Digital Image Watermarking Through Encryption and DWT for Copyright Protection

Sarita P. Ambadekar, Jayshree Jain and Jayshree Khanapuri

Abstract Sharing of copyright documents, images, audios, and videos on Internet has become easier due to content authentication using digital watermarking. It also finds applications in the area of content protection, copyright management, and tamper detection. With the use of sophisticated signal/image processing algorithms, manipulations and duplications of audio, images, and videos are much easier. Hence, content authentication through encryption and resistance to general attacks such as noise, compression, and geometric has become an urgent and important issue. In this study, authors have proposed digital image watermarking technique based on discrete wavelet transform (DWT) and encryption. Watermark embedding and extraction algorithm using DWT coefficients, distance measurement, and encryption are demonstrated. DWT through multiresolution analysis provides the much needed simplicity in watermark embedding and extraction through watermark encryption. The technique results in PSNR greater than 50 dB and is resistance to noise, geometric, and compression attack. The proposed technique may be applied for copyright and content authentication applications.

Keywords Image watermarking · Discrete wavelet transform · Encryption
PSNR · Copyright protection

1 Introduction

The tremendous growth of high-speed LAN, WAN, MAN, and Internet technology have delivered means of new business, scientific, entertainment, and social prospects in the form of electronic broadcasting and marketing. The cost-effectiveness of sharing information and data in the form of digital documents, images, audios, and video

S. P. Ambadekar (✉) · J. Khanapuri
K. J. Somaiya Institute of Engineering and Information Technology, Mumbai, India
e-mail: sarita.ambadekar@somaiya.edu

J. Jain
IICE, Udaipur, India

S. Bhattacharyya et al. (eds.), *Recent Trends in Signal and Image Processing*,
Advances in Intelligent Systems and Computing 727,
https://doi.org/10.1007/978-981-10-8863-6_19

sequences by transmission over high-speed computer networks is greatly improved due to the advancement in Internet technology. Moreover transmission of digital information through Internet is very fast, low cost, and last but not least mostly without losing quality. Editing, copying, and tempering of data are easy because one can get access to the data through various means. Furthermore, a copy of a digital record is indistinguishable from the original record. Therefore, copyright protection and content authentication are becoming increasingly difficult tasks for digital data. Encryption/decryption techniques can be applied to restrict access to the data. However, encryption technique is unsuitable whenever the important data or information is decrypted and that can be manipulated and freely shared over the network. Digital image watermarking techniques are widely used for copyright protection and content authentication. However, continuous efforts are required to improve its performance due to new requirements and challenges such as multiple attacks and information sharing on social media Web sites [1–3]. A lot of information, authentic documents, government circulars, photographs, audios, and videos are shared on whats app and facebook. These original documents and images are subject to manipulations using sophisticated signal/image processing algorithms. Typically original images undergo various forms of manipulations such as cropping, geometric translation, contrast enhancement, and compression before being shared on Web sites or apps. Also when these images are shared and transmitted through communication networks are vulnerable to noise attack. Digital image watermarking plays important role in protection and authentication of images through watermark. Watermark can be an image embedded into the original image through watermarking algorithms. Yet watermark image can be visually invisible and recognizable when recovered from the original image even after being prone to multiple attacks [4–7]. It is possible to identify, remove, or change embedded watermark through sophisticated signal/image processing algorithms. Watermark being the identity of the content owner needs protection even after removed from the original document or image or video. Encryption provides additional security to the original watermark image in the event of unauthorized watermark extraction and manipulation. By the application of transforms such as DFT, DCT, and DWT, watermarking can be applied in the frequency domain [4–6]. Watermarking techniques using DCT are found to be more robust as compared to simple techniques applied in temporal domain [8]. Transform domain algorithms are robust against common signal and image processing operations like contrast enhancement, low-pass filtering, brightness adjustment, blurring [9–12]. However, their disadvantages are computationally expensive, difficult to implement and weak against geometric attacks like rotation, scaling, cropping [11]. DWT through multiresolution analysis provides the much-needed simplicity in watermark embedding and extraction through watermark encryption. DWT decomposes image with a normalized basis set. Thus, it can embed the watermark in any frequency band of a cover image [3]. In this study, authors have proposed digital image watermarking technique based on discrete wavelet transform (DWT) and encryption. Watermark embedding and extraction algorithm are devised and results are compared using watermarking parameters and its resistance to attack. The paper is organized as Sect. 2 describes the embedding and extraction algorithm, Sect. 3 illustrates results and concluded in Sect. 4.

2 Watermark Embedding Algorithm

Firstly, an image encryption algorithm based on row and column rotation through random number generator key k of the watermark image is performed. In this paper, we have used 90 × 90 pixels grayscale baboon image as watermark. Figure 1 shows the original watermark image and encrypted image.

Secondly, the original input image is decomposed using two-dimensional (2D) DWT to obtain the relevant scaled images with reduced size. Also, the encrypted watermark image is decomposed using 2D DWT to obtain decomposed scaled watermark images. Figure 2 shows the multiresolution decomposed images obtained after 2D DWT on original input and watermark image.

Thirdly, the pixel point at decomposed input image for embedding of the decomposed watermark image was identified based on Euclidean distance. More is the similarity between the input and watermark image, perceptibility of the input image does not change and increases the strength of watermark. Thus, it is more suitable for embedding watermark into the input image.

Fourthly, encrypted watermark was embedded into input image using (1) depending on the match between decomposed images of input and encrypted watermark image

$$y(i, j) = (1 - \text{alpha}) * i(i, j) + \text{alpha} * iw(i, j) \quad (1)$$

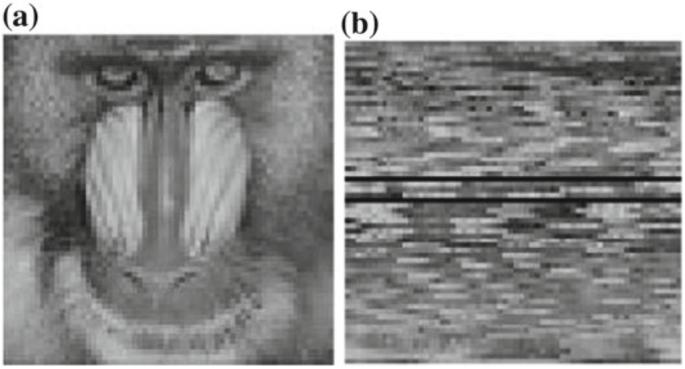

Fig. 1 **a** Original watermark image **b** encrypted watermark image

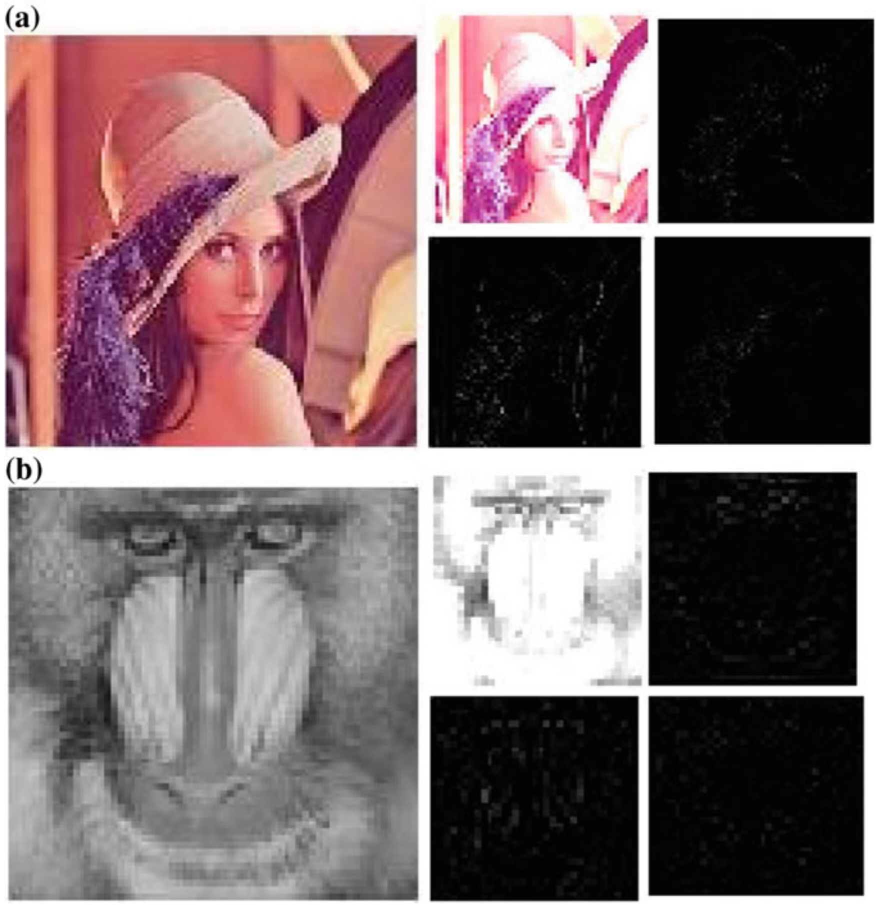

Fig. 2 Decomposition of image through 2D DWT **a** original input image **b** watermark image

where alpha is visibility coefficient, i(i, j) are DWT coefficients of respective decomposed input image, iw(i, j) are DWT coefficients of respective decomposed watermark image, and y(i, j) are the DWT coefficients of the watermark embedded output image.

The process for the watermark embedding algorithm is shown in Fig. 3.

3 Watermark Extraction and Detection Algorithm

The watermark extraction is exactly reverse procedure of watermark embedding. The algorithm presented in this paper is non-blind and therefore requires original input image and encryption key for watermark extraction and detection. The similarity between the original watermark image and extracted watermark image was measured

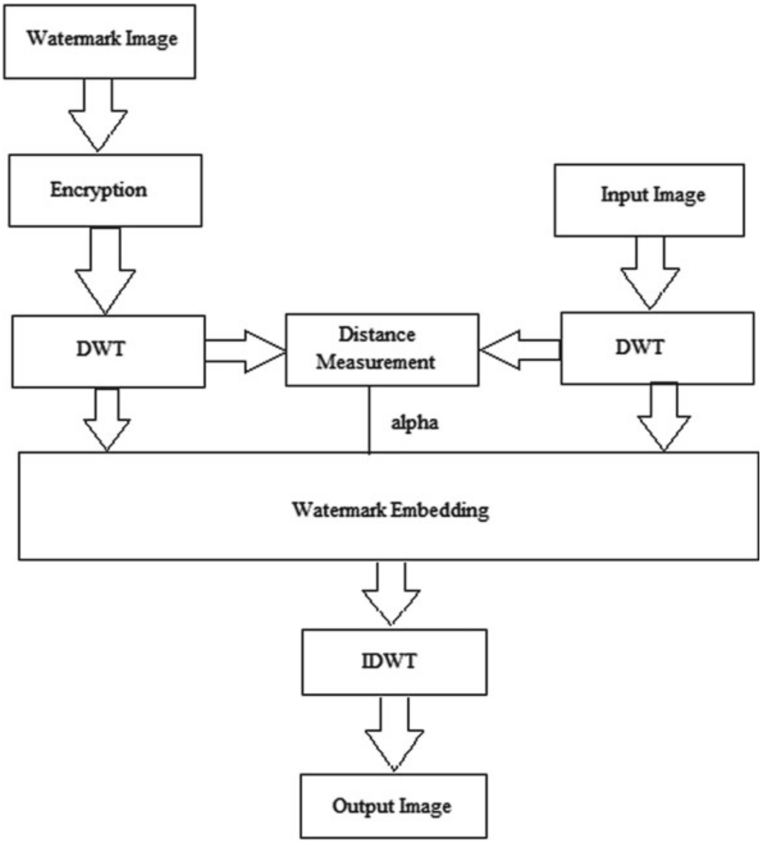

Fig. 3 Watermark embedding algorithm

using three parameters: mean square error (MSE), normalized correlation coefficient (CC), and peak signal to noise ratio (PSNR). In general, value of CC > 0.75 and PSNR > 30 dB is considered acceptable. Also, it is necessary to evaluate these watermarking parameters at various signal processing attacks. Watermark extraction algorithm is shown in Fig. 4.

4 Results and Discussion

Watermark embedding and extraction algorithm was implemented using MATLAB software and executed on intel i5 processor with 1 GB RAM and 3 GHz processing speed. In this paper, Lena image of size 228 × 228 and baboon image of size 90 × 90

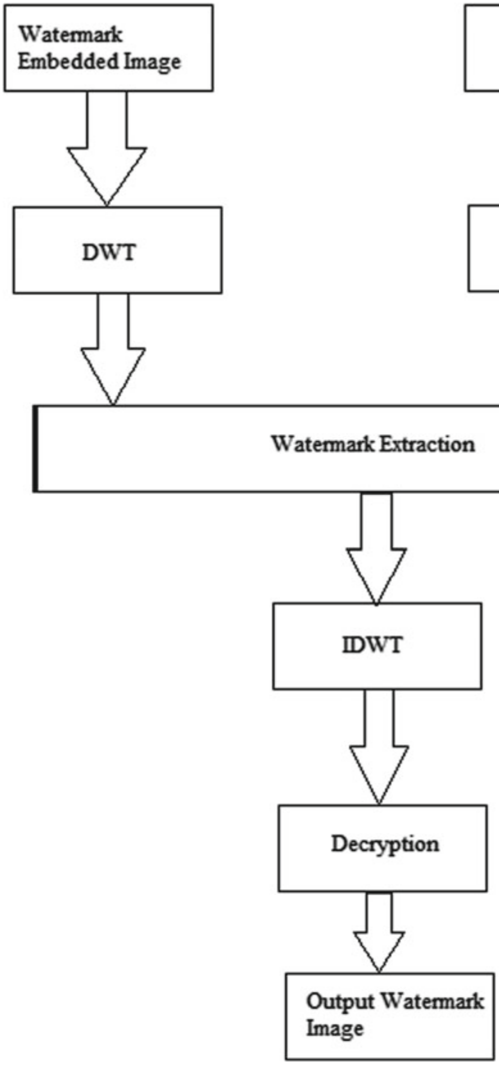

Fig. 4 Watermark extraction algorithm

were selected as input and watermark images, respectively. Figure 5 shows the original input image, watermark image, watermark embedded image, and extracted watermark image.

The performance of the presented algorithm is evaluated through three parameters MSE, CC, and PSNR. Also, the comparison of the experimentally obtained parameters was performed under two different conditions with and without attacks. Three general attacks such as salt-and-pepper noise, geometrical attack through rotation and JPEG compression attack were considered. In this experiment, salt-and-pepper

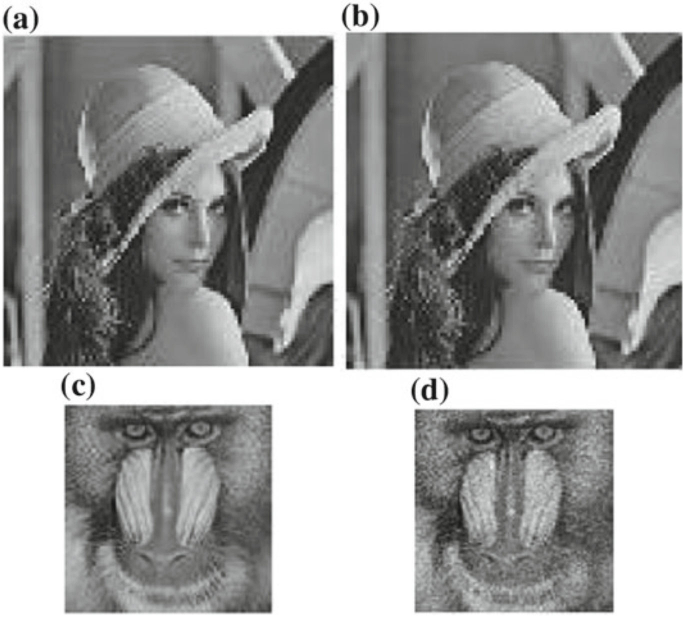

Fig. 5 **a** Original input image **b** watermark embedded image **c** original watermark image **d** extracted watermark image

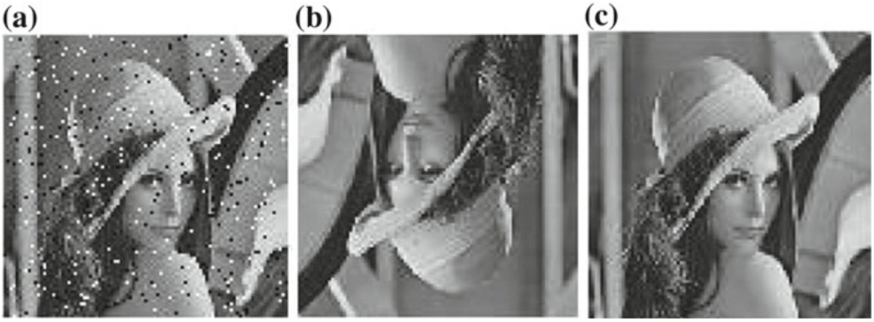

Fig. 6 Attacks on watermark embedded image **a** salt-and-pepper noise **b** rotation and **c** compression

noise of density 0.01, compression ratio of 2, and rotation of 90° was added into the watermark embedded image. Figure 6 shows the three types of attacks on watermark embedded image used for extraction algorithms. Table 1 shows the watermarking parameters evaluated between original watermark image and extracted watermark image at various attacks and without attacks. Comparison of PSNR with other methods through DWT is given in Table 2.

Obtain results validate the presented watermark embedding and extraction algorithm. DWT along with encryption provides better robustness to the algorithm for

Table 1 Watermarking parameters

Parameter	With attack			Without attack
	Noise	Geometric	Compression	
MSE	0.2053	0.2071	0.2033	0.2047
PSNR (dB)	55.006	54.96	55.04	55.01
CC	0.92	0.97	0.97	0.9749

Table 2 Comparison of PSNR (dB) values

Images	Proposed method	Vaidya et al. [2]	Peng et al. [13]
Lena	54.96	47.29	32.96

three general attacks. It has especially demonstrated better robustness against compression attack. Presented algorithm is simple to implement and provides some security to watermark through encryption key that can be suitable for applications such as Facebook and what's up that runs on android operating systems based devices.

5 Conclusion

In this paper, digital image watermarking algorithm through DWT and encryption for most common application facebook and whats app is presented. Robustness of the algorithm for general attacks such as salt-and-pepper noise, rotation, and compression is demonstrated. The presented algorithm is more suitable since simple convolution technique can be employed for computation of DWT, encryption with simple row and column rotation and pseudo-random number generator can be easily implemented on any device operating on android operating system. Further, robustness against geometrical distortions is focus of research in the implementation of watermarking algorithms.

References

1. Huang X, Zhao S (2012) An adaptive digital image watermarking algorithm based on morphological Haar wavelet transform. In: International conference on solid state devices and materials science, vol 25. Elsevier, Physics Procedia, pp 568–575
2. Vaidya P et al (2015) Adaptive digital watermarking for copyright protection of digital images in wavelet domain. In: 2nd international symposium on computer vision & internet, vol 58. Elsevier, Procedia Computer Science, pp 233–240
3. Chen L, Zhao J (2015) Adaptive digital watermarking using RDWT and SVD. In: IEEE international symposium on haptic, audio and visual environments and games (HAVE)
4. Roldan LR, Hernández MC, Chao J, Miyatake MN, Meana HP (2016) Watermarking-based color image authentication with detection and recovery capability. IEEE Lat Am Trans 14(2):1050–1057

5. Roy A, Maiti AK, Ghosh K (2015) A perception based color image adaptive watermarking scheme in YCbCr space. In: 2nd IEEE international conference on signal processing and integrated networks (SPIN)
6. Yadav N, Singh K (2015) Transform domain robust image-adaptive watermarking: prevalent techniques and their evaluation. In: IEEE international conference on computing, communication and automation
7. Shukla D, Tiwari N, Dubey D (2016) Survey on digital watermarking techniques. Int J Sig Process Image Process Pattern Recogn 9(1):239–244
8. Tao H et al (2014) Robust image watermarking theories and techniques: a review. J Appl Res Technol 12:122–138
9. Maity HK, Maity SP (2015) Multiple predictors based RW scheme with adaptive image partitioning. In: IEEE international conference on advances in computing, communications and informatics
10. Pushpa Mala S et al (2015) Digital image watermarking techniques: a review. Int J Comput Sci Secur 9(3):140–156
11. Maiorana E et al (2016) High-capacity watermarking of high dynamic range images. EURASIP J Image Video Process. Springer
12. Jagadeesh B et al (2015) Fuzzy inference system based robust digital image watermarking technique using discrete cosine transform. In: International conference on information and communication technologies, vol 45. Elsevier, Procedia Computer Science, pp 1618–1625
13. Peng F et al (2012) Adaptive reversible data hiding scheme based on integer transform. Sig Process 92(1):54–62