$P = \{f_A^{-1}[f_B^{-1}(Y_1)]\} \cup \{f_A^{-1}[f_C^{-1}(Y_2)]\} \tag{5}$$

Lemma 1 *If $Y = \{f_A^{-1}[f_B^{-1}(Y_1)]\}$ for any complex compound mapping with function f_x with parameter x then $P = \{f_A^{-1}[f_B^{-1}(Y_1)]\} \cup \{f_A^{-1}[f_C^{-1}(Y_2)]\}$ for all values of P, Y, A, B and C . Proof* Substituting the value of Y_1 and Y_2 from (2) in (5) results in the following:

$$P = \{f_A^{-1}[f_B^{-1}(f_B(Q_1))]\} \cup \{f_A^{-1}[f_C^{-1}(f_C(Q_2))]\} \tag{6}$$

Substituting the values $\{f_A^{-1}[f_B^{-1}(f_B(Q_1))]\} = f_A^{-1}(Q_1)$ and $\{f_A^{-1}[f_C^{-1}(f_C(Q_2))]\} = f_A^{-1}(Q_2)$ in (6) yields

$P = \{f_A^{-1}(Q_1)\} \cup \{f_A^{-1}(Q_2)\}$ which can also be written as

$$P = \{f_A^{-1}(Q_1 \cup Q_2)\} \text{ and } Q_1 \cup Q_2 = Q, \text{ thus leading to } P = \{f_A^{-1}(Q)\} \tag{7}$$

substituting the value of Q from (1) into the RHS of (7) results in

$$P = \{f_A^{-1}(f_A(P))\}$$

where f_A^{-1} and f_A cancel and P is obtained as expected according to lemma 1.

The process of embedding the visible watermark in this algorithm is based on complex compound mapping. In this method, the HVS perception as well as the image content upon which the visible watermark is embedded is considered. The scaling factor, α , is derived by transforming the non-overlapping 8×8 block image into the appropriate DCT domain. The scaling factors are derived from the transform coefficients obtained from the 8×8 block defined as α_n according to:

$$\alpha_n = \frac{1}{\sqrt{2 \prod \sigma^2}} \exp \left[\frac{-[J_n(1, 1) - \mu]^2}{2\sigma^2} \right] + \hat{v}n \tag{8}$$

$$\alpha = \frac{\alpha_n}{N} \tag{9}$$

where N represents the total number of 8×8 blocks, $J_n(1,1)$ represent the DC component of each block and the other parameters are defined as follows:

$$\mu = \frac{1}{N} \sum_{n=1}^N J_n(1, 1) \tag{10}$$

$$\sigma^2 = \frac{1}{N} \sum_{n=1}^N [J_n(1, 1) - \mu]^2 \tag{11}$$

The scaling factor α is then averaged from all the recorded values of α_n . More information about this method can be found in [11, 16]. The proposed state-of-the-art was performed in this study by taking the arithmetic mean (α) of all scaling factors α_n and embedding factor as $(1 - \alpha)$. Instead of embedding a watermark in every pixel, the watermark image was embedded in a single pixel without altering its four nearest neighbour pixels, as shown in Fig. 2. The intensity of four nearest neighbours pixels are reduced by the scaling factor (α) determined by using the contrast-sensitive function. This method effectively reduces the chances of incorrectly estimating the pixel values during the recovery process.

Our method is based on Pixel mapping which may leads to overflow/underflow problem. The values of some pixels in the marked image may exceed the upper bound and/or below the lower bound. If this problem may persist it may violate lossless criteria. To avoid this we use modulo 256 addition along with a location map. A location map is a m by n matrix whose value may be either 0, 1 and empty. The Pixel mapping which may cause under/overflow during embedding, as not used for embedding. The pixel value of original image remains unchanged. The corresponding location is marked with 0 in location map. Similarly 1 is placed if pixel mapping does not cause overflow/underflow problem and corresponding pixel value of original image is mapped with new value. If none of the above condition occurs the location map remain empty. During extraction for any pixel if we found zero in corresponding location map we keep the pixel value unchanged. If 1 is encountered in location map we run our extraction algorithm. The algorithm for watermark embedding and extraction is summarised below.

2.1 Watermark embedding and extraction algorithm

$I[m,n]$ is the original image matrix, and $W[p,q]$ is the watermark image matrix. Ideally, the watermark image, $W[p,q]$, should be embedded within the original image, $I[m,n]$. So the size of the watermark image, W , is less than or equal to the size of the original image, I . Let the Value of I_{mn} pixel of $I[m,n]$ be i_{mn} and value of W_{mn} pixel of $W[m,n]$ be w_{mn} . $L[\text{row,col}]$ is Location map with

EXTRACTION PROCESS

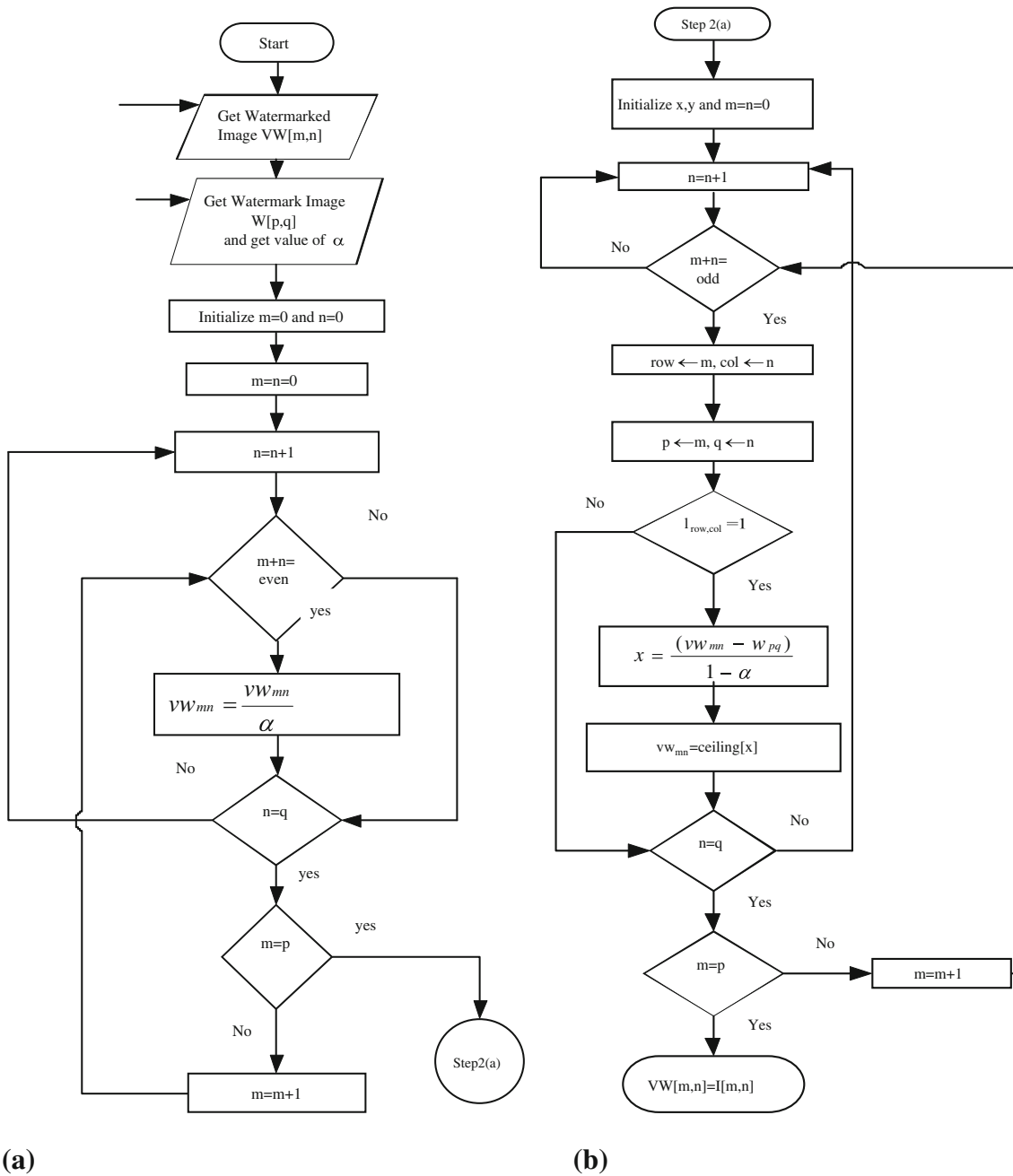


Fig. 4 Flow graph (a, b) demonstrating watermark extraction process

corresponding value of $L_{row,col}$ is $l_{row,col}$

Step 1: Starting from $m=n=0$ and $p=q=0$
 If $m+n$ is an odd integer
 Then the new value of X_{pq} is modified by taking the average pixel value (including the four nearest neighbours) and assigning the value as $X_{pq} = a_{pq}$
 Reiterate until $p=p$ and $q=q$

Step 2: (a) Starting from $m=n=0$ and $p=q=0$
 If $m+n=0$ or an even integer
 Then the new value of X_{pq} is
 $z = (\alpha * x_{pq})$
 Assign the new value as X_{pq}

(b) Starting from $m=n=0$ and $p=q=0$
 If $m+n$ is an odd integer
 Then the new value of X_{pq} is
 $z = [y_{pq} + a_{pq}(1 - \alpha)]_{mod256}$

If $0 \leq Z \leq 256$ go to step 3 otherwise
 Pixel value remain unchanged and mark 0 in corresponding position in location map

Step 3: Modify the pixel value of X_{pq} until $m=p$ and $n=q$.
 mark 1 in corresponding position in location map

Step 4: Set the values as appropriate for the rest of the pixels within the $(m-p)*(n-q)$ set.

2.2 Watermark extraction algorithm

$VW_{m \times n}$ is the watermarked image, $S_{p \times q}$ is the area of the original image corresponding to $W_{p \times q}$.

Step 1: Get the value of α , and the original watermark image.

Step 2: (a) Starting from $m=n=0$
 If $m+n=0$ or an even integer
 Then the new value assigned to S_{pq} is
 $z = (x_{pq} / \alpha)$
 Modify the pixel value of S_{pq} until $m=p$ and $n=q$
 (b) Starting from $m=n=0$
 If $m+n$ is an odd integer and
 (i) if corresponding value of location map is 0
 Keep pixel value unchanged
 (ii) else if corresponding value of location map is 1
 $a = \left(\frac{S_{pq} - w_{pq}}{1 - \alpha} \right)_{mod256}$
 Then the new value assigned to S_{pq} is
 $z = [5a - \text{sum of the four nearest neighbours}]$

Step 3: Modify the pixel value of S_{pq} until $m=p$ and $n=q$.

Step 4: Set the values as appropriate for the rest of the pixels within the $(m-p)*(n-q)$ set.

The following flow chart will explain the watermark embedding and extraction process (see Figs. 3, 4).

3 Results

The proposed watermarking scheme has been implemented in MATLAB and tested on several standard grayscale images and has achieved satisfactory results. Here the results of commonly used grayscale images “Lena” and “F-16” are provided. Watermark of different size has been added for testing maximum PSNR achievable in reference of watermark area and embedded bits per pixel. To subjectively assess the visual quality of the visible watermarked image we uses WSNR and Structural similarity model in this paper [19, 20]. Then we compare proposed work with other state-of-the-art reversible watermarking algorithms proposed by Yang et al. [11] and Liu and Tsai [18]. A comparative plot has been drawn in Figs. 5 and 6 depicting that our scheme outperform as compare to other two scheme. The experimental results are tabulated in Table 1. From data in PSNR column in the table, we can see that, with the increase in payload PSNR value gradually decreases. The minimum value of PSNR is obtained for F-16 which has large smoother region then Lena image. Similarly WSNR and SSIM values of this test images is minimum for F-16. This suggest that visible noise distortion is more in smooth regions, which can be further demonstrated by seeing watermarked images (Fig. 7). Watermark is more visible in F-16 image.

The SSIM value in third column of Table 1 is near one for most images which implies that our watermarking scheme well preserve the visual quality of host image. As the size of watermark increases the SSIM value between original image and watermarked image decreases. This might be due to increase in quantization error that is introduced by our method. This may be thought as drawback of proposed scheme. On comparing with other state-of-the-art, proposed scheme well preserves the visual quality of original image. In Tables 2, 3 and 4 the performance of proposed scheme is compared with other state-of-the-art proposed in [14, 19] on the basis of image quality by employing WSNR and SSIM and the large value indicate the higher quality watermarked image. These comparison result suggest that the fidelity of watermarked image by proposed method is better then other. The higher value of PSNR shows the better performance over other state-of-the-art. Since Yang et al embed reconstruction packet within the watermarked image, so as larger the watermark area less will be the area for reconstruction packet. Thus embedding performance is affected and leading to less visual distortion. Which is reflected with higher SSIM value for larger watermark and can be verified in Table 3.

Fig. 5 Performance comparison of embedded distortion on Lena image with different watermark coverage area in terms of PSNR (a), WSNR (b) and SSIM (c)

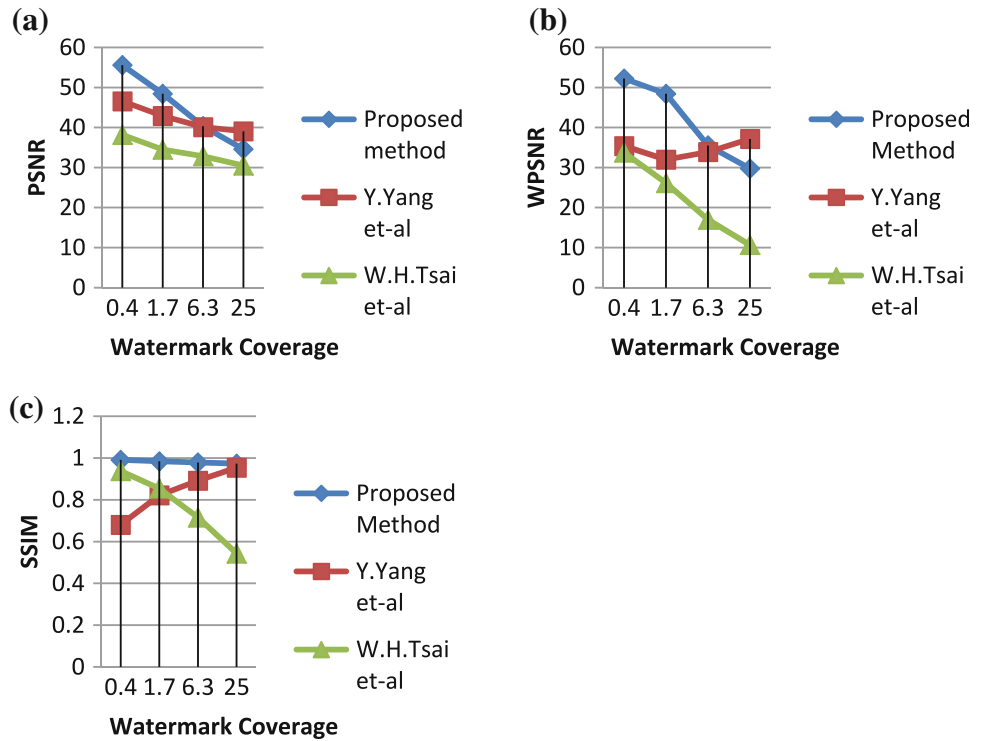


Fig. 6 Performance comparison of embedded distortion on F-16 image with different watermark coverage area in terms of PSNR (a), WSNR (b) and SSIM (c)

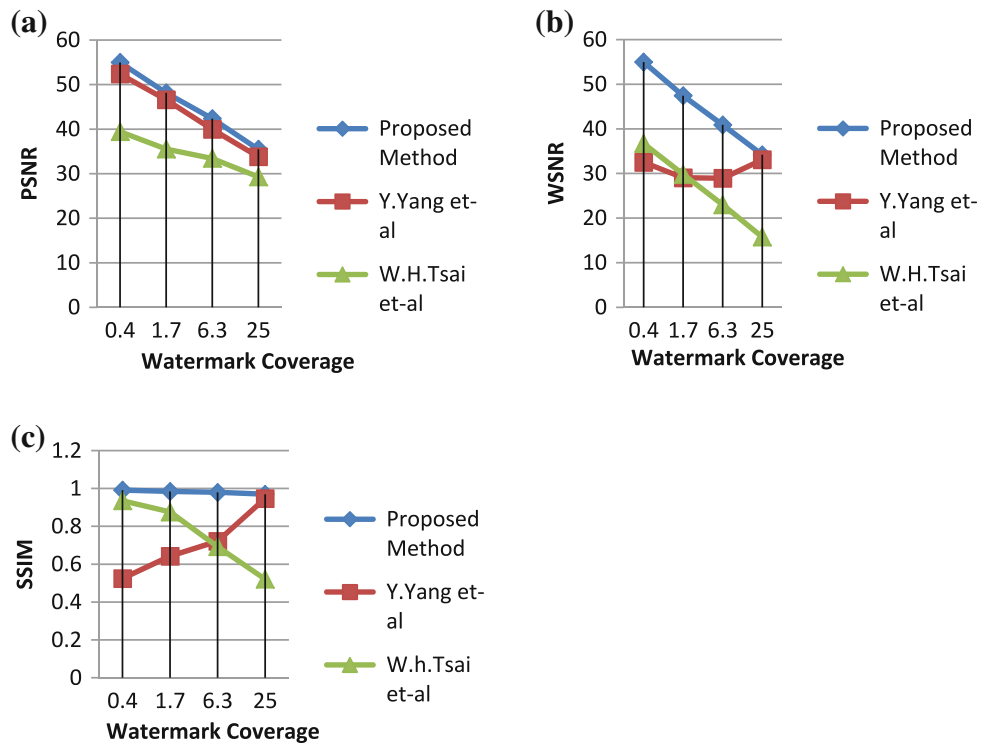




Fig. 7 F-16 and Lena images with different size of watermark embedded

3.1 Security aspects

In our Scheme we require the value of scaling factor ' α ' and location map to retrieve original image. Thus only legitimate user which have correct location map

and correct value of scaling factor ' α ' can extract correctly. The location map can be embedded in encrypted form within watermark image, but it limits the size of watermark that can be embedded in original image.

Table 1 PSNR values with varying watermark coverage area

Original image	Payload (bpp)	PSNR	WSNR	SSIM
F-16	0.012	54.97	54.90	0.9910
	0.05	48.15	47.44	0.9882
	0.15	43.09	42.16	0.9819
	0.19	42.35	40.90	0.9735
	0.34	39.68	38.42	0.9574
	0.52	36.90	35.43	0.9395
	0.60	35.81	34.20	0.9023
	0.75	35.47	33.89	0.8819
	0.99	28.16	27.82	0.8745
	Lena	0.012	55.59	52.22
0.05		48.42	44.74	0.9861
0.15		44.04	42.50	0.9833
0.19		43.54	41.52	0.9765
0.34		40.84	39.35	0.9685
0.52		38.44	37.65	0.9510
0.60		36.59	35.75	0.9489
0.75		35.90	34.06	0.9354
0.99		30.37	30.21	0.9214

Table 2 Performance comparison with different state-of art on the basis of PSNR at different watermark coverage area

	Watermark image size	Watermark coverage (%)	Proposed method	Yang et al. [11]	Tsai et al. [18]
F-16	32 × 32	0.4	54.97	52.37	39.43
	64 × 64	1.7	48.15	46.58	35.52
	128 × 128	6.3	42.35	39.95	33.42
	256 × 256	25	35.47	33.80	29.27
Lena	32 × 32	0.4	55.59	46.57	38.17
	64 × 64	1.7	48.42	42.89	34.49
	128 × 128	6.3	40.34	40.11	32.84
	256 × 256	25	34.58	33.05	30.51

Table 3 Performance comparison with different state-of art on the basis of WSNR at different watermark coverage area

Original image	Watermark image size	Watermark coverage (%)	Proposed method	Yang et al	Tsai et al
F-16	32 × 32	0.4	54.98	32.50	36.71
	64 × 64	1.7	47.44	29.03	29.80
	128 × 128	6.3	40.89	28.91	22.99
	256 × 256	25	34.20	33.08	15.76
Lena	32 × 32	0.4	52.22	35.39	33.76
	64 × 64	1.7	48.42	31.99	26.14
	128 × 128	6.3	35.51	33.88	16.99
	256 × 256	25	29.75	37.14	10.68

Table 4 Performance comparison with different state-of art on the basis of SSIM at different watermark coverage area

Original image	Watermark image size	Watermark coverage (%)	Proposed method	Yang et al	Tsai et al
F-16	32 × 32	0.4	0.9911	0.5247	0.9352
	64 × 64	1.7	0.9844	0.6424	0.8759
	128 × 128	6.3	0.9795	0.7214	0.6927
	256 × 256	25	0.9695	0.9473	0.5213
Lena	32 × 32	0.4	0.9910	0.6807	0.9375
	64 × 64	1.7	0.9843	0.8215	0.8542
	128 × 128	6.3	0.9786	0.8917	0.7156
	256 × 256	25	0.9730	0.9541	0.5429

4 Conclusions

In this study we presented a reversible visible watermarking technique based on pixel mapping. The proposed algorithm considers contrast sensitive functions for the estimation of pixel values to achieve the desired features of visible watermarking. As demonstrated by the experimental results, the proposed method better preserve the visual quality of image. In contrast to the previous reversible watermarking scheme we can add watermark of size nearly equal to the size of host image. The PSNR value for the original and unrecovered watermark image is better than the other methods currently in used. Future work may be directed at making this method blind recoverable and at finding more applications for the presented method such as video watermarking.

References

- Mintzer F, Braudaway GW, Yeung MM (1997) Effective and ineffective digital watermarks. In: Proceeding of international conference on image processing, vol 3
- Mohanty SP, Ramakrishnan KR, Kankanhalli MS (2000) A dct domain visible watermarking technique for images. In: Proceeding of IEEE conference on multimedia and expo, vol 2, pp 1029–1032
- Huang CH, Wu JL (2004) Attacking visible watermarking schemes. *IEEE Trans Multimed* 6(1):16–30
- Bertalmio M, Sapiro G, Caselles V, Ballester C (2000) Image inpainting. In: Proceedings of the 27th annual conference SIG-GRAPH, pp 417–424
- Fridrich J, Goljan M, Du R (2002) Lossless data embedding new paradigm in digital watermarking. in *EURASIP. J Appl Signal Process* 2:185–196
- Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circuits Syst Video Technol* 13(8):890–896
- Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. *IEEE Trans Circuits Syst Video Technol* 16(3):354–362

8. Huang BB, Tang SX (2006) A contrast-sensitive visible watermarking scheme. *IEEE Trans Multiméd* 13(2):60–66
9. Hu Y, Kwong S, Huang J (2006) An algorithm for removable visible watermarking. *IEEE Trans Circuits Syst Video Technol* 16(1):129–133
10. Yang Y, Sun X, Yang H, Li C-T (2008) Removable visible image watermarking algorithm in the discrete cosine transform domain. *J Electron Imaging* 17(3):1–11
11. Yang Y, Sun X, Yang H, Li C-T, Xiao R (2009) A contrast-sensitive reversible visible image watermarking technique. *IEEE Trans Circuits Syst Video Technol* 19(5):656–666
12. Hu Y, Jeon B (2006) Reversible visible watermarking and lossless recovery of original images. *IEEE Trans Circuits Syst Video Technol* 16(11):1423–1429
13. Yip SK, Au PC, Ho CW, Wong HM (2006) Lossless visible watermarking. In: *Proceeding of IEEE international conference on multimedia expo*, Toronto, Canada, pp 853–856
14. Tsai HM, Chang LW (2007) A high secure reversible visible watermarking scheme. In: *Proceeding of IEEE multimedia expo*, Beijing, China, pp 2106–2109
15. Farrugia RA (2010) A reversible visible watermarking scheme for compressed images. In: *Proceeding of IEEE international conference*. MELECON, Valletta, Malta
16. Huang BB, Tang SX (2006) A contrast-sensitive visible watermarking scheme. *IEEE Trans Multiméd* 13(2):60–67
17. Xuan G, Chen J, Zhu J, Shi YQ, Ni Z, Su W (2002) Lossless data hiding based on integer wavelet transform. In: *IEEE workshop on multimedia signal processing*, pp 312–315
18. Liu TY, Tsai WH (2010) Generic lossless visible watermarking—a new approach. *IEEE Trans Image Process* 19(5):1224–1235
19. Venkata ND, Kite TD, Geisler WS, Ivons BL, Bovik AC (2000) Image quality assessment based on degradation model. *IEEE Trans Image Process* 9(4):636–650
20. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structure similarity. *IEEE Trans Image Process* 13(4):600–612
21. Kalker T, Willems FMJ (2002) Capacity bounds and constructions for reversible data-hiding. *Digital Signal Processing* 1:71–76. doi:[10.1109/ICDSP.2002.1027818](https://doi.org/10.1109/ICDSP.2002.1027818)
22. Mintzer F, Lotspiech J, Morimoto N, Heights Y, Almaden T (1997) Safeguarding digital library contents and users. *D-Lib Magazine*
23. Alattar AM (2004) Reversible watermarking using the difference expansion of a generalized integer transform. *IEEE Trans Image Process* 13(8):1147–1156