http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (4): 841-848, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.841.848

ISB Watermarking Embedding: A Block Based Model

[1]Akram M. Zeki and [2]Azizah A. Manaf
[1]Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University of Malaysia, Malaysia
[2]Advanced Informatics School (AIS), University of Technology Malaysia, Malaysia

Abstract: Many watermarking methods have been developed with different methodological complexity levels. Each of these methods tries to reduce exposure in different attack. In this study, the ISB watermarking method was implemented based on average of block of pixels together in order to improve the watermarking method to be more resistant against attacks than a single pixel. The results show that the quality of the images is suitable for the application of the proposed method, based on any size of block. In additional to that the robustness has been improved by increasing the size of the block for all the attacks, including the geometric transform attacks, although they were not improved when the method was applied based on only one pixel.

Key words: Watermarking, robustness, LSB, ISB, block based model

INTRODUCTION

The watermark is hidden in the host data, in such a way that it is inseparable from the data and so that it is resistant to many operations which do not degrade the host document. Thus, by means of watermarking, the work is still accessible but permanently marked (Lu, 2005). Watermarks added to digital content serve a variety of purposes. The following list details some purposes of digital watermarking (Kutter and Hartung, 2000; Seitz, 2005; Qureshi and Tao, 2006). Fingerprinting, Data authentication, Indexing, Data Hiding, Content labelling, Usage Control, Owner Identification, Copyright protection, Copy protection, Broadcast monitoring, Medical applications, Unfortunately.

There are two types of watermarking methods (spatial domain and transform domain), depending on the domain of working. The later method is the subject of the current research. The advantages of using this technique are being very simple, fast and efficient and it provides a high capacity and the watermarked image quality could be easily controlled (Wu and Hwang, 2007). In addition to these, the technique could easily be applied to any image, regardless of the subsequent processing (Wu, 2001). On the other hand, the spatial domain techniques have some disadvantages. One of them is that it is not robust against attacks (Li and Yang, 2003; Venkatraman *et al.*, 2004). The aim of this study is to enhance the watermarking method to be applied based on the blocks of few pixels instead of one pixel only.

PREVIOUS METHODS

Maniccam and Bourbakis (2004) proposed an information hiding scheme, based on the fragile watermarking scheme for the greyscale image. In their work, the image was divided into overlapping blocks of size 3×3 pixels. The centre of each block was the embedded pixel for each block, as shown in Fig. 1. The major concept of their scheme was to define the complex regions of the host image and embed the secret data into these complex regions; the number of embedded bits, (supposed to be 0, 1, 2, 3, or 4) would be decided for every embedded pixel. This decision was made according to the variation σ of the neighbouring eight pixels of the embedded pixel. Let p be the current embedded pixel in an image and pi be the ith neighbouring pixel of p. The variation σ of p is computed by Eq. 1.

$$\sigma = \sum_{i=1}^{8} (p_i - p_{(i+1) \bmod 8})^2 \quad (1)$$

Here, the thresholds are set as t1, t2, t3 and t4. The number of the embedded bits would be 0, 1, 2, 3, or 4 if $0 \le \sigma \le t1$, $t1 \le \sigma \le t2$, $t2 \le \sigma \le t3$, $t3 \le \sigma \le t4$, or $t4 \le \sigma \le 255$, respectively. Finally, the complexity matrix, which represents the number of embedded bits for every embedded pixel, would be obtained.

An extended authentication scheme was proposed by Chang *et al.* (2006) in which the rightful ownership of an image could be confirmed and the forged part of the

Corresponding Author: Akram M. Zekiand, Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University of Malaysia, Malaysia

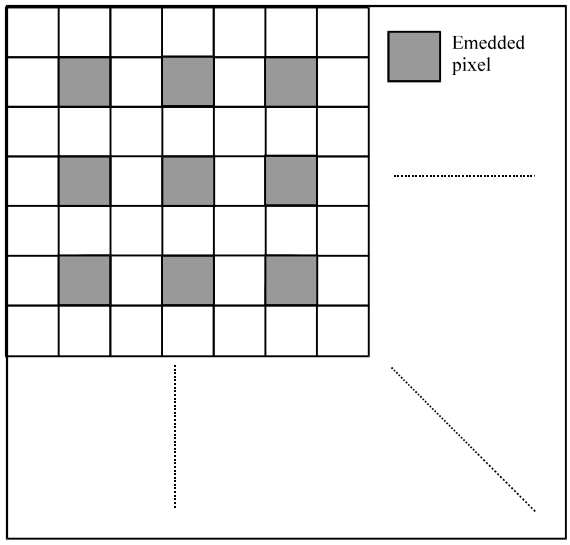

Fig. 1: The embedded pixel of an image (Maniccam and Bourbakis, 2004)

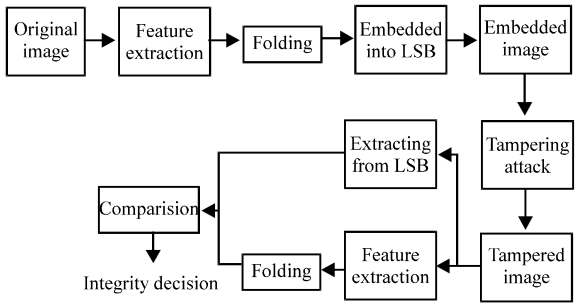

Fig. 2: The proposed image authentication scheme (Chang *et al*., 2006)

image could be detected. The diagram of this scheme is shown in Fig. 2. The feature extraction method and the authentication procedure are given in the subsequent sub-sections.

Yin *et al.* (2002) proposed an embedded annotation data, museum copyright logos and fragile watermarks simultaneously within an archive image. Annotation data were embedded within eight surrounding pixels of each 3×3 image block using the LSB replacement method. The multiple copies of annotation were also embedded. Each copy of the annotation was separated by boundary line signals, which were embedded together with the fragile watermark. The annotation data within the cropped images might still be extracted if any two consecutive vertical and horizontal boundary lines (which embraced a square area) could be found. A museum copyright logo was also embedded to prove the ownership of the archive image. Finally, a fragile watermark, based on the human visual system, was embedded in the central pixels of 3×3 blocks imperceptibly. Any alteration to the watermarked image could be detected and located with a high probability. A visual inspection tool could also be provided if an image had already been tampered.

Al-Jaber and Aloqily (2003) introduced a new algorithm which made use of the LSB method to embed the information within the inhomogeneous areas of the cover image. In this algorithm, an error correction code is used to increase the probability of retrieving the message and to enable the receiver to detect any alterations in the cover Media. In this case, the receiver informs the sender about such alterations. This model makes use of the HVS properties and embeds the message in the most important areas of the image. Experimental results showed that this method is efficient and effective to be used in addition to the finding which revealed that it produces high quality images.

Another study for watermarking of coloured images (such as cartoon images, line-draw images, binary images, maps and the like) was proposed by Pan *et al*. (2002). The main idea of this method was to use the prioritized sub-blocks by pattern matching in selecting the pixels with the least visual quality reduction of embedding. Based on this a sub-block with size 3×3 was employed to evaluate the embeddable priority of its central pixel by examining its eight neighbours. Each sub-block was associated with a rank, indicating the effect on its visibility by assuming the change of the central pixel. The higher rank implies that the alteration of the central pixel reduces less visual quality and it should have a higher priority for embedding. A good performance was revealed by the experimental results.

In the scheme proposed by Kailasanathan (2003) the polarity of the central pixel of an image block was determined by calculating the difference between the centre pixel of the image block and the mean of the image block pixels. A new fragile watermarking scheme, which embeds the marks on the central pixels of the image blocks based on the polarity of the pixels, had also been proposed. The security level of the scheme and the possible extension to multiple watermarking schemes were also investigated.

A robust spatial domain technique has been presented by Mohammad and Asad (2006) the method was based on Cox *et al.* (2001). A bit of binary pixel value (0 or 1) was embedded in a block of the host image. Before insertion, the host image was decomposed into N×N blocks. Depending on the contrast of a block, the pixels in the block were adaptively modified to maximize the robustness and guarantee invisibility. The position or

block for embedding was selected based on the pseudo-random number generator, using a seed value k. Let g_{max}, g_{min} and g_{mean} represent the maximal, minimal and average intensities of the block, respectively, as correspondingly stated in Eq. 3, 4 and 5:

$$g_{max} = \max (b_{ij}, 0 \le i, j < N) \quad (2)$$

$$g_{min} = \min (b_{ij}, 0 \le i, j < N) \quad (3)$$

$$g_{mean} = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} bij \quad (4)$$

where, b_{ij} represents the intensity of the $(i, j)^{th}$ pixel in the block. Assume that the embedded pixel value b_w is 0 or 1. The embedding process modifies the intensities of the pixels in the block according to the rules stated in Eq. 5.

$$g' = \begin{cases} g_{max} \text{ if } b_w = 1 \text{ and } g > g_{mean} \\ g + \delta \text{ if } b_w = 1 \text{ and } g \le g_{mean} \\ g_{min} \text{ if } b_w = 0 \text{ and } g < g_{mean} \\ g + \delta \text{ if } b_w = 0 \text{ and } g \ge g_{mean} \end{cases} \quad (5)$$

where, g' is the new pixel (watermarked pixel) after modifying intensity and δ is a small value used to tune the intensities. The embedding of the watermark depends on the content of each block. If the block is of higher contrast, the intensities of the pixels will be greatly modified. Otherwise, the intensities are tuned slightly. Thus, the proposed algorithm could adaptively modify the content of a block. The extraction of a watermark must make reference to the original host image. For each selected position, compute the sum of pixel intensities, S_o and S_w of the original and watermarked blocks. If $S_w > S_0$, the embedded bit is 1; meanwhile, if the $S_w = S_0$, the embedded bit is 0.

Kao and Hwang (2005) used a new method, developed using the block greyscale pixels value contrastive relation, which might not be destroyed even after lossy compression and decompression processes. The embedding steps were started using a seed *S* to find the location of one 3×3 block in the cover image. Then, the average of all pixels was calculated in the block Ave_{block} and the selected pixel value E was found (at the middle of the block). After that, a threshold value t was decided (for example t = 8). According to the value of each bit in hiding data, some changes would be done to the selected pixel value E in the cover image and their neighbouring eight pixels grey-level, using the following steps: If the secret bit is 0, (when E- $Ave_{block} \ge t$), keep all the values; otherwise, simultaneously alter selected pixel value and all its neighbouring eight pixel values by the same difference until E-$Ave_{block} \ge t$. If the secret bit is = 1 (when E - $Ave_{block} \le -t$), keep all the values; otherwise, simultaneously alter the selected pixel value and all its neighbouring eight pixel values by the same difference until E-$Ave_{block} \le -t$. If the receivers want to extract the hidden data, they will use the seed S to find the location of the hiding block. Then, the average of all the pixels in the block Ave_{block} can be calculated and the selected pixel with value E can be found. If the difference of E and Ave_{block} is bigger than 0, the extraction data is 0, or 1 otherwise.

Proposed scheme: In this study, the ISB watermarking method (Zeki and Manaf, 2009) will be tested and implemented based on average of block of 3, 5, 7 and 9 pixels together. The ranges of the each bit-planes have been found first, the length of the range L is 2^{k-1}, k is the number of each bit-plane. 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. 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. The bias value is the distance from the position of the watermarked pixel to the edge of the range.

A further contribution of this study is finding the best pixel value (threshold value) between the middle and the edge of the ranges, which survive against the different types of attacks and at the same time keeping the minimum image distortion. By testing all the possible positions of pixel between the edge and the middle of the range and by considering the acceptable image quality if the peak signal to noise ratio PSNR is greater than 30 db, the best normalized cross correlation was found to be in the 4th bit-plane, when the bias value was 6 (Zeki and Manaf, 2009).

Watermark embedding in the blocks of pixels: In this section, robustness is improved by watermark embedding based on the average of pixels values. One bit in a block of pixels should be embedded instead of embedding in only one pixel. A block should contain an odd number of pixels, so that the majority of bits can be evaluated without ambiguity, since in case the number of bits is even an equal number of ones and zeros may occur. The size of the block to be tested here contains three pixels, five pixels, seven pixels and nine pixels, as shown in Fig. 3 . If the size of the block increases, the capacity of embedding will also be decreased.

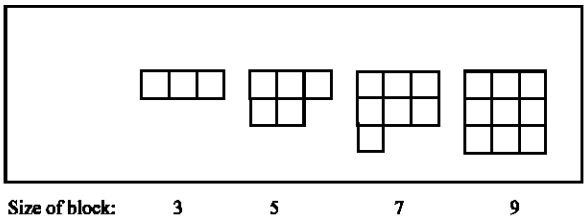

Fig. 3: Different sizes of blocks used in this study

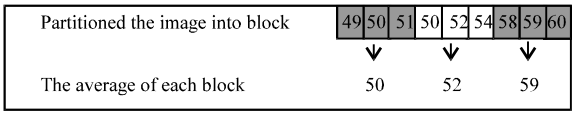

Fig. 4: Finding the average of each block

For every block, the average of the pixels is measured, as shown in Eq. 6 below. The ISB method is applied to the average. In other words, no direct embedding is done to the pixels, but the average of pixels values is shifted according to the ISB method (Zeki and Manaf, 2009).

$$\bar{A} = \frac{\sum_{i=1}^{n} Pi}{n} \quad (6)$$

Assume that the average of the pixels in a block is $\bar{A}$, after applying the ISB method to $\bar{A}$ the new value $\bar{A}'$ may be bigger or smaller, according to the method. Assume that $\bar{D}$ is the difference between $\bar{A}$ and $\bar{A}'$, (i.e. $\bar{D} = \bar{A} - \bar{A}'$), which may be of positive or negative values. The new pixels in the block are shifted by $\bar{D}$ (i.e. $P_i' = P_i - \bar{D}$); notice that the new pixel P_i' decreases if $\bar{D}$ is positive (in the other word $\bar{A}'$ is less than $\bar{A}$), while P_i' is found to increase if $\bar{D}$ is negative (in other words, $\bar{A}'$ is greater than $\bar{A}$).

For example, if the host image has been partitioned into blocks with size of 3 pixels, the average of each block is then calculated and the embedding is done in each bit within that block, as shown in Fig. 4.

For example, if the embedding process is applied into the 4th bit-plane at bias value equal to 6 as found (Zeki and Manaf, 2009) by inserting bit of value 1 into the average of pixels value in block 50, the watermarked value after embedding becomes 54 (the minimum of the same range+bias value); notice that the value 50 is increased by +4; all the pixels in the block (49, 50 and 51) are therefore increased by the same value and they become 53, 54 and 55, as shown in Fig. 5.

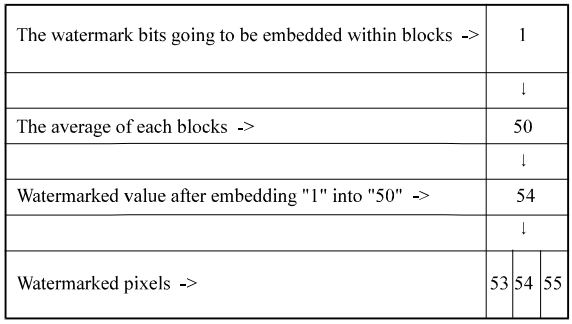

Fig. 5: Embedding based on the average of pixels values

During the extraction, the average of pixels values is measured (53+54+55)/3 = 54 and the direct extracted bit from the forth bit-plane is found to reconstruct the watermarked object.

The idea behind applying the ISB method using blocks is due to the fact that blocks are more resistant against attacks than a single pixel. For instance, if the pixel is modified by H and moved to another period, the extracting result is therefore wrong. In case of blocks, individual modification of pixels by H (up or down) may not affect the extraction of the whole block. However, the total summation of the pixels needs to be modified by H×Number of pixels in block to give a total result in one direction (up or down) so that this will result in a failure in extraction. It is obvious that this is less probable than the case for a single pixel.

Notice that the new pixel P_i' may be more than 255 or less than 0 and in this case, every pixel with a value more than 255 is reduced to 255; while any pixel with a value less than 0 is increased to 0. Notice that after this adjustment, the new average is no longer the same after embedding $\bar{A}'$. To solve this problem, the other pixels in the block are changed, either by increasing or decreasing them to adjust the average of pixels values so that they are the same as that of $\bar{A}'$. Thus in this case, the pixels in the block will not increase or decrease by same value of $\bar{D}$.

IMPLEMENTATION AND EXPERIMENTAL RESULTS

In this study, three grey scale images (logos) contains 90×90 pixels as shown in Fig. 6 will be embedded within three host images containing 256×256 pixels as shown in Fig. 7.

The security of the system has been improved; the watermark object has been encrypted by using Random Pixel Manipulation Technique (Venkatraman *et al*., 2004)

Table 1: The NCC of embedding the watermark 1 in Host 1 within different size of blocks

Block size (in pixels)	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.931264	0.910986	0.919141	0.847613	0.932271	0.799517	0.809247
3	0.99739	0.975346	0.978342	0.99161	0.994686	0.82993	0.8554
5	1	0.991882	0.993771	0.999248	0.998363	0.84342	0.88312
7	1	1	1	0.999951	0.999883	0.86012	0.90127
9	1	1	1	1	1	0.883423	0.913684

Table 2: The NCC of embedding the watermark 1 in Host 2 within different size of blocks

Blocksize (in pixels)	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.917325	0.899574	0.911418	0.871249	0.886982	0.799517	0.809229
3	0.996764	0.978988	0.984445	0.991263	0.988596	0.82291	0.84528
5	1	0.996135	0.997091	1	0.998394	0.8501275	0.88934
7	1	0.998163	0.998317	0.999765	0.998852	0.877131	0.901244
9	1	0.999735	0.999741	1	1	0.8997599	0.924225

Table 3: The NCC of embedding the watermark 1 in Host 3 within different size of blocks

Block size (in pixels)	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	0.90519	0.863423	0.873039	0.855802	0.817691	0.799517	0.8093
3	0.998648	0.975808	0.981095	0.991663	0.97108	0.81321	0.85354
5	1	0.995461	0.996722	0.999442	0.994648	0.83112	0.905727
7	1	0.997487	0.998289	0.999569	0.998083	0.86021	0.93155
9	1	0.99806	0.998532	1	0.999604	0.895729	0.94037

Fig. 6: Grey scale logo with 90×90 pixels

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

The sizes of the block tested contained 3, 5, 7 and 9 pixels, as shown in Fig. 3. Here, the new average value should be taken after embedding the information within the 4th bit-plane and the bias value = 6 as found (Zeki and Manaf, 2009) as a threshold value. 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).

After applying different attacks, the new average was measured and the embedded bit was extracted from the 4th bit-plane. 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 NCC values were calculated for all the different sizes of the block, after embedding the watermark 1 in various hosts, as shown in Table 1-3.

Table 4: The NCC values after 9 embedding watermark 2 in different hosts using block of 3×3 pixels

Host	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	1	0.999491	1	1	1	0.899983	0.921481
2	1	0.999584	0.999644	1	1	0.88144	0.901167
3	1	0.998324	0.998906	1	0.999051	0.896124	0.910982

Table 5: The NCC values after 9 embedding watermark 3 in different hosts using block of 3×3 pixels

Host	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
1	1	0.998766	0.99927	1	1	0.895864	0.927078
2	1	0.999657	0.999947	1	1	0.888013	0.892073
3	1	0.998526	0.998735	1	0.999504	0.88921	0.89525

Table 6: The PSNR values using blocks of 3×3 for various watermarks in different hosts

Host	Host1	Host2	Host3
Watermark1	30.97664	30.22819	30.97848
Watermark2	29.90807	30.10636	30.08635
Watermark3	30.89151	30.10032	29.98435

In Table 1-3, the NCC values were found to improve by increasing the size of the block for all the attacks, including the geometric transform attacks (Rotation and Scaling), although they were not improved when the method was applied based on only one pixel.

To test the other watermark objects, watermark 2 and 3, were embedded in the big size of block, with nine pixels (3×3) of host images 1, 2 and 3; giving the best extracted ratio, the NCC values were also calculated for every embedding, as shown in Table 4 and 5.

The results show that the NCC values improved for all the attacks and became 1 or very close to 1 at block of 9 pixels for five attacks (JPEG, Blurring, Gaussian, Wiener and Speckle noise). Meanwhile, the NCC values are about 0.9 for Rotation and Scaling. For the above results, the PSNR was also measured for every embedding, based on the block of 9 pixels (3×3 pixels), as given in Table 6.

Fig. 7: Grey scale host image with 256×256 pixels

Table 6 shows that the quality of the images is suitable for the application of the proposed method based on any size of block. This is because the embedding in the 4th bit-plane with bias value = 6 is the threshold value which keeps the quality of the image. In other words, applying the proposed method, based on the pixels or blocks changes the values of the pixels but with some limitations and adjustments and this is important for quality.

RESULTS AND DISCUSSION

Robustness has been improved in this research by embedding the watermark based on the average of pixels values which had been tested in this study. Different size of blocks have been tested of 3, 5, 7 and 9 pixels; embedding watermark 1, 2 and 3, was done to all the host images in the 4th bit-plane with the bias value = 6.

The NCC values were also calculated for all the different sizes of the block, after embedding watermark 1 within all the host images, as shown in Fig. 8.

The Fig. 8 show that applying the proposed method, on the block with three pixels, is better than using only one pixel; the block with five pixels is better than the block with three pixels, the block with seven pixels is better than the block with only five pixels. Thus, the best NCC was for the biggest block size with nine pixels. This is because the effect of attacks is limited for the big size of blocks, so the average of the pixels in block is difficult to change after applying the attacks. From the above results, the block of 3 pixels might be enough for all the attacks, except Rotation and Scaling which might need a bigger size of block.

A comparative study: Carrying out a comparison among the different watermarking methods is not easy because

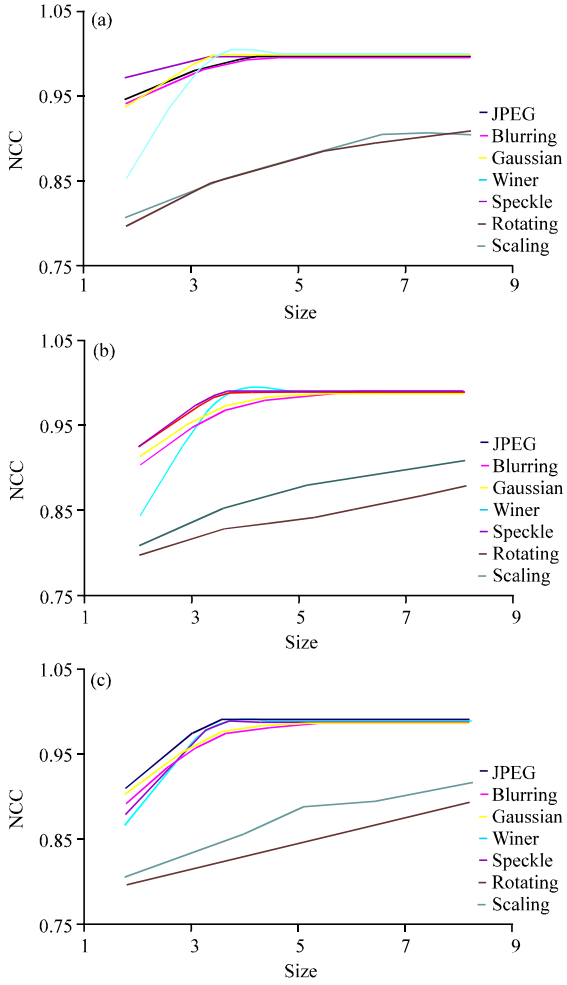

Fig. 8: The NCC values for the extracted logo (watermark 1) from the different host images, at the embedding within 4th bit-plane, at bias value = 6, (a) Host 1; (b) Host 2; (c) Host 3

Table 7: The NCC values for different attacks after embedding watermark 1, within Host 1 by the proposed method and by the other methods

Host	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
Proposed method	1	1	1	1	1	0.883423	0.913684
Kao and Hwang (2005)	0.9637	0.898313	0.981677	0.449417	0.880839	0.483094	0.621223
Mohammad and Asad (2006)	0.971465	0.988367	0.998167	0.95804	0.763987	0.774928	0.828392

Table 8: The NCC values for different attacks after embedding watermark 1, within Host 2 by the proposed method and by the other methods

Host	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
Proposed method	1	0.999735	0.999741	1	1	0.899759	0.924225
Kao and Hwang (2005)	0.959522	0.923708	0.991968	0.475682	0.825208	0.418821	0.667894
Mohammad and Asad (2006)	0.960575	0.963103	0.991661	0.932324	0.742347	0.784563	0.858676

Table 9: The NCC values for different attacks after embedding watermark 1, within Host 3 by the proposed method and by the other methods

Host	JPEG	Blurring	Gaussian	Wiener	Speckle	Rotation	Scaling
Proposed method	1	0.99806	0.998532	1	0.999604	0.895729	0.94037
Kao and Hwang (2005)	0.953702	0.872594	0.992328	0.536651	0.758269	0.497161	0.63486
Mohammad and Asad (2006)	0.978006	0.963368	0.991555	0.946726	0.723533	0.794033	0.772462

every method applies different techniques and models. In addition, these techniques can hide different capacities of embedded information. It is not right to compare a method with a low capacity with a method of high capacity, since less capacity may give a better watermarked image quality. In short, this comparison should be done on the basis that the methods to be compared should be of similar nature (e.g., both should be blind methods). The other difficulties are that different techniques use different host images and different watermarked objects which are embedded within the host images. Another difficulty is that the attacks tested were of different quality, when they were applied for each method.

The comparison carried out in this study was between the proposed and other methods, based on the average of pixels values. Two watermarking methods, based on spatial domain techniques, were chosen for this comparison, with the two methods embedded one bit within one block of 3×3 pixels. The two methods were proposed by Kao and Hwang (2005) and Mohammad and Asad (2006).

Watermark 1 was embedded within the different host images using the proposed and the other two methods, based on the average of pixels values; the results of comparison are shown in Table 7-9 for Hosts 1 to 3, respectively.

Based on the results presented, it is clear that the proposed method is better than the other methods selected for this comparison. In addition, it can also be noticed that the proposed method is working properly with all types of attacks (robustness against all attacks), while the other methods are not robust against all attacks (Kao and Hwang, 2005) and is not robust (fragile) against Rotation, Wiener and Scaling, while it is semi-fragile against Speckle and Blurring. This is supported by Mohammad and Asad (2006) who also found that the technique is semi-fragile against Speckle, Rotation and Scaling. The NCC for the above two methods could not reach 1 for all the attacks, although only one bit was embedded within a block with the size of 3×3 pixels.

CONCLUSION

Here, robustness is improved by watermark embedding based on the average of block of 3, 5, 7 and 9 pixels together. In this study, three grey scale images have been embedded within three host images. One bit in a block of pixels should be embedded instead of embedding in only one pixel. The results show that using ISB method for embedding the watermark within the block of three pixels is better than using only one pixel. the block with five pixels is better than the block with three pixels, the block with seven pixels is better than the block with only five pixels. Thus, the best NCC was for the biggest block size with nine pixels. This is because the effect of attacks is limited for the big size of blocks, so the average of the pixels in block is difficult to change after applying the attacks.

REFERENCES

Al-Jaber, A. and I. Aloqily, 2003. High quality steganography model with attacks detection. Inform. Technol. J., 2: 116-127.

Chang, C.C., Y.S. Hu and T.C. Lu, 2006. A watermarking-based image ownership and tampering authentication scheme. P attern Recognition Lett., 27: 439-446.

Cox, I.J., M.L. Miller and J.A. Bloom, 2001. Digital Watermarking. 1st Edn., Morgan Kaufman, San Francisco.

Kailasanathan, C., 2003. Fragile watermark based on polarity of pixel points. Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis, Sept. 18-20, USA., pp: 860-865.

Kao, C.H. and R.J. Hwang, 2005. Information hiding in lossy compression gray scale image. Tamkang J. Sci. Eng., 8: 99-108.

Kutter, M. and F. Hartung, 2000. Introduction to Watermarking Techniques. In: Information Hidingtechniques for Steganography and Digital Watermarking, Katzenbeisser, S. and F.A.P. Petitcolas (Eds.). Artech House, Boston.

Li, C.T. and F.M. Yang, 2003. One-dimensional neighbourhood forming strategy for fragile watermarking. J. Electr. Image., 12: 284-291.

Lu, C.S., 2005. Multimedia Security, Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, Hershey, PA. USA., pp: 255.

Maniccam, S.S. and N. Bourbakis, 2004. Lossless compression and information hiding in images. Pattern Recognition, 37: 475-486.

Mohammad, A.M.F. and N.M. Asad, 2006. An optimization approach for selecting blocks of embedding process in robust watermarking system. J. Comput. Sci., 2: 114-117.

Pan, G., Z. Wu and Y. Pan, 2002. A data hiding method for few-color images. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, May 13-17, Orlando, Florida, pp: 3469-3472.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Seitz, J., 2005. Digital Watermarking for Digital Media. Idea Group Inc., Hershey, PA., USA.

Venkatraman, S., A. Abraham and M. Paprzycki, 2004. Significance of steganography on data security. Proceedings of the International Conference on Information Technology: Coding and Computing, April 5-7, Las Vegas, Nevada, pp: 347-351.

Wu, C.F., 2001. The research of improving the image quality of digital watermarking technique and its applications. Ph.D. Thesis, National Sun Yat-Sen University, Kaohsiung, Taiwan.

Wu, N.I. and M.S. Hwang, 2007. Data hiding: Current status and key issues. Int. J. Network Sec., 4: 1-9.

Yin, C.Y., D.C. Wu and W.H. Tsai, 2002. New data hiding methods for copyright protection, annotation and authentication of BMP archive images in digital libraries and museums. Proceedings of the 1st Workshop on Digital Archives Technologies, (WDAT'02), Taipei, Taiwan, pp: 168-183.

Zeki, M.A. and A.A. Manaf, 2009. A novel digital watermarking technique based on ISB (intermediate significant bit). Proceedings of the International Conference on Applied Computing and Engineering Mathematics, Feb. 25-27, Penang, Malaysia, pp: 989-996.