World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 2, No. 5, 163-168, 2012

Robust Digital Image Watermarking Technique Based on Histogram Analysis

Hamza A. Ali
Computer Engineering Department
College of Engineering, University of Basrah
Basrah, Iraq.

Sama'a A. K. khamis
Electrical Engineering Department
College of Engineering, University of Basrah
Basrah, Iraq.

Abstract—Watermarking techniques can be classified into two main categories; Spatial and Transformational approaches. They are characterized to rely on descriptive global models through which each technique is formalized and structured using models of Steganography and Encryption.

This paper presents a robust digital image watermarking technique that attributes the watermarking process to signal modulation model. It is based on the histogram analysis for maximum intensity value of pixels. First, carrier image is properly segmented into blocks, then the histogram for each block is drawn and the peak frequency of occurrence for intensity moments in the carrier image is identified. Then bit values of the modulating (watermark) image are used to modulate the histogram peaks of the intensity.

Experimentation and analysis on the proposed algorithm show that it is not only simpler and easier to implement, but also it is very effective, secure and robust against different kinds of attacks such as noise, resizing and rotation. Therefore one can conclude that it establishes a concrete judgment for ownership decision to approve ownership in copy write and ownership disputes.

Keywords- Image in image hiding; Digital watermarking; Steganography; Histogram.

I. 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].

II. CHARACTERISTICS OF WATERMARKING

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

1. *Visibility*: an embedded watermark can be either visible or not visible according to the requirement.

2. *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 [10].

3. *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.

4. *Integrity*: No loss of original multimedia carrier.

5. *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.

6. *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 [11].

2.1 Histogram process

Intensity histogram is one simple but very important statistical feature of an image. It has been commonly used in image processing; intensity histogram is a distribution of the gray level values of all pixels within the image. Each bin in the histogram represents the number of pixels whose intensity values fill in that particular bin. A 256 gray level histogram is often used, where each gray level correspond to one bin. Using bi to represent the ith number of bins, the histogram can be represented by equation 1.

$$h(i) = \#\{(x, y), f(x, y) \in b_i\} \quad . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \quad (1)$$

Where # represents the cardinality of the set, figure 1 shows an example of the histogram of color image [12].

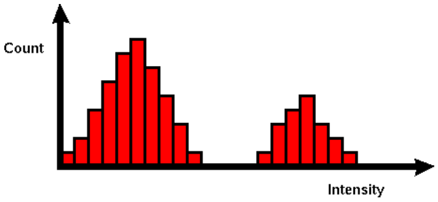


Figure 1. Intensity Histogram [12]

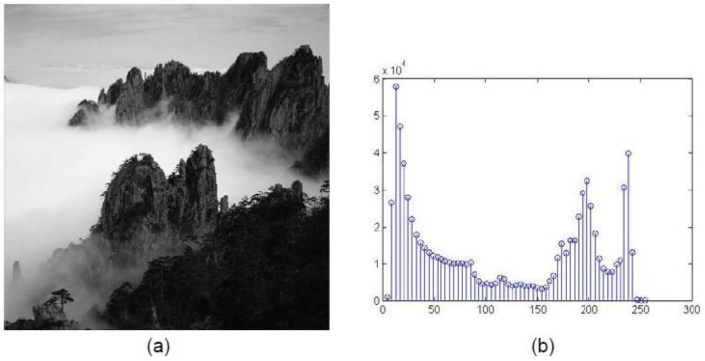


Figure 2. A mountain image (a) and its 64 bins gray level histogram (b) [12]

2.2 Histogram equalization

It is the fact that the histogram of an intensity image lies within a limited data range. Those images usually have black or white foreground and background. Figure 2 shows an example whose intensity distribution is either black or white. From figure 2-b, it can be seen that a very large portion of pixels whose intensity resets within the range [0-50] or [180-255]. A very small portion of pixel resides in the range of [50-180]. This made some details of the image hardly visible such as the tree on the mountains in the image shown in figure 2-a. This problem can be solved by a histogram stretching technique called histogram equalization.

The basic idea of histogram equalization is to find the intensity transform such that the histogram of the transformed image is uniform. Of the existing probabilistic theories, there exists such an intensity transform. Suppose that we have an image f(x, y), and its histogram h(i), then the accumulative function of h(i) can be found by equation 2 as follows.

$$C(i) = \int_0^i h(t)dt \quad . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \quad (2)$$

It can be proved that such a transform makes the variable y = C(i) follow a uniform distribution. Thus, for a 256 gray level image, the histogram equalization can be performed by applying equation 3 below.

$$T = \frac{256}{n} * c\big(f(x,y)\big) \quad . \ . \ . \ . \ . \ . \ . \ . \ . \ . \quad (3)$$

Where n is the total number of pixels in the image [12].

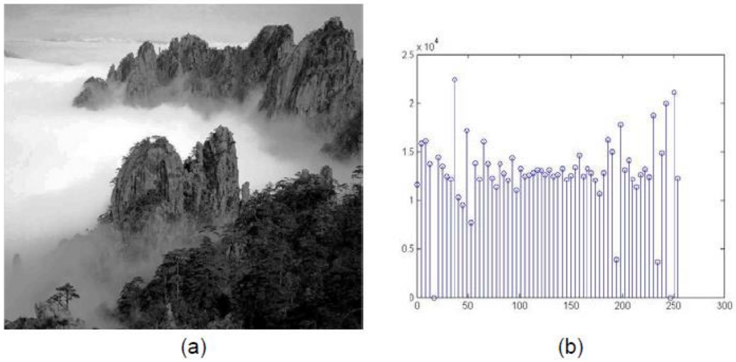


Figure 3. (a) The mountain image after equalization. (b) Histogram [12].

III. The Proposed Watermarking Processes

General description of the watermarking algorithm proposed in this paper can be thoroughly done in terms of two main activities, namely modulation and demodulation. They are outlined here after.

A. *Modulation process*

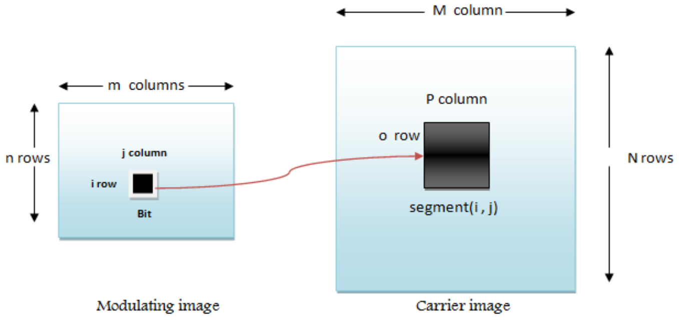
Step 1: Read both of the carriers and modulating images.

Step 2: Convert carrier image from its color space into gray scale.

Step 3: Resizing the modulating image into proper. Dimension parameters (i.e.' rows and columns) such that the carrier image parameter can be evaluated as even multiplicands of modulating image parameters. A suitable process that translates this matter is to detect the dimension parameter of the modulating image first, step by step reducing each parameter and test for the division modules of the carrier parameter by the modulating parameter. The criteria for ending this procedure is decided when the modulus of the related division operation becomes zero. The resulted parameters are then used to resize the modulating image into its new dimension.

Step 4: The modulating image is converted into black and white color space. Now it is possible to map one regional segment from the carrier image into one bit of modulating image as illustrated in figure 4.

Step 5: After dividing image into blocks (segment) and finding the maximum value of histogram for each block that means the intensity that having the maximum value of pixels. Then embedding process is done depending on the bit value of binary image, if the value is 1 then the intensity is increased by a predefined amount , else if the bit value is 0 then the intensity is decreased by the same amount. The said predefined value must be selected such that it gives good enough copy right evidance without affecting the carrier image quality. In the reported algorithm here this value is taken as two. However, other values might prove practical too.



o=N/n , p=M/m

Figure 4. Bit to segment configuration between Modulating and Carrier Images

Step 6: Finally the modulating image, original and resized modulating image are saved for usual data handling and future disputes as evidences for ownership judgment.

The overall activity of the modulation is interpreted in a suitable programming structure with the aid of the flow chart of figure 5.

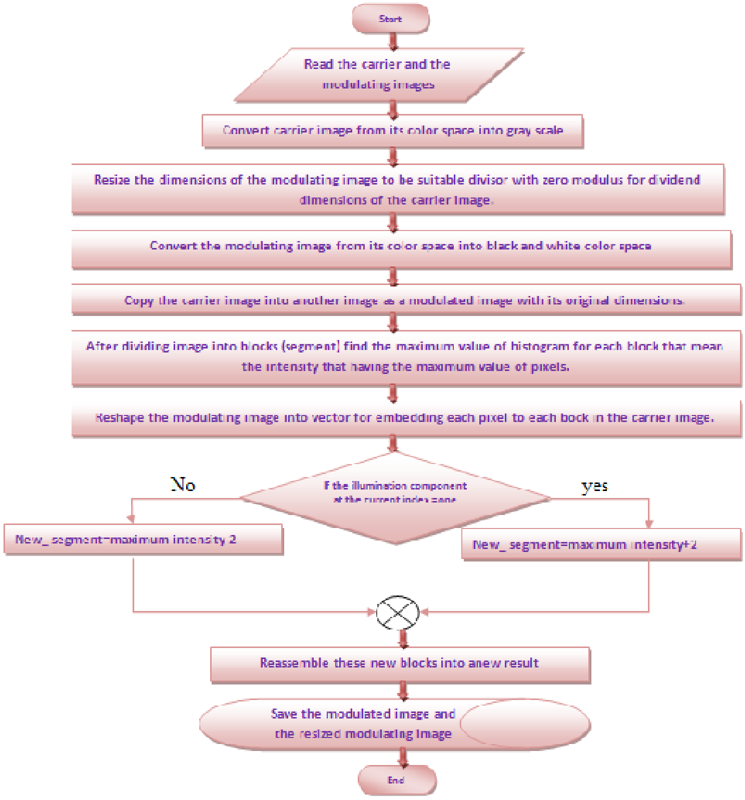

Start
Read the carrier and the modulating images
Convert carrier image from its color space into gray scale
Resize the dimensions of the modulating image to be suitable divisor with zero modulus for dividend dimensions of the carrier Image.
Convert the modulating image from its color space into black and white color space
Copy the carrier image into another image as a modulated image with its original dimensions.
After dividing image into blocks (segment) find the maximum value of histogram for each block that mean the intensity that having the maximum value of pixels.
Reshape the modulating image into vector for embedding each pixel to each bock in the carrier image.
No
F the illumination component at the current index =one
yes
New_ segment=maximum intensity 2
New_ segment=maximum intensity+2
Reassemble these new blocks into anew result
Save the modulated image and the resized modulating Image
End

Figure 5. Modulation process

B. *Demodulation Process*

This process is used to extract the watermark from the modulated image in order to prove its ownership. As this is not blind watermarking, the original image and the modulated image are supposed to be available. The overall activity of the watermark demodulation outlined in the following steps and illustrated in figure 6 below.

Step1: Read the original image (carrier image), and the modulated image.

Step2: Divided the carrier image into equal blocks (segment) according to the available information of the watermark size. Then find the intensity that have the maximum value of pixels in histogram for each block.

Step3: Divided the modulated image into blocks and find the intensity for each block after embedding.

Step4: Apply equation 4 to determine pixel values of the watermark.

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

Where D is the difference value between the maximum values of the two histograms.

Step5: Save the extracted watermark image.

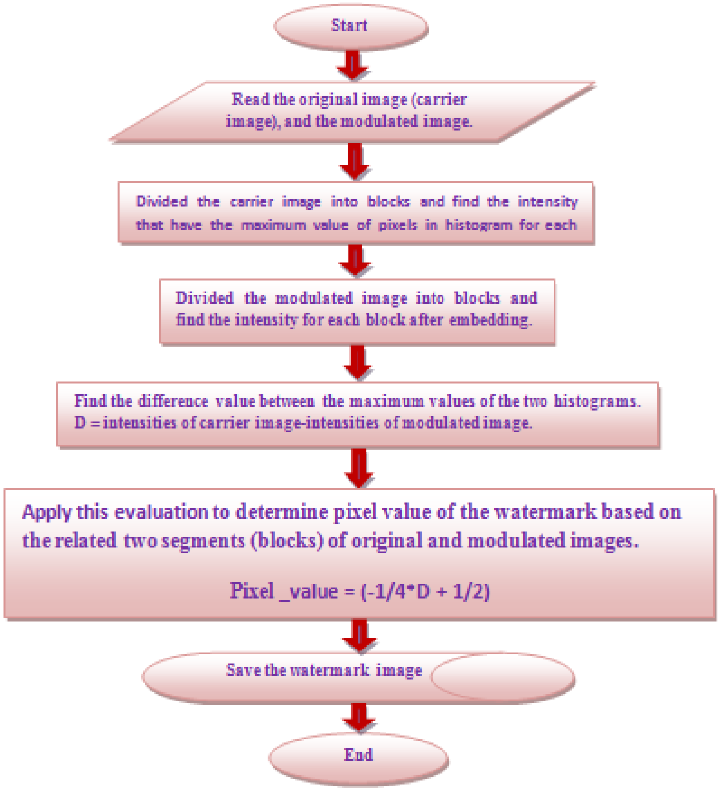

Start
Read the original image (carrier image), and the modulated image.
Divided the carrier image into blocks and find the intensity that have the maximum value of pixels in histogram for each
Divided the modulated image into blocks and find the intensity for each block after embedding.
Find the difference value between the maximum values of the two histograms.
D = intensities of carrier image-intensities of modulated image.
Apply this evaluation to determine pixel value of the watermark based on the related two segments (blocks) of original and modulated images.
Pixel _value = (-1/4*D + 1/2)
Save the watermark image
End

Figure 6. Demodulation process

IV. Implementation and Results

In this prototype algorithm, the carrier and the modulating images are selected for computation convenience to be of (512x512) pixels and (16x16) bits sizes respectively. The carrier image is a gray scale image but the modulating image is a binary image. Therefore one would have 256 bit (pixel value) of modulating image (binary image) that can be embedded in the carrier image into 256 blocks each block of size (32*32). The proposed algorithm, namely modulation and demodulating algorithm were run to embed and extract the watermark, respectively as follows.

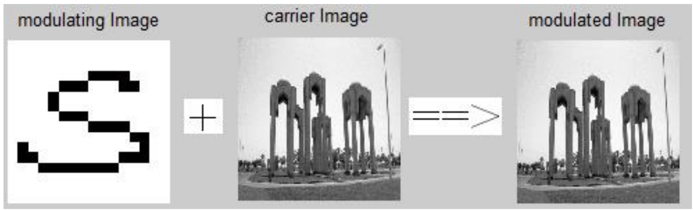


Figure 7. Embedding Process Result

Figure 7 shows the embedding (modulating) process as the carrier image and the modulating image produced the modulated image. Figure 8 illustrates the extraction (demodulation) algorithm as having carrier image and the modulated image only, then from which the watermark is extracted.

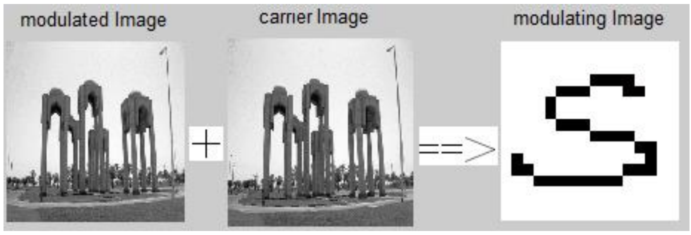


Figure 8. Extraction Process Result.

Comparing watermarked image with the original image results requires a measure of image quality. Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are the commonly used measures for evaluation of image quality.

The mean-squared error (MSE) between two images is given by equation 5.

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{m}\sum_{j=1}^{n}(fc(i,j) - fm(i,j))\,2 \quad . \; . \; . \quad (5)$$

Where $fc(i,j), fm(i,j)$ represent the pixel values of original carrier image and the modulated image, respectively. The parameters (m, n) specify row and column size of images respectively. MSE depends strongly on the image intensity scaling.

However, the Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling MSE according to the image range, R, and it is calculated by the equation 6.

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad . \; . \; . \; . \; . \; . \; . \; . \; . \; . \quad (6)$$

PSNR is a good measure for comparing restoration results for the same image; however comparisons of PSNR between-image are meaningless, therefore it only give a rough approximation of the quality of the watermark.

Some testing and measurements of MSE and PSNR were conducted on the algorithm implementation and the results are listed in table 1. The performed experiments on the modulated image involved attacking the modulated image by the addition of a different types of noise including Gaussian noise, Poisson noise, salt and pepper noise, and Multiplicative noise. PSNR of modulated image were calculated having performed each one of the mentioned attacks on the modulated image. Moreover, the table also listed the effect of median filter, image resizing and rotation. Photographs of the modulated images including different types of attacks and interference are also illustrated in figure 11.

TABLE 1. IMPLEMENTATION RESULTS FOR CARRIER IMAGE

Kind of attack	*MSE*	*PSNR(db)*	*Correlation*
Gaussian noise	**180.29**	**25.61**	**0.98**
Poisson noise	**146.92**	**26.49**	**0.99**
salt and pepper noise	**450.55**	**21.63**	**0.96**
Multiplicative noise	**884.24**	**18.70**	**0.92**
Median Filter	**65.11**	**30.03**	**0.99**
Image resizing	**0.0026**	**73.95**	**1.00**
Rotating	**0.0012**	**77.47**	**1.00**

Histograms for the calculated PSNR and correlation measurements are plotted for the considered attacks; Gaussian noise, Poisson noise, salt & pepper noise, speckle noise, median filter, image resizing, image rotation attacks on the modulated image in figures 9 and 10.

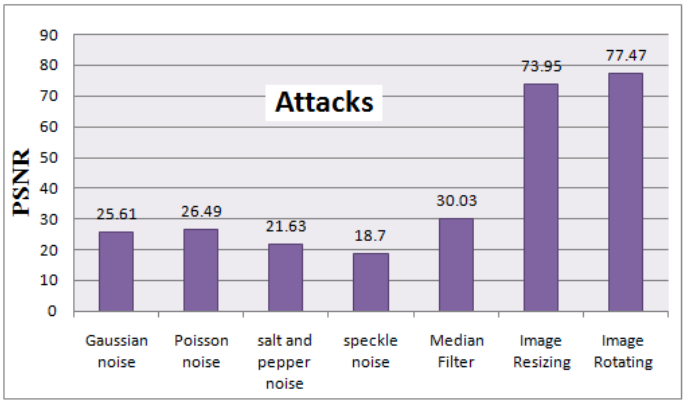


Figure 9. PSNR vs. Types of Attacks

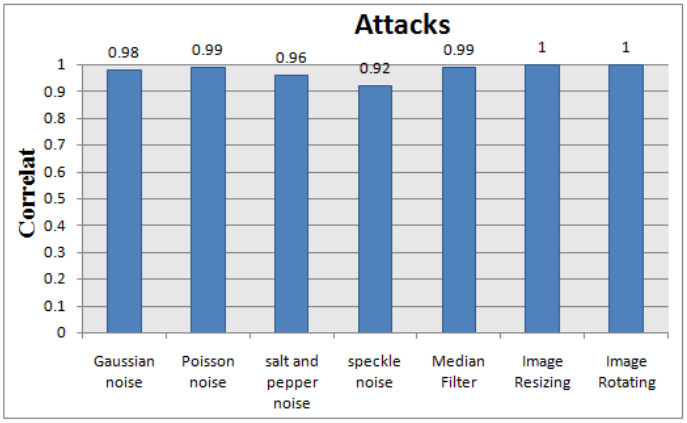


Figure 10. Correlation vs. Types of Attacks

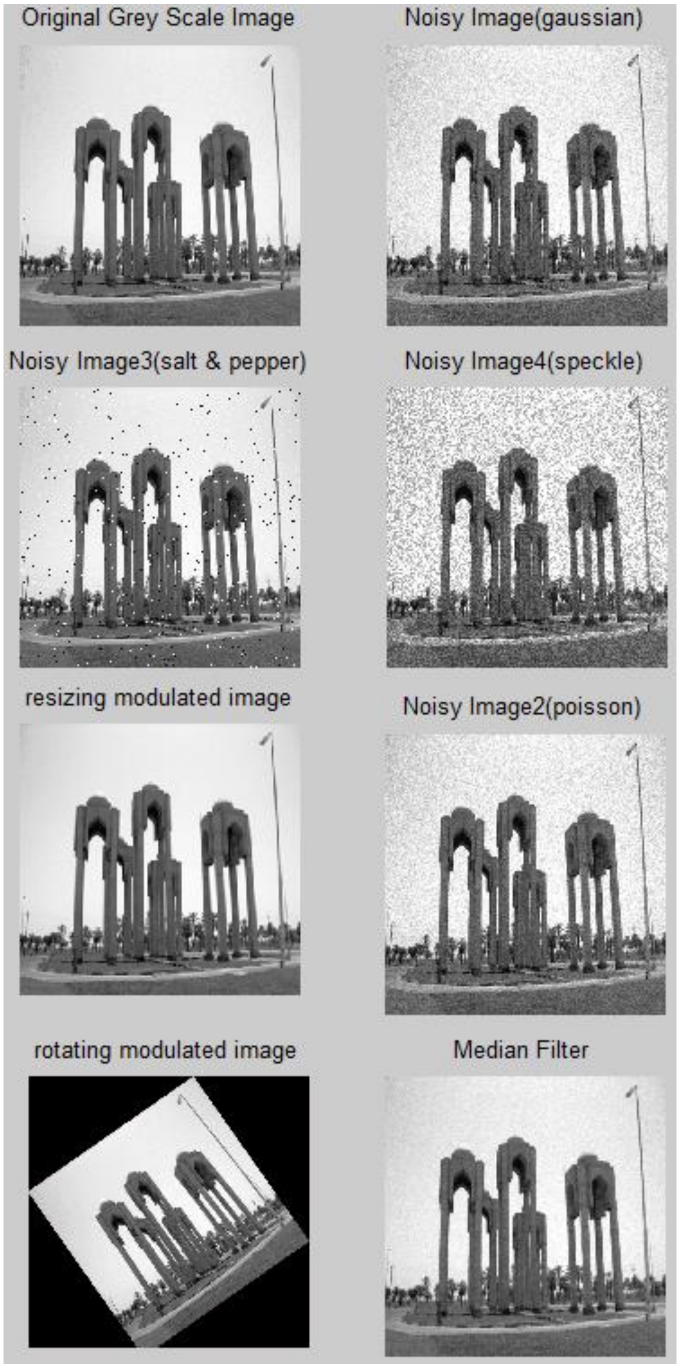


Figure 11. Types of attacks on the modulated image

V. CONCLUSIONS

The proposed watermarking technique relies on modification efforts to the histogram of the frequency of occurrence of pixels intensities in a digital image. The carrier image is first segmented into blocks, a histogram for each block is plotted and the maximum value of the pixels is changed by a predefined value. The watermark, the original and modulated images are all saved for usual data handling and future disputes as evidences for ownership judgment.

Testing the proposed algorithm by calculation of the Mean Square Error (MSE) and Peak signal to noise ratio (PSNR) for the modulated images using various attacks such as addition of Gaussian, Poisson, salt & pepper and speckle noise are performed. Moreover, other effects such as inclusion of median filter, resizing and rotating the modulated image are also performed. The obtained results show that the proposed technique is very secure and robust against these attacks. Besides it embeds the watermark bits information evenly throughout the carrier image with the flexibility of using different predefined value for the modification of the chosen location.

References

[1] [1] Malik H., Ashfaq Khokhar and Rashid Ansari, “Robust Audio Watermarking Using Frequency Selective Spread Spectrum Theory”, IEEE. PP 385-388, 2004.

[2] [2] Muntean T., E. Grivel and Mohamed Najim, “Audio Digital Watermarking Based on Hybrid Spread Spectrum”, Proceedings of the Second International Conference on WEB Delivering of Music (WEDELMUSIC.02), 2002.

[3] [3] Cox I.J., J. Kilian, T. Leighton and T.Shamoon, “Secure Spread spectrum Watermarking for Multimedia”, IEEE Transactions on Image Processing, Vol. 6 No. 12, PP 1673-1687, December 1997.

[4] [4] Podilchuk, C.I. and E.J. Delp, “Digital Watermarking: Algorithms and Applications”, IEEE Signal Processing Magazine, PP 33-46, July 2001.

[5] [5] Cox I.J., M.L. Miller and J.A. Bloom, “Digital Watermarking”, Morgan Kaufmann Publishers, 2002.

[6] [6] Chun-Shien Lu., “Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property”, Idea Group Publishing, 2005.

[7] [7] Wolfgang P., E.J. Delp, “A Watermark for Digital Images”, Proceeding IEEE International Conference on Image Processing (ICIP“96),Vol. III, Lausanne, Switzerland, PP 219-222, September 1996.

[8] [8] Nikolaidis N., I. Pitas, “Robust Image Watermarking in the Spatial Domain”, Signal Processing. Vol. 66, PP 385-403, 1998.

[9] [9] Celik M.U., G. Sharma, A. M. Tekalp, E. Saber, “Lossless Generalized-LSB Data Embedding”, IEEE Transaction on Image Processing, Vol.14, PP 253-266, 2005.

[10] [10] 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.

[11] [11] 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.

[12] [12] H. Zhou, J. Wu and Zhang, “Handbook of digital image processing”, Part1, 2010.