Improving the Robustness of ISB Watermarking Techniques by Repetition of the Embedding

Akram M. Zeki[1], Azizah A. Manaf[2], and Shayma'a S. Mahmod[3]

[1] Department of Information System,
Kulliyyah of Information & Communication Technology,
International Islamic University Malaysia, Malaysia
akramzeki@iiu.edu.my
[2] Advanced Informatics School (AIS),
University Technology Malaysia, Malaysia
azizah07@ic.utm.my
[3] Department of Electrical and Computer Engineering,
Kulliyyah of Engineering,
International Islamic University Malaysia, Malaysia
shay_sinan@yahoo.co.uk

Abstract. Digital watermarking is a direct embedding of additional information into the original content or host image, this study is overcome the problems existing in the classic LSB method by adapting the method to intermediate significant bits (ISB), which improve the robustness and maintain the quality of the image. Enhancing the proposed method has been done by repeating the watermark data certain number of times (3, 5, 7, and 9 times) in order to improve the robustness of the watermarking technique, correspondingly, a majority criterion is used in the watermark detecting procedure, which makes the algorithm more robust, especially to the geometric transform attacks.

Keywords: Watermarking, Robustness, ISB, LSB.

1 Introduction

In general, watermark can be embedded in spatial domain or in transform domain of an image. The spatial domain is a domain in which an image is represented by the intensities at given points in space. This is the most common representation for image data. In the spatial domain approach, the pixel value of an image is modified to embed the watermark information [1]. Many studies [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] have used these spatial domain techniques.

In the transform domain approach, some sorts of transform are applied to the original image first. The watermark is embedded by modifying the transform domain coefficients. The applied transform may be Discrete Cosine Transform (DCT) [14] [15] [16], Discrete Fourier Transform (DFT) [17], or Discrete Wavelet Transform (DWT) [18].

J.M. Zain et al. (Eds.): ICSECS 2011, Part I, CCIS 179, pp. 592–599, 2011.

2 Bit-Plane Model

A bit-plane of digital images is a set of bits having the same position in the respective binary numbers. To penetrate an image, the grey-scale of each pixel is decomposed into its 8 different bits; the first bit-plane contains the set of the most significant bits and the 8th bit-plane contains the least significant bits. This simple LSB embedding approach is easy for computation, and a large amount of data can be embedded without great quality loss. The more LSBs are used for embedding, the more distorted result will be produced. Not all pixels in an image can tolerate equal amounts of changes without causing notice to an observer. The largest number of the LSBs, whose grey values can be changed without producing a perceptible artifact in each pixel, is different.

The next step after selecting one bit-plane for embedding is to find the ranges of the chosen bit-plane, the length of the range L is 2k-1 (L = the maximum value of each range – the minimum value of the range + 1) and the number of ranges in each bit-plane is 256 / L. It can be noticed that in each range, the bit changes between 0 and 1, as shown in Figure 3 below.

3 Bit-Plane Model

In this paper, the ISB method founded by (Akram and Azizah, 2009) will be implemented and repeated 3, 5, 7 and 9 times in order to improve the robustness. In the proposed technique a tradeoff between the image quality and robustness has to be reached and the robustness of the system will be improvement by repeating the embedding. Figure 1 show the structure of the proposed scheme.

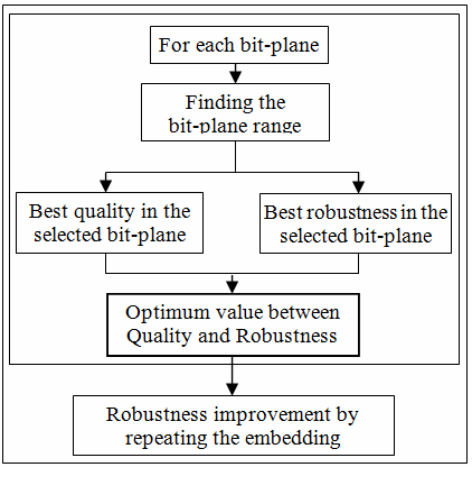

Fig. 1. A flow chart of the proposed approach based on bit-plane model

3.1 Embedding Model

The embedding model is based on the ISB method [19], this method was found the best embedding status that can survive against different types of attacks and at the same time keeping minimum image distortion (the threshold value) where the best pixel value in between the middle and the edge of the range of bit-plane model, assume that the bias value is at least the distance from the position of the watermarked pixel to the edge of the range (which is more close to the original pixel). That means if the distance from the pixel to the edge of the range is greater than the bias value, then the position of the pixel will not change. While if the distance from the pixel to the edge of the range is smaller than the bias value, then the position of the pixel will change to be as far as the bias value.

The best robustness can be obtained when the bias value is maximum, (in the middle of ranges) while the worst one when the bias value is minimum (in the edges of ranges). Regarding the quality, the best image quality when the bias value is minimum, while the worst one when the bias value is maximum. And the best embedding status was addressed when the bias value is 6 [19].

3.2 Repetition of the Embedding

In this section, robustness is improved by repeating the embedded bits. The first step of the watermark generation is to repeat each bit of the hidden information for a certain number of times. Correspondingly, a majority criterion is used in the watermark detecting procedure, which makes the algorithm more robust, especially to the geometric transform attacks and noise attack [20].

The watermark is then encoded by repeating the original signal R times, in a block section, known s the block section (R, 1). For example, in case three repetitions are done (R=3), the image is partitioned into blocks with the size of 3 pixels, as shown in Figure 2 below.

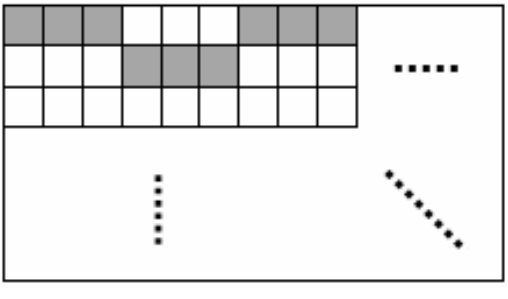

Fig. 2. Partitioned the image into blocks in the size of 3 pixels to repeat the embedding within each block

During the embedding, the watermarked object is considered as a long sequence of bits; if the watermark bits contain the following bits: (101010), every bit is embedded 3 times, as shown in Figure 3 below.

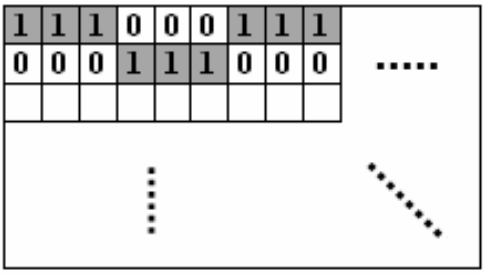

Fig. 3. Repeating the embedding within the blocks

In the decoding process, the majority elements of the block section are used to reconstruct the original signal. For example, R=3 in the binary signal and the (000) represents 0, the (111) represents 1; while (010, 100 or 001) represent 0 and (101, 110 or 011) represents 1, i.e. the reconstructed signal becomes '0' if the number of '0's is 2 or more in the block section; otherwise, it is '1' [22].

In other words, if the value of the extracted bit is repeated (1 + number of repetition / 2) times or more, (i.e. R` ≥ 1 + R/2) the value is then selected as an extracted bit, i.e. if "1" is extracted in most of the pixels in the block, the bit with value "1" is considered for reconstructing the watermark. If "0" is extracted in most of the pixels in the block, the bit with value "0" is considered for reconstructing the watermark. For 5 repetitions, if the value of the bit is redundant (R`) 3 times or more, the value is selected as an extracted bit. As for 7 repetitions, if the value of the bit is redundant (R`) 4 times or more, the value is selected as an extracted bit. For 9 repetitions, if the value of the bit is redundant (R`) 5 times or more, the value is selected as an extracted bit [23].

As for a higher number of repetitions, it can give better robustness because the maximum number of repeating watermarks embedding R is shown in Equation 1.

$$R = floor\ R' \tag{1}$$

Where the floor is a function whose value is the largest integer less than or equal to R', and R' is the size of host image / the size of watermark object. If the number of repetition increases, the capacity of embedding is decreased, as shown in Equations 2 and 3.

$$New\ Capacity\ (C`) = Old\ Capacity\ (C) / Size\ of\ the\ block \tag{2}$$

$$New\ Capacity = \frac{\text{Total numberof bytes of data hiding}}{\text{Total numberof bytes of coverimage} \times \text{Size of the block}} \tag{3}$$

3.3 Implementation and Experimental Results

In this study, grey scale image (logo) contains 90 × 90 pixels as shown in Figure 4 will be embedded within three host images containing 256 × 256 pixels as shown in Figure 5. To improve the security of the system, the watermark object is encrypted using Random Pixel Manipulation Technique [21]. In this technique, a key is chosen.

This key is a string which can be effectively manipulated to obtain a random number sequence. This sequence is then used to 'scramble' the hidden data.

The repetition of the embedding will be done 3, 5, 7 and 9 times in the 4th bit-plane of the host images with the bias value = 6. The idea of repeating the embedding was to increase the robustness of the watermark system against all types of attacks, specifically against the geometric transform attacks.

Fig. 4. Grey scale logo with 90 × 90 pixels.

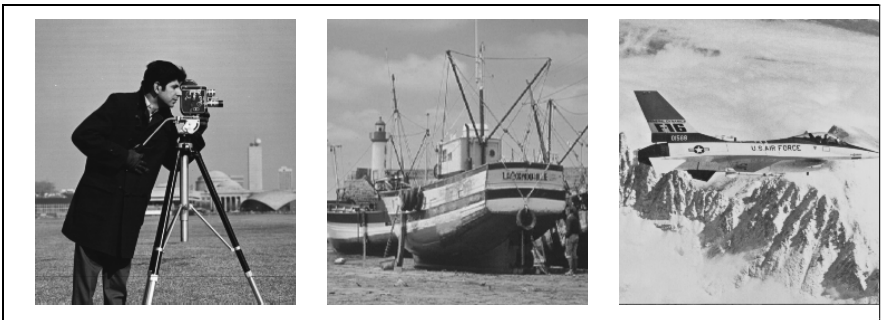

Fig. 5. Grey scale host image with 256 × 256 pixels.

To study the proposed method, under different image processing operations (Attacks), the following attacks will be applied to the image: Lossy compression with 85% compression level, Blurring, Gaussian filter, Wiener filter, Speckle noise, and geometric transform attacks (Rotation and Scaling).

During the extracting stage the encrypted logos have been extracted and they are decrypting to the original images by the same key has been used during encryption stage.

The watermark image was extracted from Hosts 1 to 3, and the normalized cross correlation (NCC) was measured for every embedding in different sizes of blocks, as shown in Tables 1 - 3, respectively.

Table 1. The NCC of the 4th Bit Plane at Bias value =6 for host 1

Repeating	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.931264	0.910986	0.919141	0.847613	0.932271	0.799517	0.809247
3	0.951085	0.968978	0.935721	0.864331	0.977016	0.852578	0.863577
5	0.97888	0.978954	0.963583	0.891514	0.989924	0.888657	0.894251
7	0.985841	0.986548	0.978995	0.94775	0.993589	0.931555	0.948953
9	0.998977	0.99039	0.981728	0.999882	0.995276	0.998842	0.993604

Table 2. The NCC of the 4th Bit Plane at Bias value =6 for host 2

Repeating	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.917325	0.899574	0.911418	0.871249	0.886982	0.799517	0.809229
3	0.947652	0.946014	0.951353	0.890363	0.936686	0.852578	0.863583
5	0.978366	0.964745	0.978446	0.911319	0.96874	0.888657	0.894242
7	0.983007	0.978428	0.98172	0.954946	0.983741	0.931555	0.948957
9	0.990667	0.98278	0.985976	0.997542	0.990698	0.998842	0.993601

Table 3. The NCC of the 4th Bit Plane at Bias value =6 for host 3.

Repeating	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.90519	0.863423	0.873039	0.855802	0.817691	0.799517	0.8093
3	0.942476	0.905038	0.910462	0.886317	0.871951	0.852578	0.863536
5	0.967077	0.934157	0.940517	0.898179	0.893755	0.888657	0.894255
7	0.984243	0.954411	0.95745	0.939749	0.929244	0.931555	0.948957
9	0.993528	0.959585	0.963423	0.999382	0.948403	0.998842	0.993604

The above tables show that the value of the NCC increases with the increasing of embedding times for all the attacks. The result of NCC was found to be very close to 1, after nine repetitions.

Figure 6 below presents the results gathered for the NCC of the different attacks, after (3, 5, 7, and 9) times repeating of the embedding.

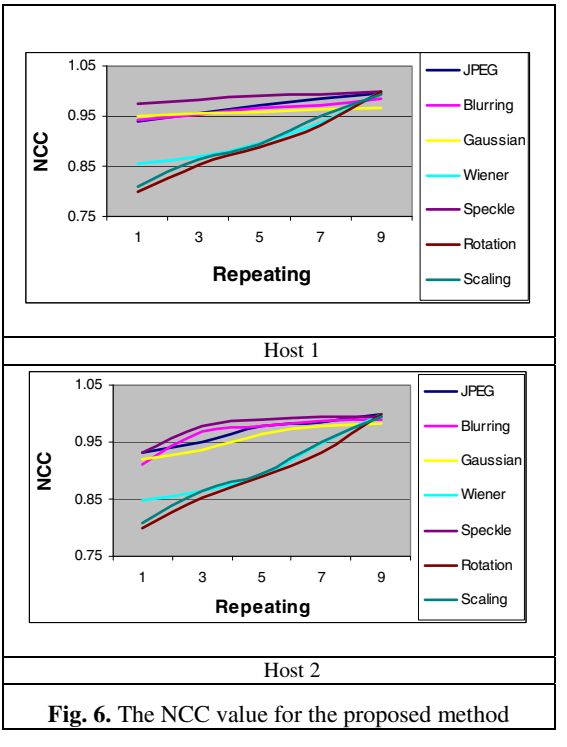

Fig. 6. The NCC value for the proposed method

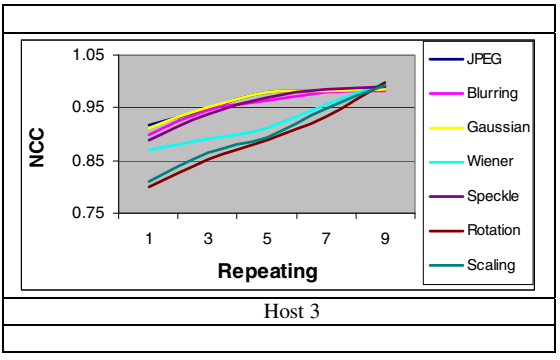

Fig. 6. (*continued*)

The above figures show different graphs for the three host images which illustrate the relation between the number of repeating and the NCC values for all the attacks. At the same time, these figures also show that the value of the NCC increased when the embedding number for all the attacks was increased, including the geometric transform attacks (Rotation and Scaling), which were not improved when the method based on only one pixel was used. The result of the NCC for all the attacks was found to be very close to 1 after nine reparations.

4 Conclusion

Digital watermarking technique based on intermediate significant bit (ISB) has been implemented by this paper. This technique can survive against different types of attacks and at the same time keep the quality of the image. The embedding data has been repeated certain number of times. The idea of repeating the embedding was to increase the robustness of the watermark system against all types of attacks, specifically against the geometric transform attacks. In the present study, the capacity of embedding was found to be decreased by increasing the number of repeating times. The repetition was done 3, 5, 7 and 9 times, by embedding the watermark image, in all host images within the 4th bit-plane with the bias value = 6. The results show that the value of the NCC increases with the increase of embedding times for all attacks. The result of NCC was found to be very close to 1, after nine repetitions.

References

1. Chen, P.C.: On the Study of Watermarking Application in WWW – Modelling, Performance Analysis, and Applications of Digital Image Watermarking Systems. Ph.D. Thesis, Monash University (1999)
2. Chan, C.K., Cheng, L.M.: Hiding data in images by simple LSB substitution. Pattern Recognition, 469–474 (March 2004)
3. Chang, C.C., Hsiao, J.Y., Chan, C.S.: Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognition 36(7), 1583–1595 (2003)

4. Chang, C.C., Tseng, H.W.: A Steganographic method for digital images using side match. Pattern Recognition Letters 25, 1431–1437 (2004)
5. Lin, C.C., Tsai, W.H.: Secret image sharing with steganography and authentication. Journal of Systems and Software 73, 405–414 (2004)
6. Lou, D.C., Liu, J.L.: Steganographic method for secure communications. Computers and Security 21, 449–460 (2002)
7. Marvel, L.M., Boncelet, C.G., Retter, C.T.: Spread spectrum image steganography. IEEE Transactions on Image Processing 8, 1075–1083 (1999)
8. Thien, C.C., Lin, J.C.: A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognition 36(12), 2875–2881 (2003)
9. Wang, R.Z., Lin, C.F., Lin, J.C.: Image hiding by optimal lsb substitution and genetic algorithm. Pattern Recognition 34(3), 671–683 (2001)
10. Wu, D.C., Tsai, W.H.: A steganographic method for images by pixel-value differencing. Pattern Recognition Letters 24(9-10), 1613–1626 (2003)
11. Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S.: Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proceedings of Visual Image Signal Process 152, 611–615 (2005)
12. Yu, Y.H., Chang, C.C., Hu, Y.C.: Hiding secret data in images via predictive coding. Pattern Recognition 38, 691–705 (2005)
13. Zhang, X., Wang, S.: Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Processing Letters 12, 67–70 (2005)
14. Barni, M., Bartolini, F., Cappellini, V.: A DCT-domain System for Robust Image Watermarking. Signal Processing (Special Issue on Watermarking) 66(3), 357–372 (1998)
15. Hsu, C.T., Wu, J.L.: DCT-Based Watermarking for Video. IEEE Transactions on Consumer Electronics 44(1), 206–215 (1998)
16. Langelaar, G.C., Lagendijk, R.L.: Optimal Differential Energy Watermarking of DCT Encoded Images and Video. IEEE Transactions on Image Processing 10(1), 148–158 (2001)
17. O'Ruanaidh, J., Pun, T.: Rotation, Scale and Translation Invariant Digital Image Watermarking. In: Proceedings of IEEE Int. Conf. Image Processing., vol. 1, pp. 536–538 (1997)
18. Voloshynovskiy, S., Deguillaume, F., Pereira, S., Pun, T.: Optimal Adaptive Diversity Watermarking with Channel State Estimation. In: Proceedings of SPIE: Security and Watermarking of Multimedia Contents III, vol. 4314(74) (2001)
19. Zeki, A.M., Manaf, A.A.: A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit). In: Akram, M. (ed.) ICACEM 2009 - International Conference on Applied Computing and Engineering Mathematics. WCSET 2009. World Congress on Science, Engineering and Technology, Penang. Malaysia, February 25-27 (2009)
20. Niu, X.: A Survey of Digital Vector Map Watermarking. International Journal of Innovative Computing, Information and Control 2(6), 1301–1316 (2006)
21. Venkatraman, S., Abraham, A., Paprzycki, M.: Significance of Steganography on Data Security. In: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004), IEEE Computer Society Press, Los Alamitos (2004)
22. Hsieh, C.T., Lu, Y.L., Luo, C.P., Kuo, F.J.: A Study of Enhancing the Robustness of Watermark. In: ISMSE Conference, pp. 325–327 (2000)
23. Ohbuchi, R., Ueda, H., Endoh, S.: Robust Watermarking of Vector Digital Maps. In: Proceedings of the IEEE International Conference on Multimedia and Expo 2002 (ICME 2002), Lausanne, Switzerland, August 26-29 (2002)