ICDIP 2015, Paris, France, 23–24 Jan. WASET 2015

A Hybrid Watermarking Model Based On Frequency of Occurrence

Presented by:

Prof. Hamza A. Al_Sewadi

Faculty of Information Technology, Isra University, Amman, Jordan

Co-researchers: **Adnan H.M. Al-Helali &**

Samaa A. K. Khamis

Contents

- Abstract
- Definitions, Applications & Attacks
- Histogram process
- Proposed Watermarking Technique
- Implementations and Results
- Comparisons with other works
- Conclusions

abstract

- Ownership proofs of multimedia such as text, image, audio or video files can be achieved by the burial of watermarks.
- This paper presents a procedure for watermarking by mixing amplitude modulation with frequency transformation histogram (referred to as **H**istogram **E**mbedding **T**echnique, **HET**).
- Results of comparison with other techniques (such as **DWT**, **DCT** & **SVD** showed an enhanced efficiency in terms of ease and performance.

(i.e. good degree of robustness against various environment effects such as resizing, rotation, and different kinds of noise. HET proved very useful technique for copy write protection and ownership judgment).

Definitions:

Information Hiding (***data hiding***): covers covert channels, anonymity, Steganography and copyright marking.

- ***Digital Watermarking***: is the process of embedding or hiding the digital information called watermark into the protected multimedia product such as an image, text, audio or video. The embedded data can be detected later or extracted from the multimedia for identifying the copyright protection & ownership.

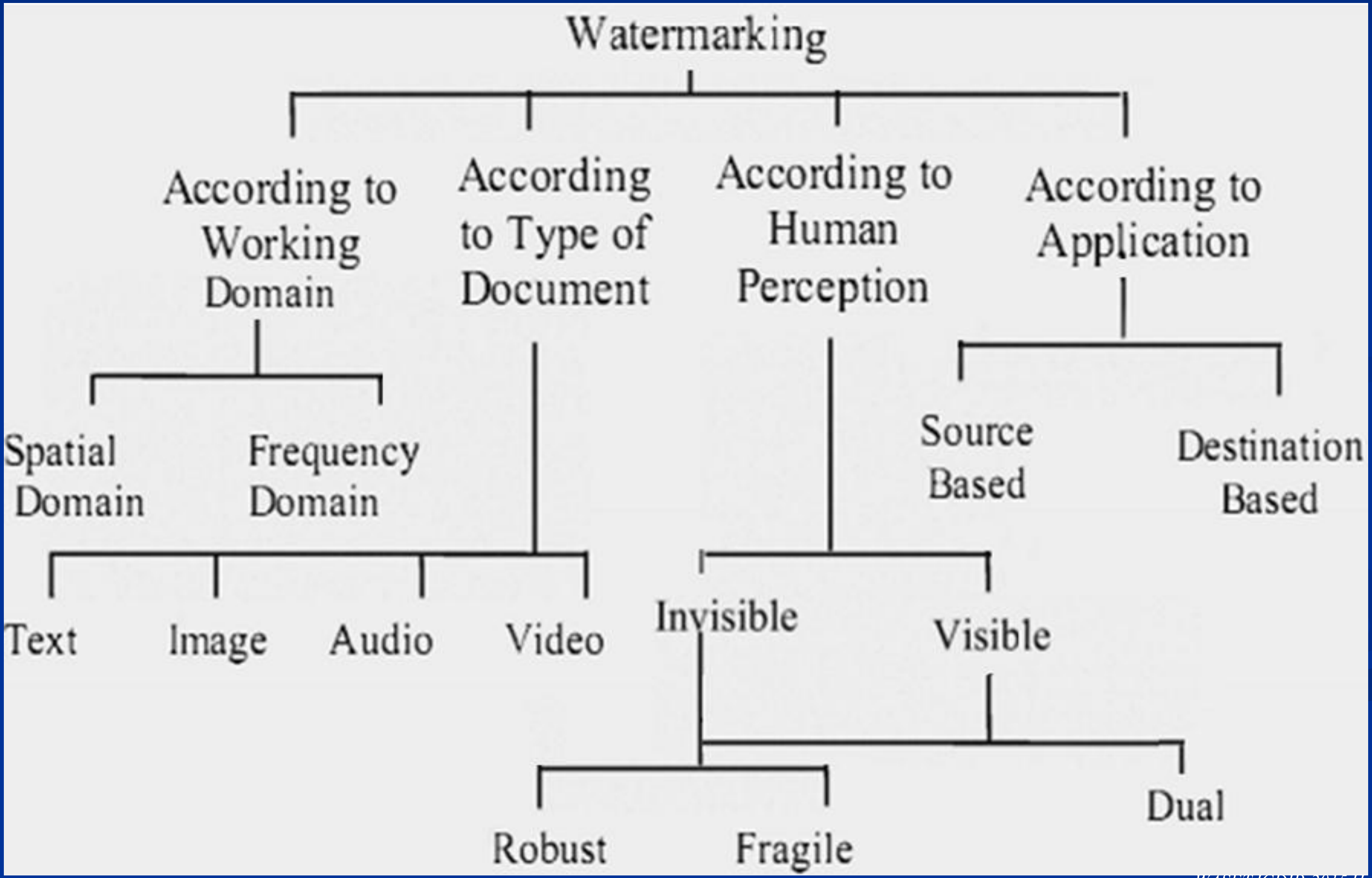
- ***It means***
  - introducing modifications, imperceptible to human senses but easily recoverable by a computer program.

- ***Watermarking is classified by:***

1. Spatial domain (time domain): (e.g. using LSB)
2. Transformation (Frequency) Domain: (e.g. Discrete Cosine-based watermarking DCT, Discrete Wavelet-based Watermarking DWT, Discrete Fourier Transformation DFT, Singular Value Decomposition SVD, ……

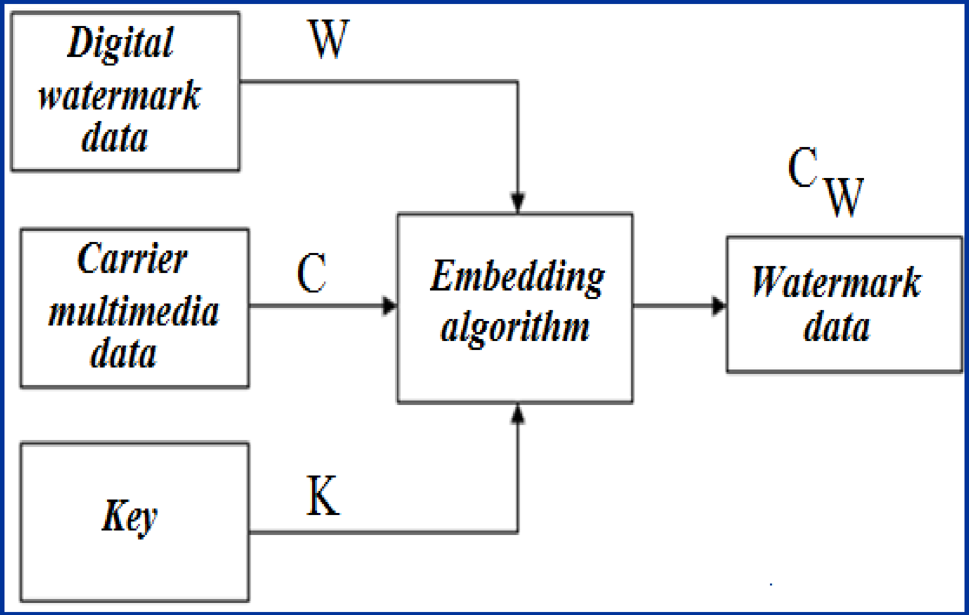
Types of watermarking (Classification)

- They can be classified according to type of document, human perception and application.

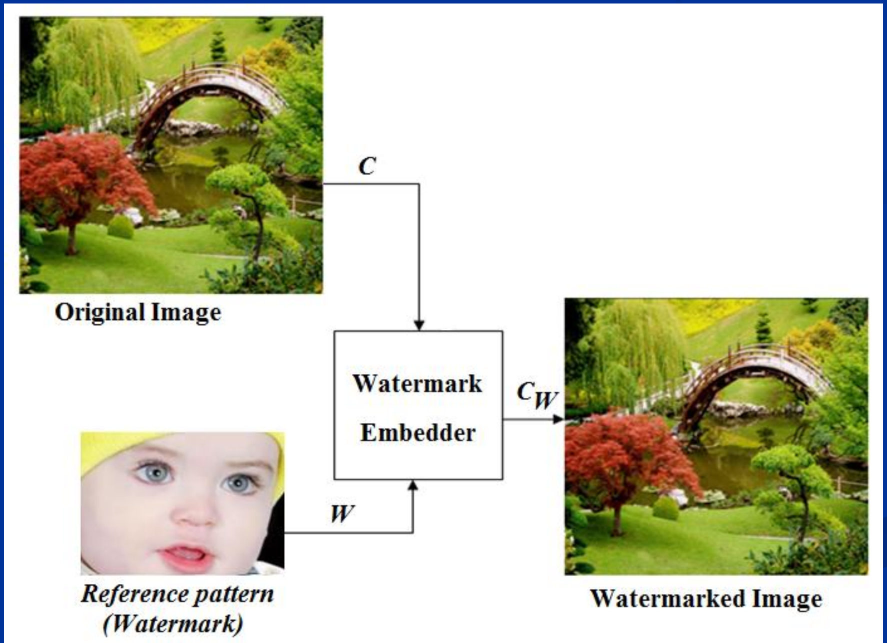


How Watermarking works

- As digital watermark data (W) is embedded in the Carrier multimedia data (C) using a certain key (K) through an Embedding algorithm in order to produce the watermarked data (C_W.



Watermarking Process Model



Illustration

Digital Watermarking Requirements

- **Perceptibility** : difficult to be noticed.
- **Robust:** high resistance to internal or external distortion.
- **Integrity**: no loss of original multimedia carrier.
- **Accessibility:** allows information handling.
- **Compatibility**: watermarked multimedia is compatible with original one.
- **Traceability:** allowing for modification and multiple watermarks.
- **Security**: provides protection of ownership against forgery and other threats.

Digital Watermarking Applications

There are so many application for watermarking of which are the followings:

- Authentication
- Copy protection
- Proof of ownership
- Broadcast monitoring
- Owner identification
- Transactional watermarks (Fingerprinting)
- . . . . . .

Digital Watermarking Attacks

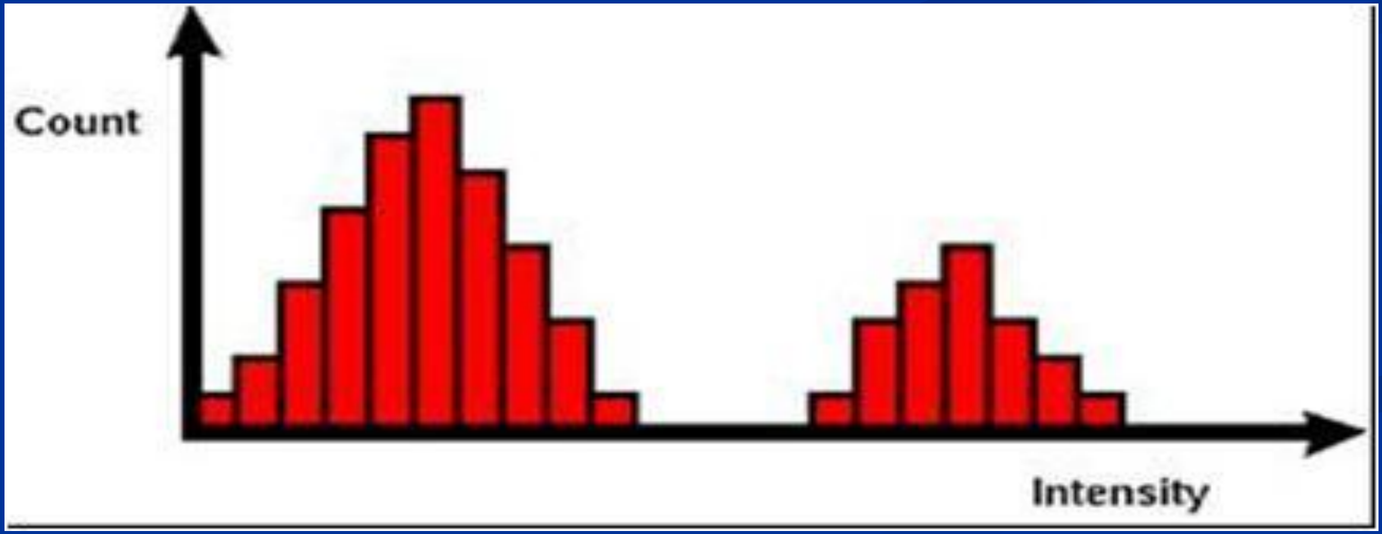
Attacks on watermark can be summarized as below:

- **Passive attacks**: not trying to remove the watermark, but is simply trying to determine whether a mark is present.
- **Active attacks**: trying to remove the watermark or make it undetectable. (Critical for owner identification, proof of ownership, fingerprinting, and copy control)
  - **Collusion attacks**: using several copies of one piece of media, each with a different watermark, to construct a copy with no watermark.
  - **Forgery attacks**: Hacker tries to embed a valid watermark, rather than remove one. This attack is a serious concern in proof of ownership.

Histogram Analysis process

- Intensity histogram is simple but very important statistical feature of an image, 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 fall in that particular bin. A 256 gray level histogram is often used, where each gray level correspond to one bin.



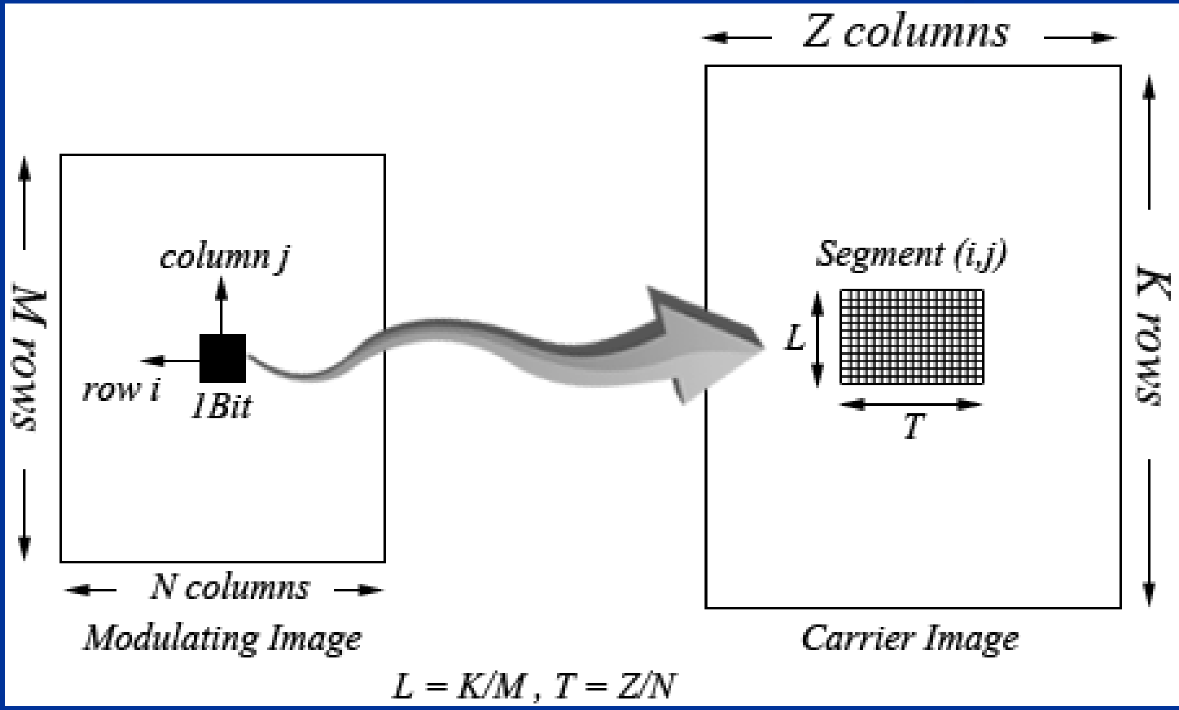
The Proposed Watermarking Processes

- This scheme involves algorithms for:
  1. segmenting carrier image into blocks,
  2. analyzing the histogram for the frequency of occurrence in each block then
  3. modifying the intensity of the first pixel that have the maximum frequency of occurrence according to the watermark.
- The general description of this algorithm can be thoroughly presented in terms of two main activities, namely embedding and extraction as outlined below:

Embedding Process: Embedding a watermark or a logo into a carrier image is achieved by the following steps:

1. Read carrier and watermark images, Convert **carrier** image its color space into YIQ, and modulating image into B/W space.

- Resized carrier to proper dimension parameters such that they become even multiplicands of watermark image dimensions (i.e. reduce rows and columns until getting integer L and T, where: $L = K/M, T = Z/N$)

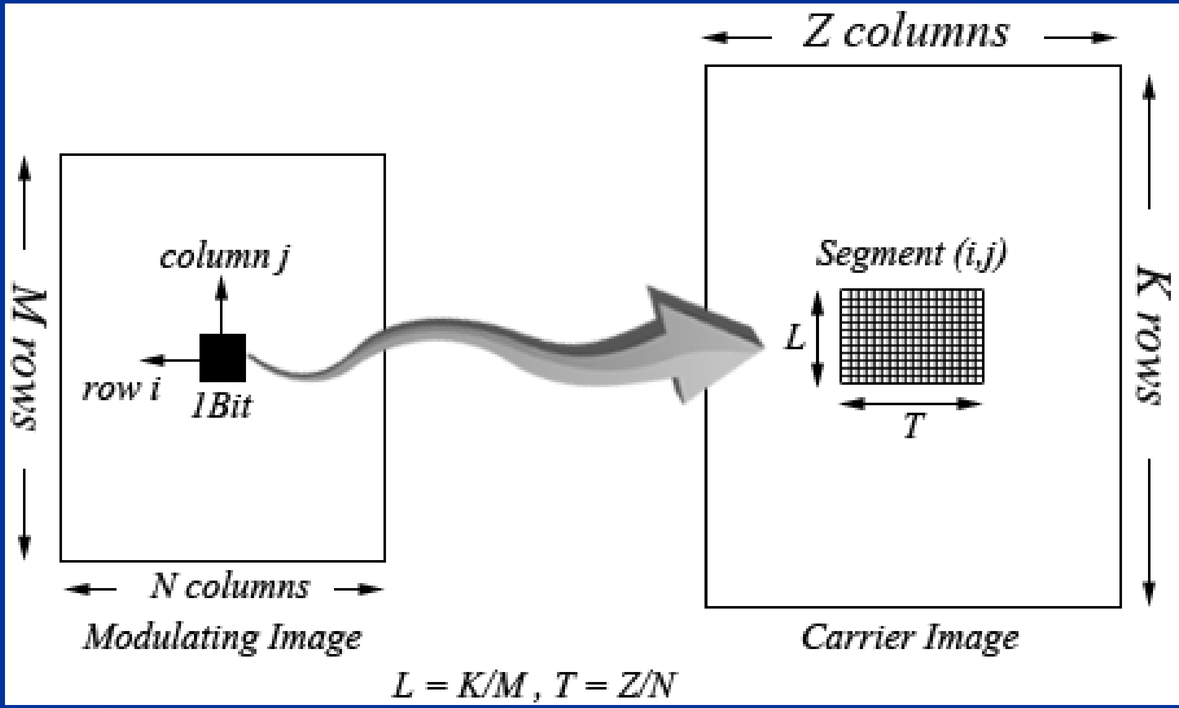


- Segment the carrier image into M x N blocks, each block of dimension L & T corresponds to one pixel of the watermark image.

2. **Mapping process**: Analyze the intensity histogram for each block to determine the intensity that have the maximum number of pixels. Then embedding process is performed depending on the bit value of binary image;

- if bit value is 1 then the intensity is increased by 1
- If bit value is 0 then the intensity is decreased by 1

3. **Reassembling** these new blocks after the modification to produce the watermarked image.



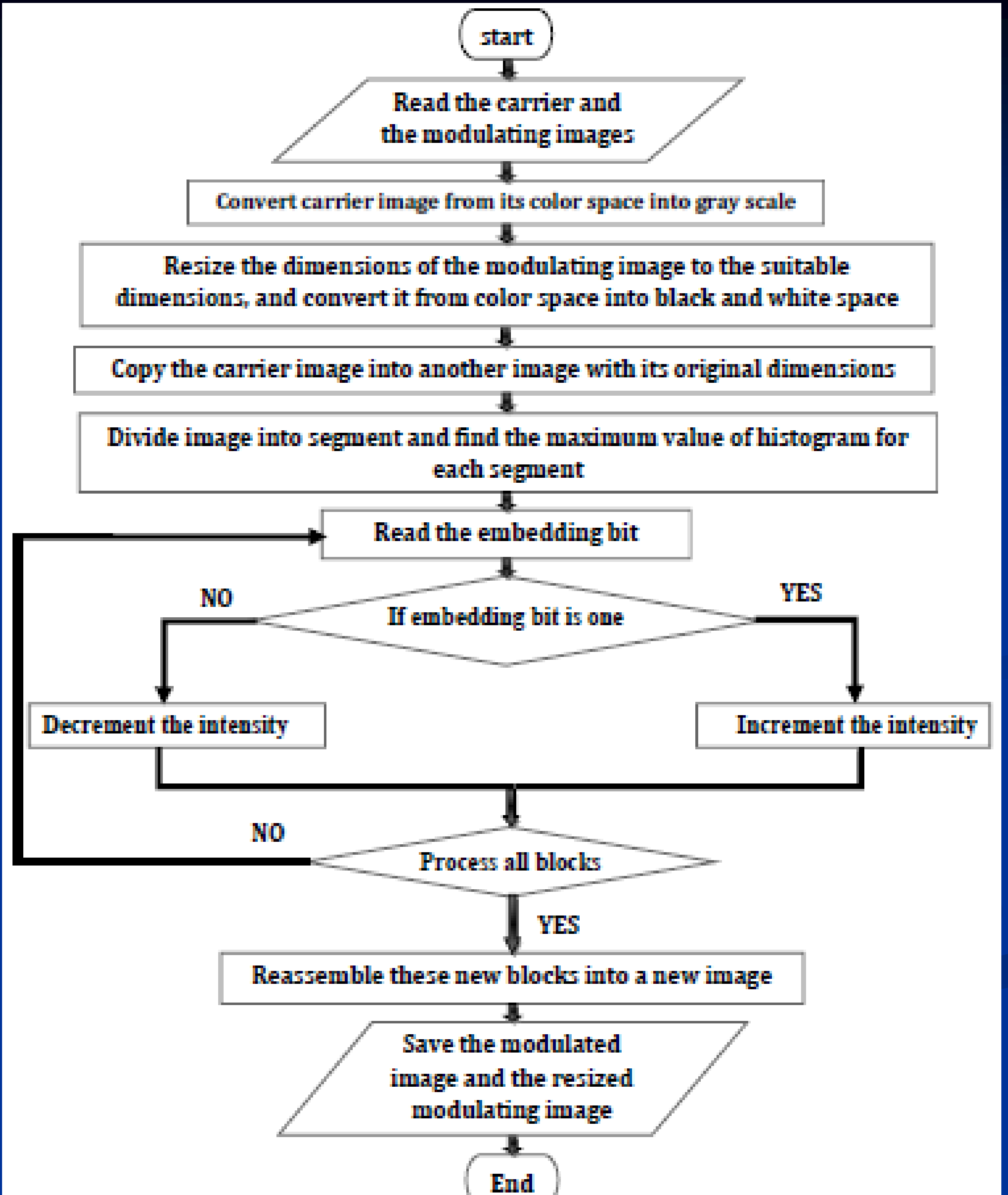
Embedding Process (Cont.)

- Finally the watermarked image, original and resized carrier image in addition to the watermark (logo) are saved for usual data handling in future disputes as evidences for ownership judgment.

- Watermark image dimensions: 32 x 32 bits totaling 1024 bits and host image dimensions: 512 x 512 pixels, segmented into 1024 blocks, each is 16 x 16 pixels.

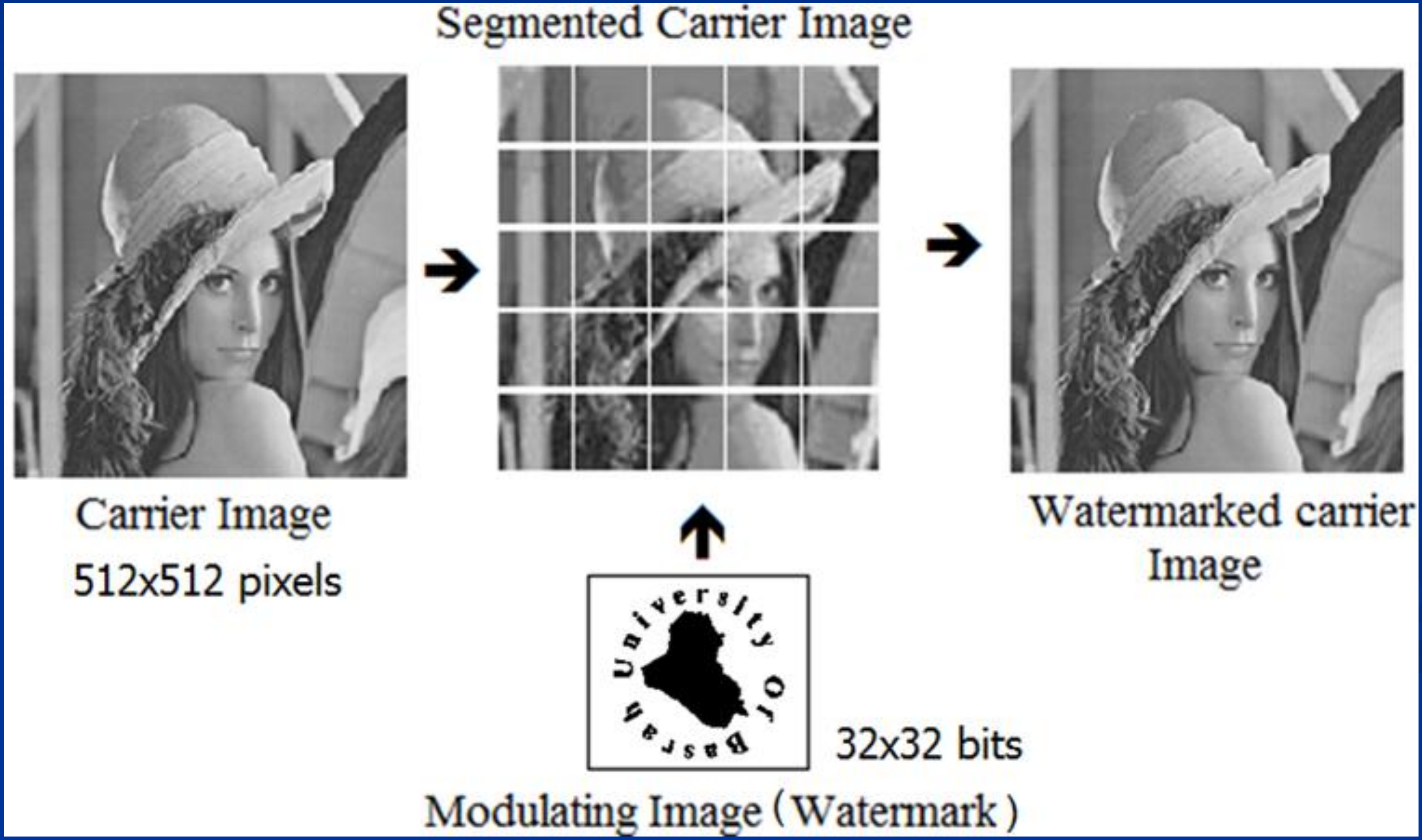
- **The overall activity of the Embedding algorithm is interpreted in a suitable MATLAB programming structure with the aid of the flow chart of the next slide.**

Embedding process flow chart



Embedding Process ...

- The carrier image and the watermark image are processed to produce the watermarked image.



Extraction Process

- Extracting the watermark from the watermarked image in order to prove its ownership. As this is not blind watermarking, the required materials are:
  1. **The original carrier image**
  2. **The modulated image**
  3. **The resized carrier image.**

- The watermark demodulation is outlined in the following steps:

1- Read the images mentioned above. (The third image only provides dimension or number of rows & number of columns).

2- Divided the modulated carrier image into equal blocks (segment) according to the available information of the watermark size (by reconstruct the Segment Boundary Table). Then find the intensity that have the maximum value of pixels in histogram for each block..

Extraction Process …

3- Scan the segments successively, handling a pair of segments each time; one of the original carrier and one of the watermarked image. Extract the histogram of the intensity color component and the related maximum frequency of occurrence.

- Then apply the equation below to determine pixel values of the watermark.

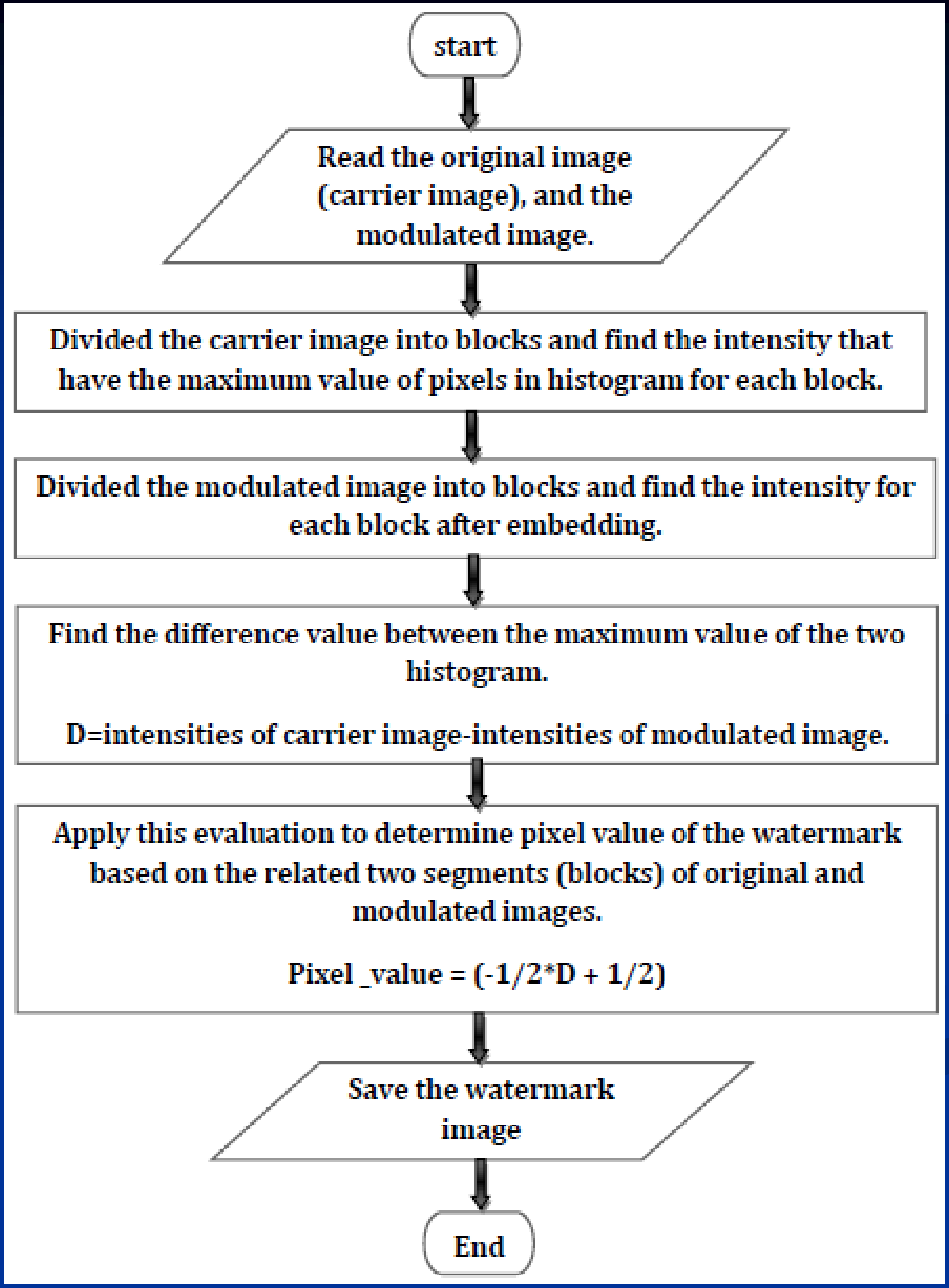
  Pixel _value = (-1/2*D + 1/2)

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

- Construct and Save the extracted watermark image .

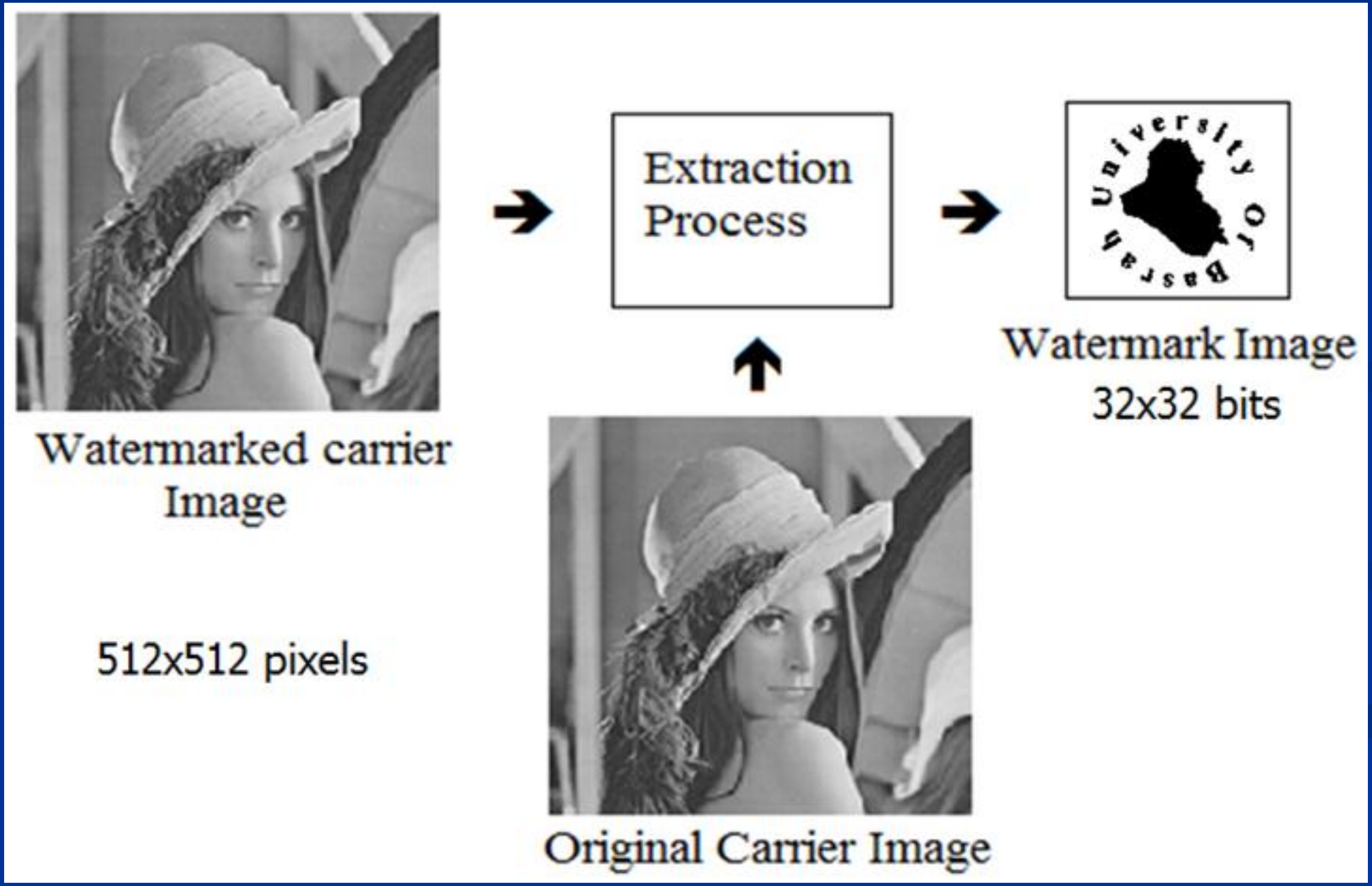
❖ The overall activity of the extraction process is also interpreted in a suitable MATLAB programming structure with the aid of the flow chart of the next slide.

Extraction process flow chart



Extraction Process …

- The watermarked and the original carrier images only are needed to produce watermark image.



Implementation and Results

- Watermarked image is compared with the original image in order to measure the image quality.

- Image quality is evaluated by means of:

1. Mean Squared Error (MSE)

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

2. Peak Signal-to-Noise Ratio (PSNR).

$$\text{PSNR} = 10\,log_{10}\left(\frac{255^2}{MSE}\right)$$

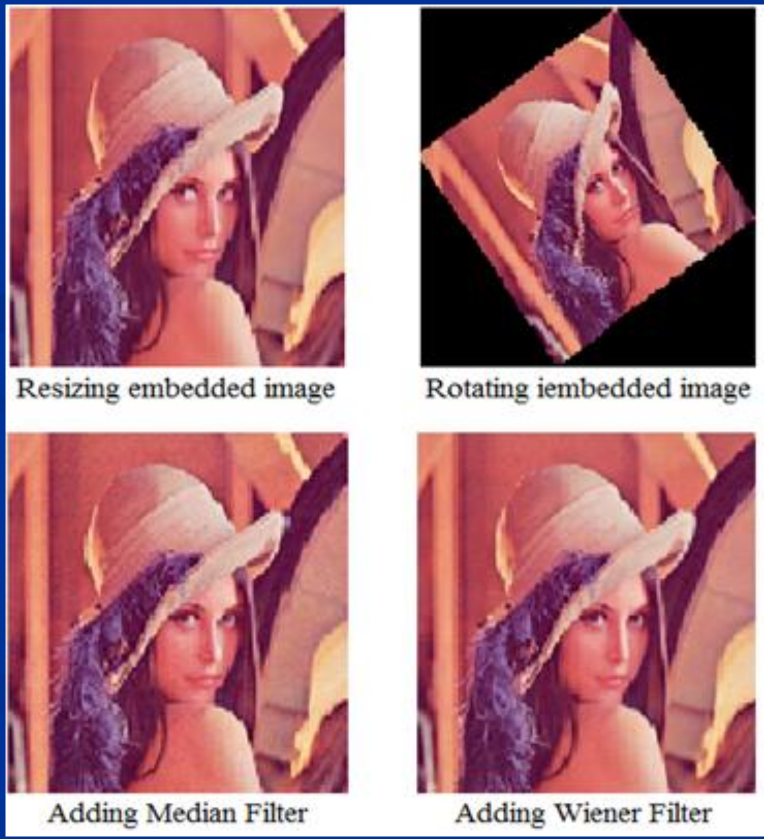
where *image range R = 255.*

3. Normalized cross Correlation (NC) is used to show the similarity between the original and the extracted watermark, which is defined by

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

Implementation and Results (Cont.)

- Experimental evaluation of MSE & PSNR values for watermark image in a gray scale carrier were conducted for different cases, such as **addition of noise**; Gaussian, Poisons, Salt and Pepper, and Multiplicative. And exposed to **disturbances**; Image Resizing, Rotating, Median filter, Wiener filter.



Implementation and Results (Cont.)

- All MSE, PSNR and Cross correlation with the original image is listed in the following table:

Kind of attack	MSE	PSNR(dB)	Correlation
Gaussian noise(0.003)	180.16	25.61	0.8938
Poisson noise	147.01	26.49	0.8409
salt and pepper noise(0.02)	444.68	21.68	0.9333
Multiplicative noise(0.04)	880.76	18.72	0.8576
Median Filter[3 3]	65.19	30.02	0.8472
Image resizing(256*256)	0.0014	76.74	0.8722
Rotating(35)	0.0005	81.140	0.8678

The Peak Signal to Noise Ratio (**PSNR**) and the Normalized Cross Correlation **NC** for the proposed scheme HET as well as DWT, DCT and SVD methods were calculated and listed in the tables of next slides for **comparison purposes** . (original image 256x256 and watermark image 8x8)

HET Scheme Versus Other Schemes

- To rate the usefulness and efficiency of the proposed HET algorithm which is based on the histogram analysis, comparison is done with available results of other published techniques.

PSNR FOR HET VERSUS OTHER SCHEMES

Effect of Attack	HET W: 125x125 C: 1024x1024	DWT W: 8x8 C:256x256	DCT W:32x32 C:256x256	SVD W:64x64 C:512x512
Gaussian Noise(0.0001)	39.9327	27.3059	NA	NA
Salt & Pepper noise (0.02)	32.1764	21.1394 For (0.01)	28.0851	31.36
Multiplicative noise (0.0001)	44.9426	27.4860	NA	NA
Median filter (3x3)	51.4763	35.0046	35.5801	34.29
Wiener filter (3x3)	30.7031	37.2799	NA	NA
Resizing (256x256)	0.0005	NA	NA	33.49

HET Scheme Versus Other Schemes

- After unifying the dimension of the original and watermark images with other available techniques, PSNR and NC for the HET scheme is recalculated and listed in Tables III, IV&V.

PSNR AND NC FOR HET VERSUS DWT SCHEME
(8×8WATERMARK AND 256X256CARRIER IMAGES)

Effect of Attack	PSNR C: (256x256), W:(8x8)			NC C: (256x256), W:(8x8)		
	HET	Prototype	DWT	HET	Prototype	WT
Gaussian noise (0.0001)	39.9800	39.3053	27.3059	0.8661	0.8650	0.8555
Salt & Pepper noise (0.02)	25.0541	25.2220	21.1394	0.8736	0.9682	0.8721
Multiplicative noise (0.0001)	29.0004	28.7790	27.4860	0.9523	0.9519	0.9434
Median Filter	31.7889	31.9100	35.0046	0.9748	0.8228	0.9824
Wiener filter	34.8883	25.4479	37.2799	0.9679	0.8018	0.9346

HET Scheme Versus Other Schemes (Cont.)

PSNR AND NC FOR HET VERSUS DCT SCHEME
(32×32 WATERMARK AND 256X256 CARRIER IMAGES)

Effect of Attack	PSNR C: (256x256), W:(8x8)			NC C: (256x256), W:(8x8)		
	HET	Prototype	DCT	HET	Prototype	DCT
Salt & Pepper noise (0.001)	35.7858	35.7292	21.1394	0.9016	0.88920	0.8643
Median Filter (3x3)	31.8184	29.8720	35.0046	0.8109	0.8567	0.9132

PSNR AND NC FOR HET VERSUS SVD SCHEME
(64×64 WATERMARK AND 512×512 CARRIER IMAGES)

Effect of Attack	PSNR C: (256x256), W:(8x8)			NC C: (256x256), W:(8x8)		
	HET	Prototype	SVD	HET	Prototype	SVD
Salt & Pepper noise	32.9430	32.8410	31.36	0.9562	0.88078	0.6674
Median filter (3x3)	42.0260	39.5425	34.29	0.9053	0.8988	0.7823
Resizing (256x256)	65.3521	64.9221	33.49	0.9587	0.9991	0.9372

Conclusions

- A new efficient and accurate algorithm has been developed and investigated for digital image watermarking that is based the histogram plot of the pixel intensities.
- Watermark image bits are distributed evenly in all the carrier image blocks, but irregular inside each block, which adds substantial improvement to the system security.
- Proved secure and robust against attacks like filtering, rotation and resizing, which is satisfactory in comparison with other schemes (such as DWT, DCT and VSD).
- Although, the modification to the chosen pixels was +1 or -1, the use of other values may prove useful to be adopted for certain applications, which gives extra flexibility for the scheme.

Thank you