International Journal of Research and Reviews in Information Sciences (IJRRIS)
Vol. 2, No. 2, June 2012, ISSN: 2046-6439

www.sciacademypublisher.com/journals/index.php/IJRRIS

Multi Image Watermarking Scheme Based on Intensity Analysis

Hamza A. Ali and Sama'a A.K. Khamis

Computer Engineering Department, College of Engineering, University of Basrah, Basrah, Iraq

Email: alsewadi@hotmail.com, sama@yahoo.com

Abstract – A new robust multi image digital watermarking scheme is proposed based on the frequency analysis of pixels intensity in the carrier images. The color image is divided into its three basic color channels (Red, Green, and Blue). Each channel is treated as a host image and broken into segments of equal sizes. A histogram is drawn for each segment in these channels formulating the number of pixels against intensity. The adopted key for embedding was by obtaining and modifying the intensity of pixels with the highest histogram in the segment. Each channel embeds one modulating image resulting into multi-watermarked image. The channels are then re-integrated back to form the watermarked image. Hence, watermark bits values are distributed irregularly all over the carrier image making it extremely difficult to be noticed or extracted unless the key is known. The proposed scheme has given peak signal to noise ratio (PSNR) reaching over 60 dB for rotation and resizing problems with cross correlation of about 0.999. Moreover, the scheme also exhibited high PSNR and good cross correlation in the presence of various types of noise and disturbances. Therefore, this method has proved to be very secure and robust against different types of noise, resizing and rotation.

Keywords – Watermarking, Histogram, Ownership proof, Steganography, Multi-watermarking

1. Introduction

Watermarking technology was developed along with protection of copyright. It is widely used for copyright protection of images, audios and videos. We can affirm the integrity and reliability of information audio production is one of the important digital multimedia factors. Along with the rapid growth of internet, the transmission of audiovisual media becomes easier which has lead to the copyright protection problem. For this reason digital watermarking has acquired wide research and application. Since Human Auditory System (HAS) is more sensitive than Human Visual System (HVS) embedding mark into the audio signal is very difficult. Recently, research on digital watermarking is mainly based on embedding mark into static images, however only a few institution has been working on audio watermarking [1-2]. Digital watermarking is the process of embedding or hiding the digital information called watermark into the protected multimedia product such as an image, audio or video. The embedded data can be detected later or extracted from the multimedia for identifying the copyright ownership. Over the past few years digital watermarking has become popular due to its significance in content authentication and legal ownership for digital multimedia data. Digital watermark is a sequence of information containing the owner's copyright for the multimedia data. It is inserted visibly or invisibly into another image so that it can be extracted later as an evidence of authentic owner [3,4,5]. Usage of digital image watermarking technique [6] has grown significantly to protect the copyright ownership of digital multimedia data as it is very much prone to unlawful and unauthorized replication, reproduction and manipulation. The watermark may be a logo, label or a random sequence. A typical good watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and spectral domain. Incorporation of the watermark in the image could be performed in various ways [7-9].

2. Watermarking Requirements

There are many characteristics that watermarking holds, some of them are as follows:

- Visibility: an embedded watermark can be either visible or not visible according to the requirement.
- Robustness: piracy attack or image processing should not affect the embedded watermark. Robustness might also incorporate a great degree of fragility to attacks, i.e. multimedia cover object is totally destroyed if it detects any tapering [8].
- Readability: A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.
- Integrity: No loss of original multimedia carrier.
- Accessibility: both types of watermarking must permit for accessibility. Visible type allows information handling for any interested entity to call attention to the copy/reproduction rights, while the invisible type necessitates extra authorization information in order to access the watermark.
- Security: Security: watermarking accounts for the protection of ownership against forgery and unlawful threats. Invisible watermark should be secret and must be undetectable by an unauthorized user in general.

It has been noted that if strong stress is been put on robustness, then invisibility may be weak, however if one puts emphasis on invisibility, then robustness is weak. Therefore, developing invisible and robust watermark is considered as very important issue [9].

3. The Proposed Watermarking Scheme

Intensity histogram is a simple statistical feature of an image that has been commonly used in image processing. Intensity histogram is a distribution of the gray level values of all pixels within the image. Each histogram bin represents number of pixels for certain intensity value. Often 256 levels histogram is used, where each level correspond to one bin [9, 10]. Detailed definition of histogram and its implementation on gray color image is given in [11].

This paper presents an algorithm that utilizes the intensity histogram technique for embedding watermarks in color image. The algorithm accepts three images (or logos) to be embedded in one color image carrier. It splits the carrier image into its three basic components (red, green and blue), then embeds one watermark evenly in each component into all parts of the image according to the frequency analysis of maximum amplitude occurrence. The resulting three watermarked images are then recombined together to get the final modulated image, as shown in figure 1. The original logos can be recovered in a reverse process when required at the time of any copyright conflict.

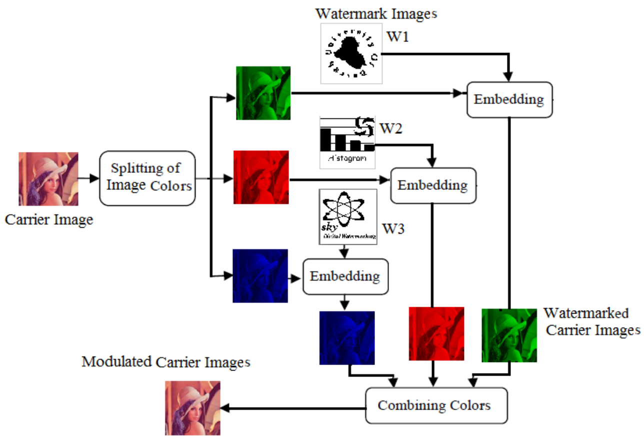

Figure 1. Block diagram of the multi-watermarking modulation process.

The whole process is accomplished in two main activities, namely modulation and demodulation and described in details in the following.

3.1. Modulation or embedding process

- Step 1: Read both of the carrier image, 1024x1024 pixels, and the three modulating images each one of size 128x128 pixels.
- Step 2: Split the carrier image into three channels according to the three original colors (Red, Green, and Blue) as shown in figure 2.
- Step 3: Convert the modulating images is converted into black and white color space.

Now it is possible to map each regional segment from the carrier image into one bit of modulating image as in the following steps.

- Step 4: Segment each color channel of the carrier image into blocks of equal dimensions according to the process adopted in [11]. Calculate and draw the histogram for the number of pixels versus intensity for each block, then select the pixel with maximum frequency of occurrence (i.e. the intensity that has the maximum value of pixels). The embedding process is performed depending on the bit value of the watermark binary image, if it is 1, the intensity is increased by 1 but if it is 0 then the intensity is decreased by 1. Then resemble these new blocks into new image.
- Step 5: The above step is repeated for the three watermarks involved to be embedded into the three color channels.
- Step 6: Integrate the resulted images of the three channels of steps 4&5 into single modulated carrier image. Save this modulated image and the resized modulating image.

The modulation process can be summarized in the flow diagram shown in figure 2.

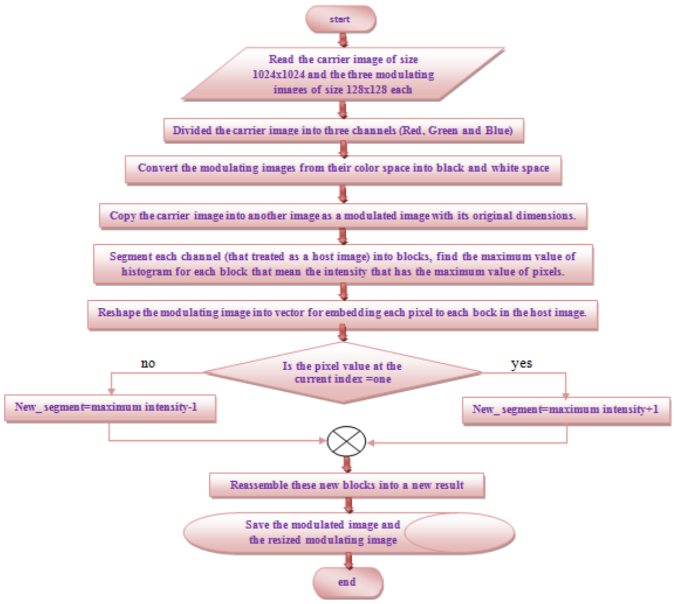

Figure 2. Flow diagram of the Modulation process.

3.2. Demodulation or extraction Process

For the ownership proof, the proposed technique requires both the original carrier image and the modulated image. To extract the watermarks, the steps below are followed.

- Step 1: Read the original image (carrier image) and the modulated image.
- Step 2: Divided the carrier image into three channels and treated each channel as a single image. Each channel is then segmented into equal blocks and finds the intensity that has the maximum value of pixels in histogram for each block.
- Step 3: Divided the modulated image into three channels and treated each channel as a single image then each channel is segmented into blocks and find the intensity for each block after embedding .
- Step 4: Apply equation 1 in order to determine pixel values of the watermark.

$$\text{Pixel\_value} = (-1/4*D + 1/2) \tag{1}$$

where D is the difference between the maximum values for the two histogram.

- Step 5: Save the extracted watermark image.

The demodulation process can be summarized in the flow diagram shown in figure 3.

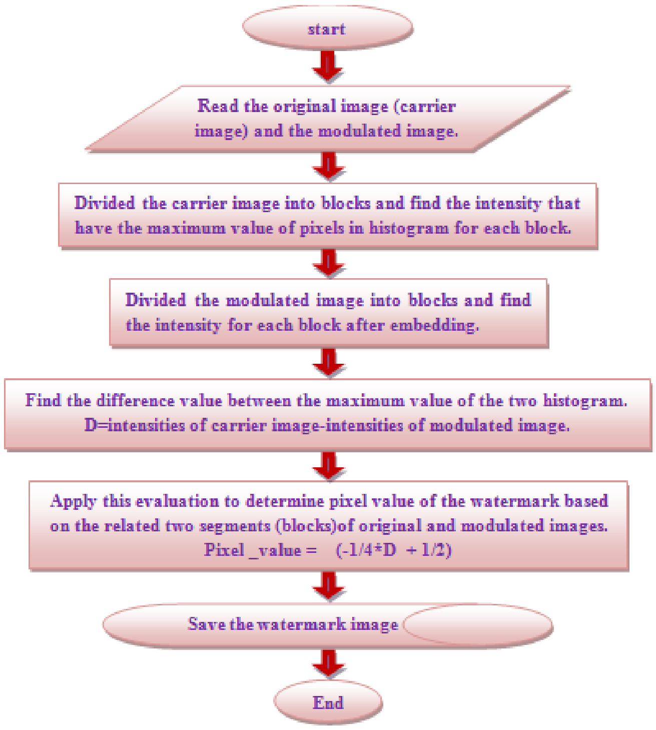

Figure 3. Flow diagram of the Demodulation process.

4. Implementation and Results

We used original image of size 1024x1024 color image, and the three modulating images of size 128x128 each. As there are 16384 bit (pixel value) in the modulating image (binary image), the carrier color image (original) is divided into three channels first as shown in figure 1. Each channel is then segmented into 16384 blocks, each block of 8x8 sizes.

The modulating algorithm is executed to embed three different watermarks in three basic color components of the carrier images. The experiments were performed on four carrier images, namely the University of Basrah symbolic domes, Lena photo, Great Wall of China and Taj-Mahal. Figure 4 shows illustrations for the carrier images, the three modulating images and the modulated image for the considered cases.

Moreover, for the extraction (demodulation) algorithm, the same original carrier images and the modulated images of the previous process are used to extract the three modulating images as shown in figure 5.

To examine the performance of the proposed watermarking technique, the normalized cross correlation is evaluated for the three watermarks where the value of the mean square error MSE have been obtained and the peak signal to noise ratio PSNR was calculated using equations 2 and 3.

$$\text{MSE}=\frac{1}{MN}\sum_{i=1}^{m}\sum_{j=1}^{n}(fc(i,j)-fm(i,j))\,2 \qquad (2)$$

And

$$\text{PSNR} = 10\,log_{10}\left(\frac{255^2}{\frac{MSE(R)+MSE(G)+MSE(B)}{3}}\right) \quad . \quad . \quad . \quad . \quad (3)$$

where $fc(i,j), fm(i,j)$ represents the pixel values of original carrier image and the modulated image, respectively. The parameters (m, n) specify row and column size of images respectively.

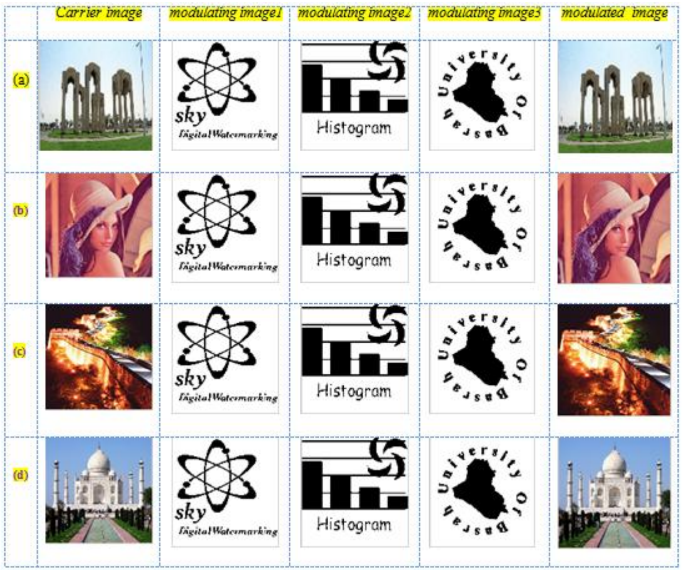

Figure 4. Embedding Process Result for (a) University of Basrah Symbolic domes. (b) Lena image, (c) Great Wall of China, and (d) Taj-Mahal.

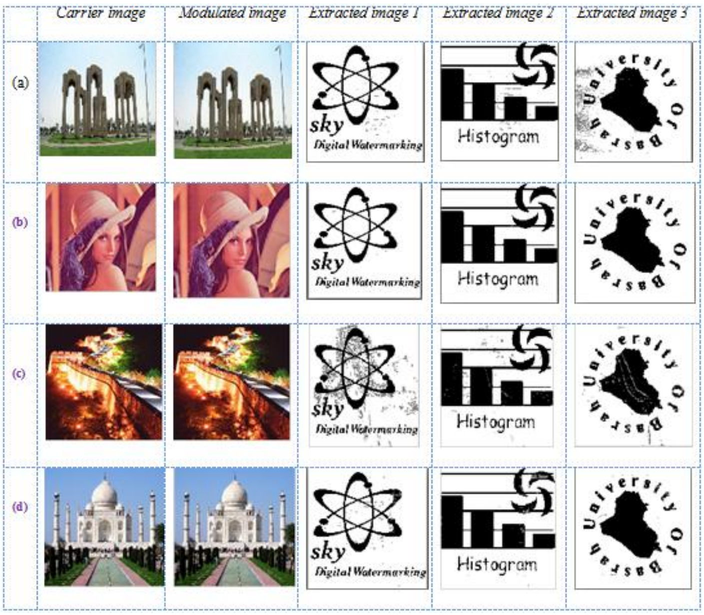

Figure 5. Extraction Process Result for (a) University of Basrah Symbol domes. (b) Lena image, (c) Great Wall of China, and (d) Taj Mahal.

The Normalized Cross Correlation NCC is calculated using equation 4.

$$\text{NCC} = \frac{\sum_{i,j}(WE_{i,j}-A)(WO_{i,j}-B)}{\sqrt{\sum_{i,j}(WE_{i,j}-A)^2\ \sum_{i,j}(WO_{i,j}-B)^2}} \quad . \quad . \quad . \quad . \quad (4)$$

where *(WE)* and *(WO)* are the extracted and original watermarks, while A and B are their pixel mean values, respectively. The subscript (i, j) denotes the index of an individual pixel of the corresponding image. The summations are over all the image pixels.

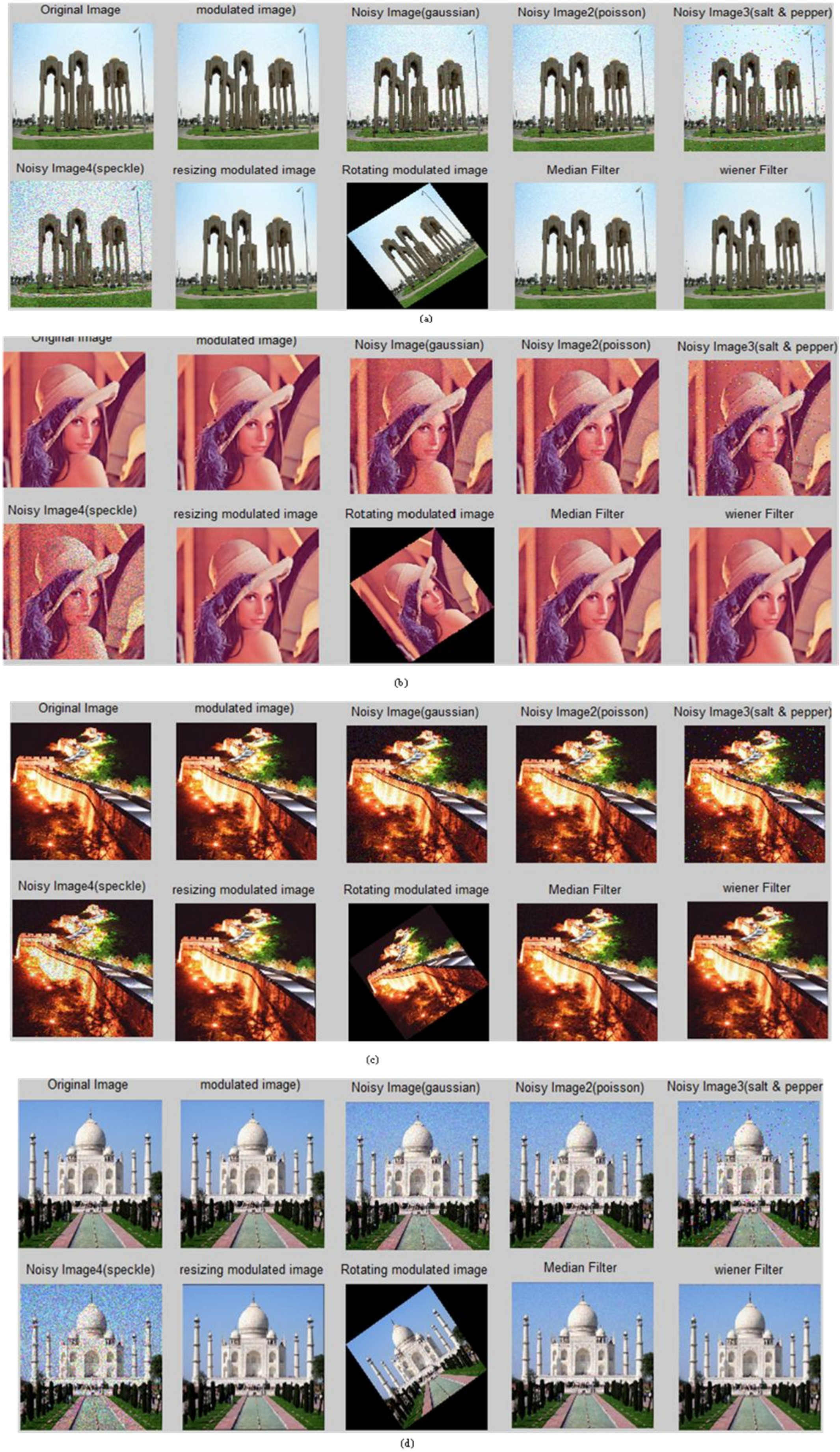

Fig 8. Attacks on images of (a) University of Basrah symbolic domes, (b) Lena, (c) Great Wall of China, and (d) Taj-Mahal.

These tests were performed for three watermarks embedded in the four carrier images considered in this paper, i.e. University of Basrah symbolic domes, Lena photo, Great Wall of China and Taj-Mahal. These tests are carried out to demonstrate the algorithm strength and weakness under various attacks. These attacks included the addition of various noises, image resizing, image rotation and filtering.

Addition of four types of noise is considered here; namely Gaussian noise, Poisson noise, salt & pepper noise, and Multiplicative noise. Besides, some image disturbances are also considered such as image resizing, rotation and filtering. All obtained results are summarized in tables 1-4. Moreover, figure 6 gives illustrations for the inclusion of noise, resizing, rotation and filtering in the considered modulated images.

Table 1. Correlation and PSNR for Basrah University Symbolic Domes

Types of attacks	Normalize cross Correlation			PSNR(db)
	Extracted Watermark1	Extracted Watermark2	Extracted Watermark3	
No attack	0.9997	0.9999	0.9847	60.2910
Gaussian noise(0.003)	0.8348	0.9322	0.7520	25.7896
Poisson noise	0.8449	0.9350	0.7779	26.7798
salt and pepper noise (0.02)	0.0348	0.9995	0.9834	21.4567
Multiplicative noise (0.04)	0.8358	0.9144	0.7330	18.7779
Image resizing [256 256]	0.9997	0.9999	0.9847	64.2157
Image rotating 35°	0.7959	0.7334	0.9068	67.2346
median filtering [3 3]	0.8345	0.9240	0.7524	32.3948
Wiener2 low pass filters[5 5]	0.8024	0.8947	0.6968	33.4626

Table 2. Correlation and PSNR for Lena image

Types of attacks	Normalize cross Correlation			PSNR(db)
	Extracted Watermark1	Extracted Watermark2	Extracted Watermark3	
No attack	1.0000	1.0000	1.0000	60.2089
Gaussian noise(0.003)	0.8498	0.9349	0.7783	25.3287
Poisson noise	0.8272	0.9039	0.8327	27.1664
salt and pepper noise (0.02)	0.9985	0.9996	0.9992	22.2329
Multiplicative noise (0.04)	0.8312	0.9140	0.7592	19.7191
Image resizing [256 256]	1	1	1	63.1987
Image rotating 35°	0.6548	0.8259	0.4992	65.4225
median filtering [3 3]	0.8319	0.9032	0.7523	32.8076
Wiener2 low pass filters[5 5]	0.8322	0.9154	0.7516	36.0248

Table 3. Correlation and PSNR for Great Wall of China image

Types of attacks	Normalize cross Correlation			PSNR(db)
	Extracted Watermark1	Extracted Watermark2	Extracted Watermark3	
No attack	0.9988	0.9995	0.9997	60.4115
Gaussian noise(0.003)	0.8623	0.9134	0.2250	25.4938
Poisson noise	0.8675	0.9422	0.8532	26.7453
salt and pepper noise (0.02)	0.9969	0.9993	0.9991	21.8642
Multiplicative noise (0.04)	0.8651	0.9304	0.7884	18.8541
Image resizing [256 256]	0.9988	0.9995	0.9997	63.2675
Image rotating 35°	0.7049	0.7990	0.2959	65.4869
median filtering [3 3]	0.3154	0.9163	0.2094	31.6175
Wiener2 low pass filters[5 5]	0.8521	0.9239	0.7876	32.0347

Table 4. Correlation and PSNR Taj-Mahal imge

Types of attacks	Normalize cross Correlation			PSNR(db)
	Extracted Watermark1	Extracted Watermark2	Extracted Watermark3	
No attack	0.9858	0.9998	0.9993	60.2456
Gaussian noise(0.003)	0.8171	0.3088	0.3419	25.6555
Poisson noise	0.8668	0.9478	0.8249	29.3539
salt and pepper noise (0.02)	0.9840	0.9993	0.9983	21.3042
Multiplicative noise (0.04)	0.8562	0.9354	0.8164	22.1569
Image resizing [256 256]	0.9858	0.9998	0.9993	63.0140
Image rotating 35°	0.6548	0.8259	0.4992	65.6242
median filtering [3 3]	0.4398	0.1883	0.3847	31.7162
Wiener2 low pass filters[5 5]	0.8580	0.9162	0.7631	32.0193

The evaluated PSNR for watermarked image and the normalized cross correlation measurements for the three embedded images and listed in tables 1-4 are plotted and compared with each other in figures 7-10.

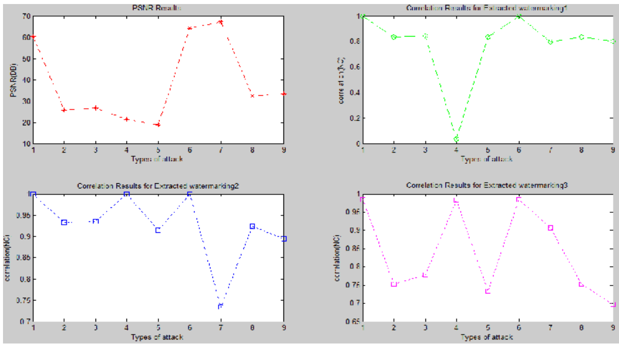

Figure 7. PSNR & NCC vs. attacks for university of Basrah symbolic domes.

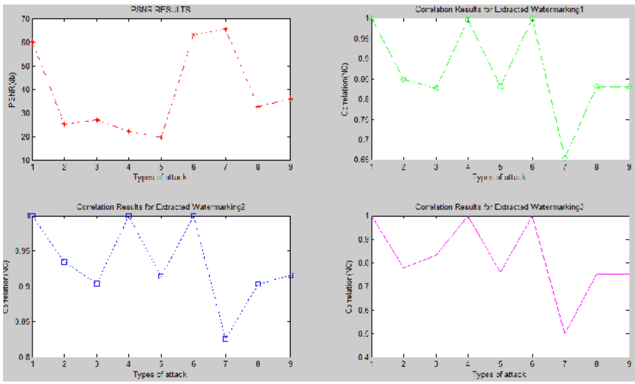

Figure 8. PSNR & NCC vs. attacks for Lena image.

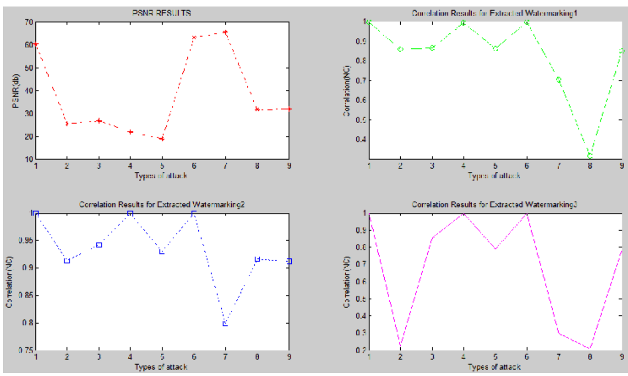

Figure 9. PSNR & NCC vs. attacks for Great Wall of China image.

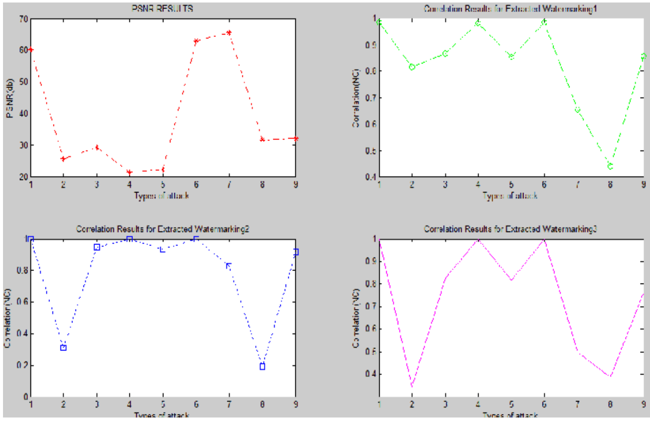

Figure 10. PSNR & NCC vs. attacks for Taj Mahal image.

5. Conclusions

A new efficient algorithm has been suggested for digital image watermarking that is based on the modification of selected maximum intensity pixels. It benefits from the histogram plot of the pixel values. Dividing the original image into equal size blocks and drawing the histogram for each block. The intensity that has the maximum value of pixels has been obtained. The selected values of intensity were used to embed the watermark into the original image, so one bit of watermark image is embedded into each block of original image. Tests have shown that the proposed method is very secure and robust against attacks.

Watermark image bits are embedded in all the blocks of the carrier image in an irregular manner. This adds difficulty to the system security.

Moreover, any of the three basic color components can be used for embedding watermark image allowed for multi-watermarking process. The algorithm implementation included embedding three logos in one carrier image.

References

[1] Bros A. and I. Pitas, “Image watermarking using DCT domain constraint”, IEEE Int. Conf. Image Processing (ICIP’96), Vol.3, pp. 231 – 234, 1996.

[2] Chang CC, Tsai CS, “A technique for computing watermarks from digital images”, Journal of Computing and Informatics, Vol. 24, No. 3, pp. 391 – 396, 2000.

[3] Hartung F. and M. Kutter, "Multimedia watermarking techniques”, Proceedings of the IEEE, vol. 87, pp. 1079-1107, 1999.

[4] Petitcolas F. A. P., R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey”, Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[5] Mintzer F., G. Braudaway, I. Center, and Y. Heights, “If one watermark is good, are better?”, Proceedings. IEEE International Conference on Acoustics, Speech, and Signal Processing, 1999. ICASSP’99, Vol.4, 1999.

[6] Daxing Zhang Zhigeng Pan Haihua Li , “A Contour-based Semi-fragile Image Watermarking Algorithm in DWT Domain”, Second International Workshop on Education Technology and Computer Science (ETCS), 2010 , Vol. 3, Pages: 228, May 2010.

[7] Bo Chen Hong Shen, “A New Robust-Fragile Double Image Watermarking Algorithm”, Third International Conference on Multimedia and Ubiquitous Engineering, 2009. MUE ’09, Pages: 153, November 2009.

[8] Cox I.J., M.L. Miller, J.M.G. Linnartz, T. Kalker, “A Review of Watermarking Principles and Practices”, Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, Marcel Dekker, Inc., PP 461-482, 1999.

[9] Rawat K.S. and D.S. Tomar, “Digital Watermarking Schemes for Authorization Against Copying or Piracy of Color Images”, Indian Journal of Computer Science and Engineering, Vol.1, PP 295-300, 2010.

[10] Huiyu Zhou, Jiahua Wu, and Jianguo Zhang , ”Handbook of Digital Image Processing”. Part 1, 2010.

[11] Hamza A. Ali and Samaa A.K. Khamis, ”Robust Digital Image Watermarking Technique Based on Histogram Analysis”, First National Scientific Conference for Computer Science and Technology, Basrah University, 7-8 March 2012.