Implementation of Dual Image Watermarking for Copyright Protection

Soumodeep Das, Subhrajit Sinha Roy, Abhishek Basu, and Avik Chattopadhyay

Abstract In this paper, a copyright protection scheme for images has been developed through dual watermarking method. Here, the watermark, i.e., the copyright information has been embedded visibly and invisibly into the cover image. The visible watermark enhances robustness against signal processing attacks, whereas the invisible watermark is used to prevent different types of malpractices. The proposed scheme has completely been developed in spatial domain, and thus, the system complexity is very low. The system proficiency has been evaluated in terms of the three major qualities: imperceptibility, robustness, and data hiding capacity. The output results, being compared with some other existing methods, confirm the efficacy of the proposed scheme.

Keywords Dual watermarking · Image · Payload · Robust · Visible

1 Introduction

In this modern era, multimedia security is extremely important for data communication and data storing; because, the multimedia objects, being available in digital form, can be augmented or manipulated easily. Data hiding is an art of secured transmission, which is being carried on from centuries [1]. Watermarking is a conventional data hiding concept, which has been used in currency, stamps, and many other

S. Das · S. Sinha Roy (✉) · A. Basu
RCC Institute of Information Technology, Kolkata, India
e-mail: subhrajitkcs@gmail.com

S. Das
e-mail: soumodeep.das@gmail.com

A. Basu
e-mail: idabhishek23@yahoo.com

S. Sinha Roy · A. Chattopadhyay
University of Calcutta, Kolkata, India
e-mail: avikjoy@yahoo.com

P. K. Mallick et al. (eds.), *Advances in Electronics, Communication and Computing*,
Lecture Notes in Electrical Engineering 709,
https://doi.org/10.1007/978-981-15-8752-8_7

government documents from years. With the advancement of data processing, paper watermarking has turned into digital watermarking. Basically, watermark is some asserting information on any multimedia object that can be concealed into that particular object through a definite process, such that the information can also be retrieve to verify the originality. This art of copyright protection is termed as digital watermarking. Data embedding can be performed either in spatial or in frequency domain [2]. Digital images are generally chosen as test object because, images can be represented easily both in spatial and frequency domain. Robustness, imperceptibility, and data hiding capacity are three main characteristics of any digital watermarking method [3]. Robustness means the amount of designated class of transformation that can be handled by the information signal without corrupting the original information. Imperceptibility is the measurement of perceptual resemblance between the original cover and the watermarked object. Data hiding capacity or payload is the maximum amount of information that can be hidden into the informational signal without causing any significant distortion in it. These three characteristics are contradictorily related to each other, and thus, these properties cannot be independently improved [2]. It is a challenging issue for researchers to overcome the trade-offs among these qualities. In this occasion, this paper has proposed a dual watermarking scheme where the watermark is embedded visibly and invisibly at the same time. The visible watermark can be perceived easily, and make an assertion on the cover object. Moreover, it is also robust against most of the signal processing attacks. But, being visible, it can be intentionally removed or manipulated. Thus, this watermark is also embedded invisibly into the cover. Least significant bit (LSB) replacement technique has been used, and for visible watermarking, pixel replacement technique has been involved.

The watermark embedding and extracting for proposed dual image watermarking scheme have been expressed in Sect. 2. The experimental results have been shown in Sect. 3, and these results are compared to the same of some state-of-the-art existing image watermarking techniques. Section 4 consists of the concluding remarks on this proposed work.

2 Proposed Methodology

2.1 Dual Watermark Embedding System

This dual watermarking scheme has been developed to embed copyright information into a gray cover image both in an invisible and a visible way.

Let, H is the gray cover image of size $M \times N$. Therefore, H can be defined as,

$$\boldsymbol{H} = \{h(m,n) | 1 \leq m \leq M, 1 \leq n \leq M \wedge h(m,n) \in [0, 1, 2, \ldots, 255]\} \quad (1)$$

The copyright information has been made binary for invisible watermarking whether it is gray for visible watermarking. For a gray scale watermark G of size $X \times Y$, a binary watermark B has been formed by taking the MSBs of the pixels of G. Let,

$$\boldsymbol{G} = \{g(x, y) | 1 \leq x \leq X, 1 \leq y \leq Y \wedge g(x, y) \in [0, 1, 2, \ldots, 255]\} \quad (2)$$

Now, for any gray scale watermark pixel $g(x, y) \in G$, its corresponding binary image pixel $b(x, y) \in B$ can be formed through a function f: $G \rightarrow B$ is defined as,

$$b(x, y) = \text{mod}\left(\left\lfloor \frac{g(x, y)}{2^7} \right\rfloor\right)$$

Thus, B can be considered as,

$$\boldsymbol{B} = \{b(x, y) | 1 \leq x \leq X, 1 \leq y \leq Y \wedge b(x, y) = [0, 1]\} \quad (3)$$

The invisible or imperceptible watermarking has been performed by embedding the bits of B into H for multiple times through LSB substitution technique, and the watermarked image W is generated. For any cover pixel $h(m, n) \in H$, its analogous watermarked image pixel $w(m, n) \in W$ is generated through a function f_e: $H \times B \rightarrow W$ is defined as,

$$\begin{aligned} w(m, n) &= \sum_{j=3}^{7} w_i(m, n)2^j + \sum_{j=0}^{2} b(x, y)2^j \quad \text{for } (m + n) \bmod 2 = 0 \\ &= \sum_{j=2}^{7} w_i(m, n)2^j \qquad\qquad \text{otherwise} \end{aligned} \quad (4)$$

The binary watermark B is embedded for $t_1 \times t_2$ times to generate the watermarked image W, and a distinct portion in cover H is left to embed the gray scale watermark G, which is kept visible. After embedding G into W, finally, the dual watermarked image D has been produced. Any pixel in W is modified with G to produce the corresponding pixel $d(m, n) \in D$ through another function f_v: $W \times G \rightarrow D$, such that,

$$\begin{aligned} d(m, n) &= g(x, y) \qquad \text{for } m > t_1.M \wedge n > t_2.N \\ &= w(m, n) \qquad \text{otherwise} \end{aligned} \quad (5)$$

Thus, the watermarked image is generated through the proposed dual watermarking method, which has been simplified in Fig. 1.

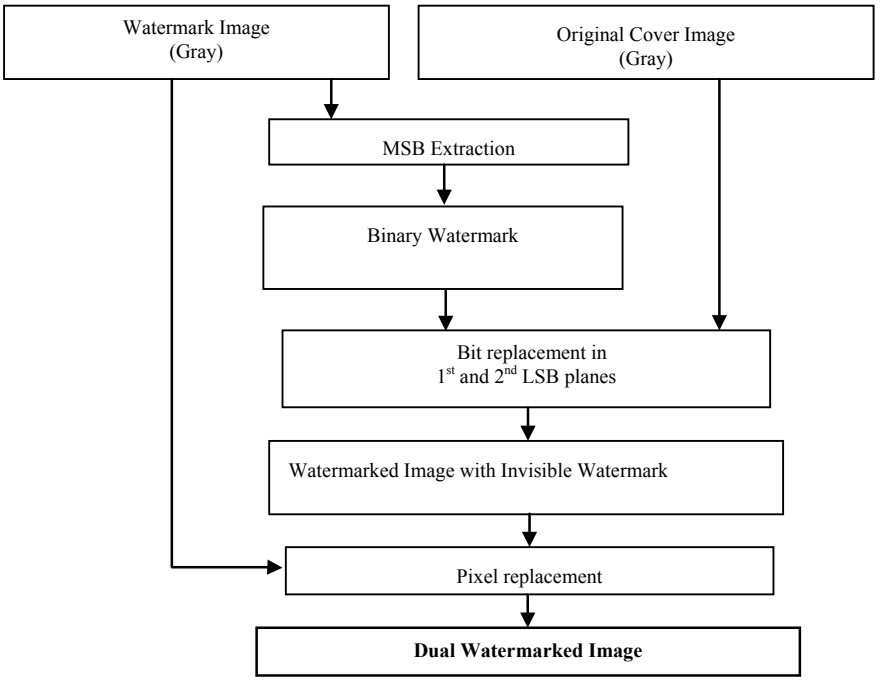

Fig. 1 Block diagram for dual watermark embedding system

2.2 Invisible Watermark Extracting System

The cover can be copyright protected through the visible watermark only. But, as the visible information is not kept in any significant region of the cover, it can be removed without hampering the fundamentals of the cover. Thus, it is very essential to verify the authenticity of the received watermarked image through the invisible watermark; and in this occasion, watermark extracting system has been developed for the invisible information. It is a simple process, illustrated in Fig. 2. Bit retrieval

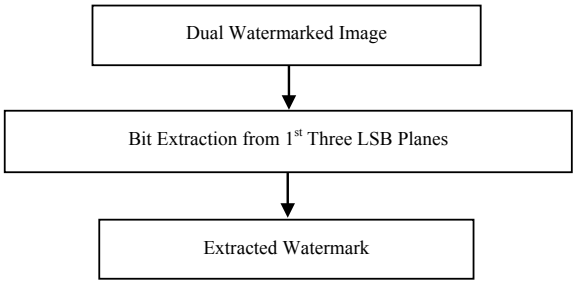

Fig. 2 Block diagram for extracting the invisible watermark

from third LSB planes generates a set of extracted watermarks, which are verified to the original one. Third bit-plane is assumed to be more robust against most of the attacks. The bit extraction process is executed through a function f_z: $D \rightarrow Z$ such that,

$$z(x, y) = \text{mod}\left(\left\lfloor \frac{d(m,n)}{2^2} \right\rfloor\right) \text{when } (m+n) \text{ mod } 2 = 0 \tag{6}$$

where, $z(x, y) \in Z$ and $d(m, n) \in D$.

3 Results and Discussion

The proposed dual image watermarking has been carried out for a few 512 × 512 Gyscale cover images [4]. A binary watermark has been formed from the MSB-plane of a gray scale image of size 130 × 210. This binary watermark has been used as invisible watermark, and for visible watermark, the size of the gray watermark is scaled down to 13 × 21. The invisible and visible watermarks are shown in Fig. 3a, b, respectively. The cover images are shown in Fig. 4a. Figure 4b–e consist of the watermarked images, along with the first three bit-planes of those, after invisible watermarking. The final watermarked images after dual watermarking have been shown in Fig. 4f.

The hiding capacity or payload has been computed as 1.88 bits/pixel for this proposed watermarking scheme. A set of image quality metrics [5, 6] has been involved to compute the imperceptibility and robustness quantitatively. Metric-values given in Table 1, computed from the deviations between the original and watermarked cover images, are related to the imperceptibility of the proposed scheme. Average PSNR value is obtained more than 38 dB, which is good enough for a watermark method, generating a visible watermark in the cover along with information, invisibly embedded in it. Moreover, the values of other metrics are very close to unity, where the values should be equal to unity for two identical signals. Therefore, it is clear that as a dual watermarking method, this proposed scheme can offer a high imperceptibility.

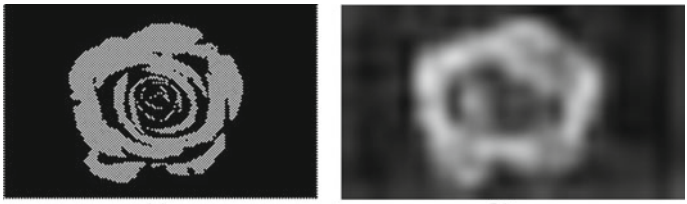

Fig. 3 **a** Binary watermark for invisible watermarking; **b** gray watermark for visible watermarking

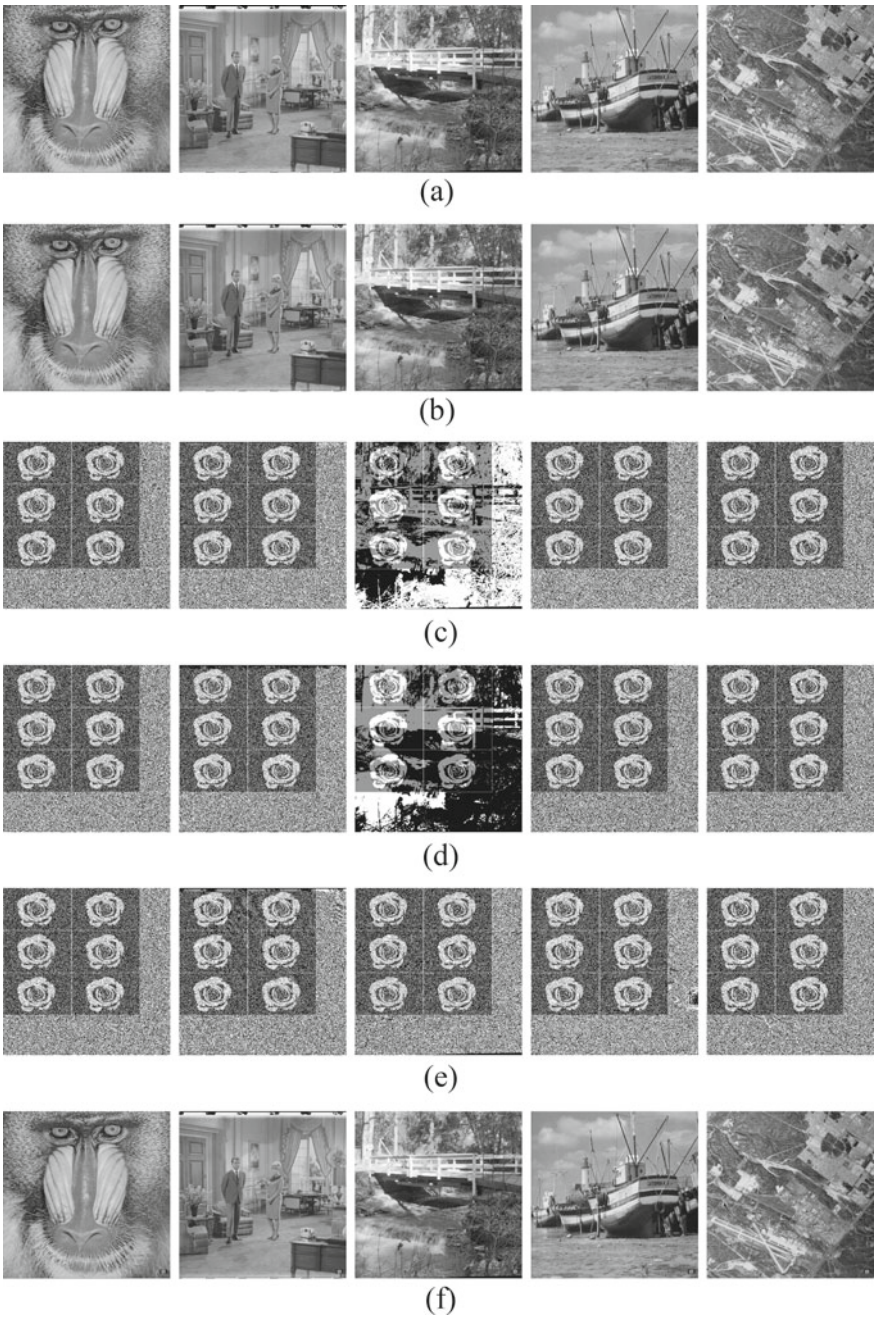

Fig. 4 **a** cover images; **b** invisible watermarked image; **c–e** 1st, 2nd, and 3rd LSB planes of watermarked images, respectively; **f** dual watermarked images

Table 1 Imperceptibility measurement table

Parameters	Lena	Brick house	Boat	Baboon	Peppers
PSNR	38.53585	38.54505	38.51235	38.43301	38.27861
UIQI	0.9997	0.9997	0.9997	0.9996	0.9997
SSIM	0.996174	0.994198	0.996948	0.992932	0.996572
NAD	0.851059	0.861069	0.866226	0.83617	0.850399
NCC	0.996123	0.995665	0.995121	0.995976	0.995868
SC	0.991239	0.991289	0.99075	0.990912	0.990866

Robustness is another important feature to assess the quality of a watermarking scheme. During transmission, the watermarked image may come under various attacks, which may cause distortion in the embedded information. Robustness is the comparison of the watermark, retrieved from the received image, with the original watermark. In this event, a few attacks have been involved here. Results, shown in Table 2, address to the robustness of the proposed scheme. The analogous images of the recovered watermark after different attacks are shown in Fig. 5.

The experimental outputs for this proposed work have been compared with some relevant state-of-the-art existing works, and the comparison results have been provided in Table 3. From this table, it is revealed that this dual watermarking is good enough to overcome the trade-offs between hiding capacity and imperceptibility.

Table 2 Robustness measurement table

Attacks	NC for visible watermark	NC for invisible watermark	SSIM for visible watermark	SSIM for invisible watermark	PSNR for visible watermark	BER for invisible watermark
No attack	1	1	1	1	∞	0%
90° rotation	1	1	1	1	∞	0%
45° rotation	0.8423	0.8883	0.388261	0.998729	14.23 dB	7.77%
Resize (0.75%)	0.9928	0.2530	0.919807	0.974762	26.03 dB	37.70
Median filtering	0.9935	0.7974	0.809286	0.988876	22.02 dB	13.25%
Salt and pepper	0.9615	0.9896	0.971167	0.998225	23.72 dB	1.02%
Gaussian filtering	0.9924	0.2578	0.982794	0.974907	29.98 dB	37.19%
LSB inversion (1st LSB $\leftrightarrow$ 2nd LSB)	1	1	1	1	∞	0%
Negative	1	1	1	1	∞	0%

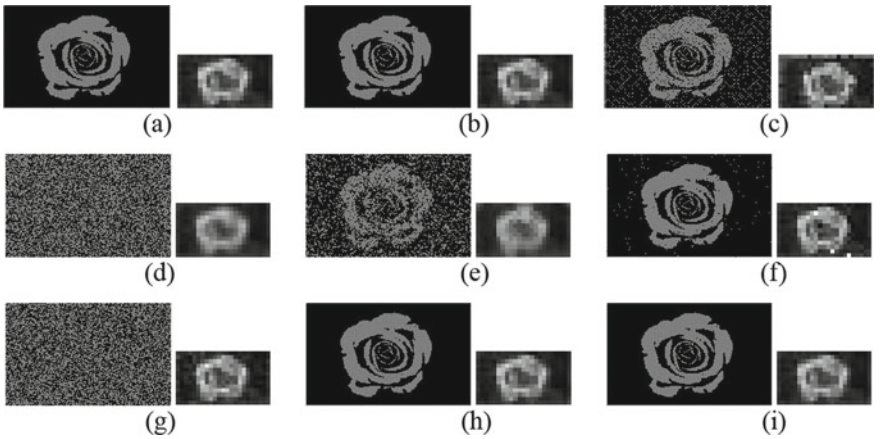

Fig. 5 Invisible and visible recovered watermark after **a** no attack; **b** 90° rotation; **c** 45° rotation; **d** resize; **e** median filtering; **f** salt and pepper attack; **g** Gaussian filtering; **h** LSB inversion; **i** negative attack

Table 3 Comparison table

Methods	PSNR (dB)	Payload (bpp)
Proposed scheme	38.5	1.88
Kumar et al.'s scheme [7]	35	0.5
Su et al.'s scheme [8]	50	0.001
Wong et al.'s scheme [9]	45.83	0.58
Gui et al.'s scheme [10]	34.26	1

4 Conclusion

A dual watermarking scheme has been executed in this proposed work as a contribution to the area of digital multimedia copyright protection. As the watermark is simultaneously appeared in the cover both in visible and invisible way, the data security is confirmed with high robustness. Moreover, the imperceptibility is also optimized with increased payload. Being a spatial domain-based technique, its hardware will be easy to implement, and thus, it can be executed in the near future with low computational cost.

References

1. Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Boston, London: Artech House.
2. Sinha Roy, S., Basu, A., & Chattopadhyay, A. (2019). *Intelligent copyright protection for images* (1st ed.). Taylor and Francis, New York, USA: CRC.

3. Mohanty, S. P. (1999). Digital watermarking: A tutorial review. https://www.csee.usf.edu. Accessed 1999.
4. https://sipi.usc.edu/database/database.php?volume=misc.
5. Sinha Roy, S., Saha, S., & Basu, A. (2015). Generic testing architectures for digital watermarking. In *Proceedings of National Conference on Frontline Research in Computer, Communication and Drive (FRCCD)* (pp. 50–58).
6. Kutter, M., & Petitcolas, F. A. P. (1999). Fair benchmark for image watermarking systems. In *Security and watermarking of multimedia contents* (Vol. 3657, pp. 226–239) Bellingham: SPIE.
7. Kumar, C., Singh, A. K., & Kumar, P. (2018). Improved wavelet-based image watermarking through SPIHT. In *Multimedia tools and application* (p. 14). Berlin: Springer.
8. Su, Q., & Chen, B. (2017). Robust color image watermarking technique in the spatial domain. *Soft Computing—A Fusion of Foundations, Methodologies and Applications, 22*(1), 91–106.
9. Wong, M. L. D., Chong, N. S., Lau, S. I. J., & Sim, K. Y. (2013). A salient region watermarking scheme for digital mammogram authentication. *International Journal of Innovation, Management and Technology, 4*(2), 228–232.
10. Gui, X., Li, X., & Yang, B. (2014). A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. *Signal Processing, 98*, 370–380.