Tamper Detection in Color Image

Ali Kadhim Mousa Khalid Kadhim Jabbar
Department of computer - Baghdad University

Abstract

This paper present a semi-fragile watermark for image authentication and blind tamper detection under DCT (discrete cosine transform) domain, for color BMP image (DCT based).

It depend on a type of attack, and the proposed method disunity between intended and un- intended attack (malicious and an malicious attack).

The proposed method was tested under different attack and it was found it provides a good detection performance and it has ability for opposition the intended attack with observance of image quality. Distortion on a watermarked image and recover watermark computed by using PSNR and MSE.

المستخلص

في هذه الورقه البحثيه نقدم العلامه المائيه من نوع semi – Fragile Watermark كموثوقيه للصوره الملونه بعد ان يتم تضمين صوره ثنائيه (شعار) Binary logo في غطاء الصوره الملونه الاصليه(frequency domain under DCT transform) ليتم فيما بعد اكتشاف اي تلاعب مقصود في الصوره من دون الحاجه الى الصوره الاصلية (Blind) لتحديد مكان التلاعب. هذه الطريق لها القدره على التمييز بين التلاعب المقصود والتلاعب الغير مقصود من خلال تعريضها الى مختلف انواع التلاعب.

تم تقييم جودة الصوره الناتجه من عملية الاخفاء بالاعتماد على قيمة (PSNR)، وبالاعتماد على قيمة (MSE) في تقييم مدى التشويه الحاصل في العلامة المائية المسترجعه.

1. Introduction

The digital watermarking technique, as an effective way used for copyright protection and image authentication, has become the research focus in international academic circles [1]. The watermarking schemes can be broadly classified into three types [2]: robust watermark, fragile watermark and semi-fragile watermark. Robust watermark [3] is generally used for copyright protection and ownership verification since it is robust to nearly all kinds of image processing operations such as lossy compression, spatial filtering and geometric distortions, etc.

Fragile watermark [4, 5] is mainly applied to content authentication since it is easy to be destroyed by any manipulation. Between these two extremes lies what is called semi-fragile watermarking. It could tolerate acceptable modifications to the watermarked image whilst it is sensitive to all other malicious manipulations and capable of localizing tampered regions. For image authentication purposes, many fragile and semi-fragile watermarking schemes have been presented.

Li et al. [6] have proposed a fragile spatial-domain watermarking scheme where a secret neighborhood is chosen for each pixel based on a pseudo-random sequence.

LI [7] proposed a transform-domain fragile watermarking scheme to watermark some selected transform coefficients so as to minimize embedding distortion. As semi-fragile watermarking could tolerate image processing manipulations as long as the image contents are preserved, the research on it has developed rapidly. Based on index constrained vector quantization, Lu et al. [8] presented a semi-fragile digital image watermarking scheme, which embeds the watermark information in the compressed bit streams.

Lin [9] presents a novel digital watermarking method for verifying the authentication of JPEG images, by applying the novel concept of lowest authenticable JPEG quality.

2. The proposed method

The start with some brass tacks:

1- The original image has size 256*256, with BMP file type and its color image to be later a watermarked image after embedding process complete.

2- The original watermark with size 128*128, with BMP file type and it's a binary logo pattern to be embedded latter in a cover image (all pixels of a watermark well embedded in a cover image), the size of watermark come from H/2 * W/2 where H represent the original image height and W represent the original image width.

3- The main steps that we depend on in the proposed method are:

A. Embedding operation.

B. Extraction operation.

C. Tamper detection.

The main diagram of proposed method shown in the stunt comer latter.

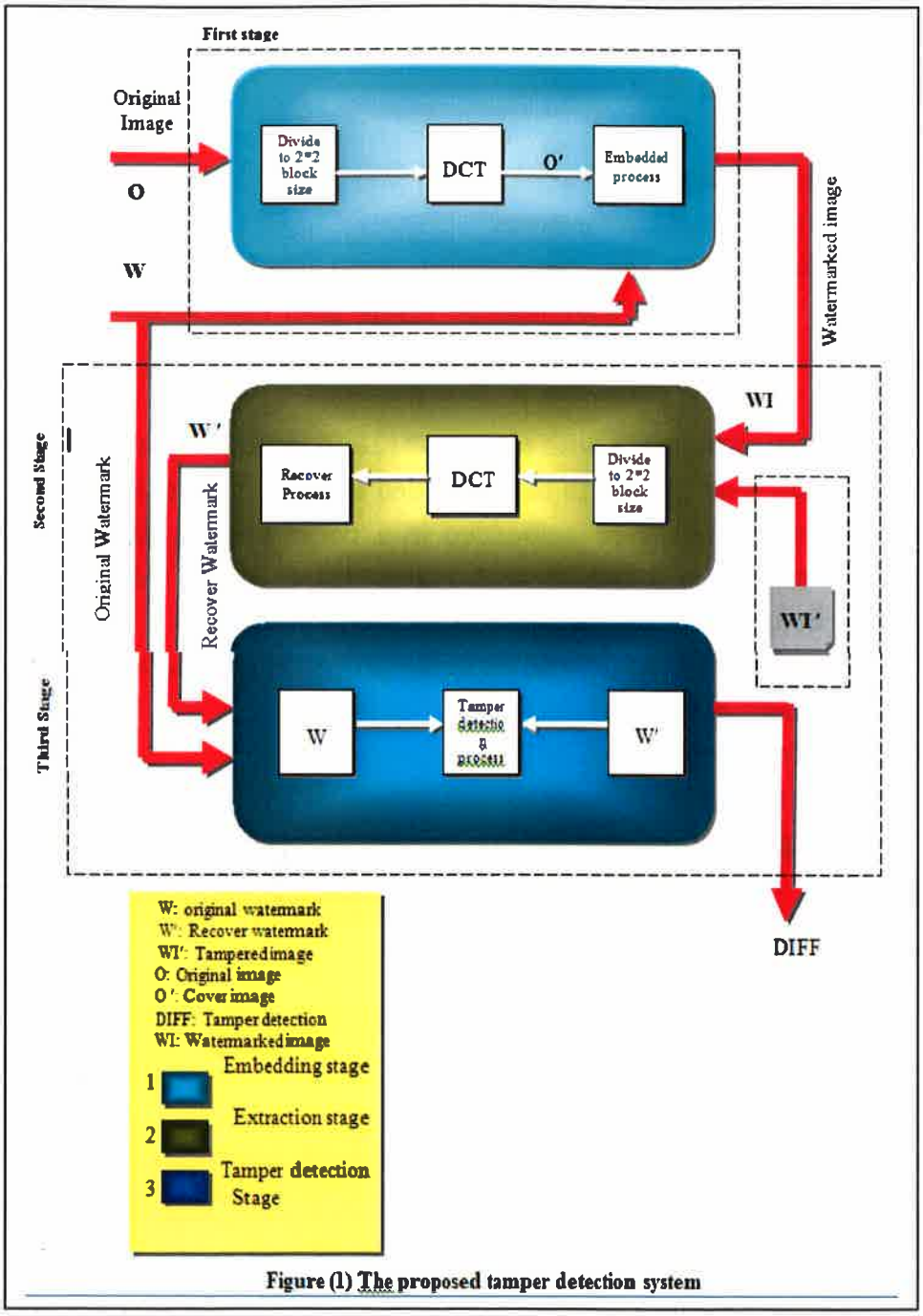

Figure (1) The proposed tamper detection system

The proposed method provides us with several image authentications such as:-

1- Exact authentication.

2- Selective authentication.

Therefore the dipper for this piper should know some important outline of the proposed method such as:

1- It is image authentication for tamper proofing in color image, and it is DCT (discrete cosine transform) based.

2- The grassroots of the work to determine if a received image is authenticate or not.

3- In the proposed method used a fixed place in every block for a whole image with three sub-bands color red, green and blue for hid watermark's pixels to produce after embedding operation complete the watermarked image.

4- The recover watermark can be extracted from test image without requiring explicit knowledge abut original image (blind).

5- If the information's content in test image unmodified (no tamper with), the extracted watermark exactly matches original watermark, otherwise

If test image modified, than the recover watermark well be different from embedding with probability vanishing close to one.

6- The differences between embedding watermark (original watermark) and recover watermark provided useful information or destroy credibility. The table bellows illustrate some commands used in the work emoted from the main inputs data and outputs in the system.

7-In the proposed method there are 9 of SP (shifting parameter) SP=2..., 10, after experiments we choose SP=2 to be depended in the work for the proposed method. Because we found that if we choose SP=2 we well gained a better PSNR (peak signal to noise ratio) value.

Notice:
SP=1 is excluded because if SP=1 then PSNR=inf .The table bellows illustrate some commands used in the work emoted from the main inputs data and outputs in the system.

Table (1) The main command used in the proposed method

Command	Signification
W	Original watermark
W′	Recover or extraction watermark
WI	Watermarked or test image
WI′	Tampered image or received image
O	Original image
O′	Cover image after DCT

2.1 Embedding process

In this operation for a proposed method, consider O as original image with size 256*256/24 bits, color BMP image, and W as original watermark with size 128*128 bmp/binary logo [W=x /2 (H of original image) * y/2 (w of original image)]. This module is used for embedding number of bits of W (Logo) in still color images, we reading an O to be after embedding operation complete WI and W for embedding it in O′.

At first O divided to 2*2 block size, to produce the blocks, DCT than applied for each block of whole O to produce the corresponding blocks of DCT coefficients. After dividing O into blocks, and apply DCT to produce O′, know O′ become prepared for embedding operation don, the overall scheme of embedding module is shown in algorithm (2.1).

Algorithm (2.1) embedding process

Input

Original image as O

Original watermark as W

Shifting parameter as SP

Output

Watermarked image as WI

Remark

This algorithm is used for read a color BMP file as original image to be cover image after DCT(discrete cosine transform)performed, than read an original watermark as W to great a watermarked image as WI after embedding process complete(all bits of original watermark W hid in a cover image).

Procedure

// main loop for three sub – bands color R, G, and B

Step1: For M ← 1:3

// select group of 2*2 block size

Step2: For I ← 1: r/2 // r=256

For J← 1: c/2 // c= 256

End;

End;

End;

Step: 3 perform DCT (discrete cosines transform) for each block of a whole image to great 2*2 map frequency components DCT (I, J).

Step: 4 embedding process

Step 5: perform IDCT (inverse discrete cosine transform) to reconstruct a WI

Step : 6 to improve a WI, the using of unit8 function is suitable to convert the elements of n_gray array to unsigned integer, n_gray of umric object (double),the output elements value ranged from 0 to 256 with class of unit8

n_rgb (: ,: ,M) ← unit8(n_gray);

Step : 7 imwrite (n_rgb,'c: \ewatermark.bmp');

End. // stop

To be continue

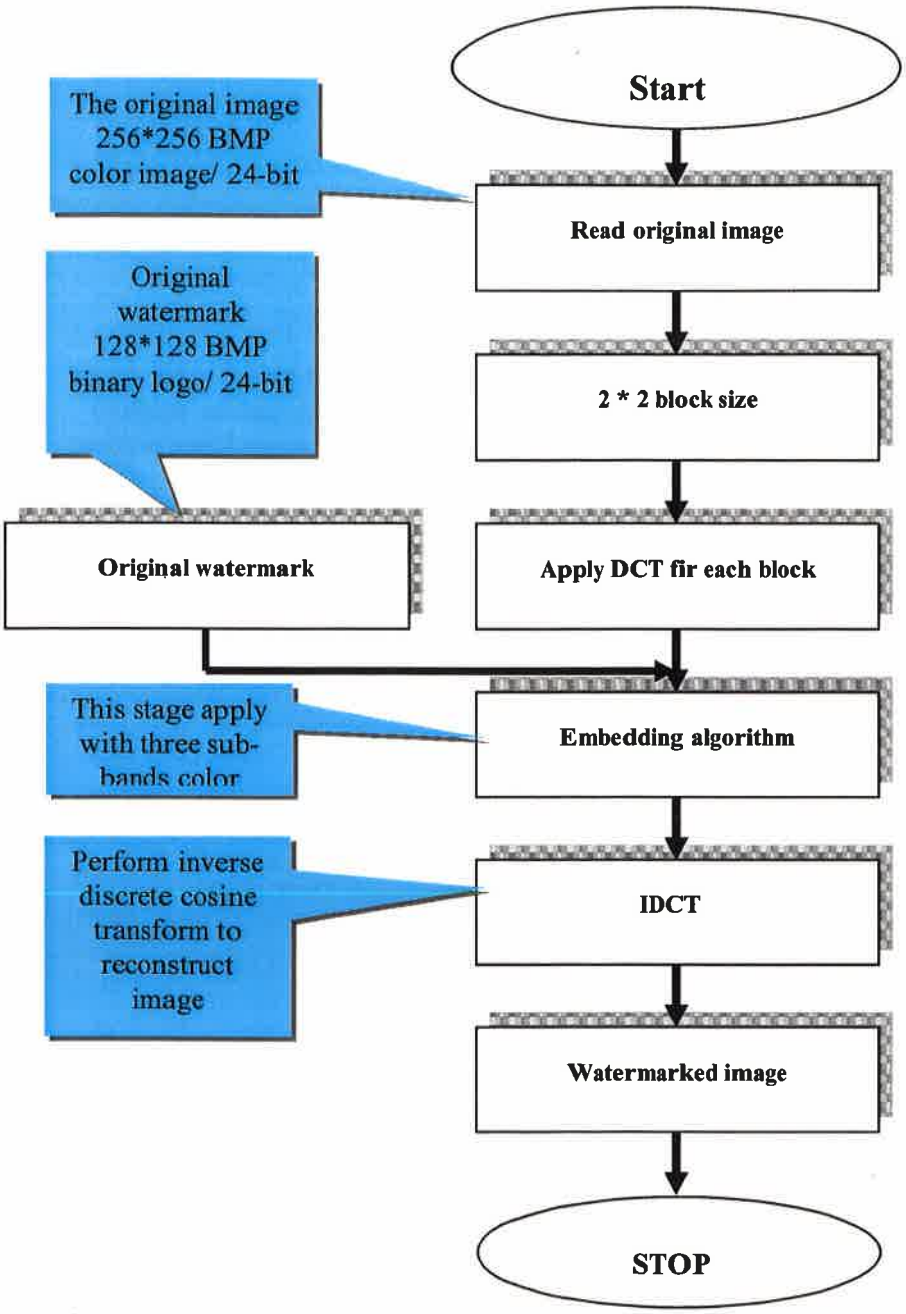

Figure (2) General flowchart for embedding process

After embedding operation done between O and W the resulting will be new image called WI, the next figure showing us the original image before and after embedding operation for two samples in the work, The value of PSNR that computed from equation (2) between O and WI after embedding operation done between O and W is illustrated in table (2).

(a) (b)

Figure (3) Watermarked image for child sample
(a) Original image (b) Watermarked image

(a) (b)

Figure (4) Watermarked image for Lena sample
(a) Original image (b) Watermarked image

2.2 Extraction process

The *extraction* process is very important and necessary to determine the status of the image (authentic or tampered). The extraction process is blind because it does not need the original image to retrieve the watermarks. With this process a received or test image divide into 2*2 block size, then applied DCT for each block of a whole WI to produce the corresponding blocks, each one have N*N size when N=2, and it contained four coefficients, this operation with circumstantialities illustrate in next the algorithm bellow:

Algorithm (2.2) Extraction process

Input
Watermarked image as WI

Output
Recover watermark as W'

Procedure
Step: 1 rgb ← imread ('ewatermark');
For M ← 1:3 // main loop for three sub – bands color R, G, and B

Step: 2 select group of 2*2 block size
For I ← 1: r/2 // r=256
For J ← 1: c/2 // c=256
End;
End;

Step: 3 apply IDCT (inverse discrete cosine transforms) for each block of a whole WI to great 2*2 map frequency.

Step: 4 Recover process

End;
End;
End. // Stop.

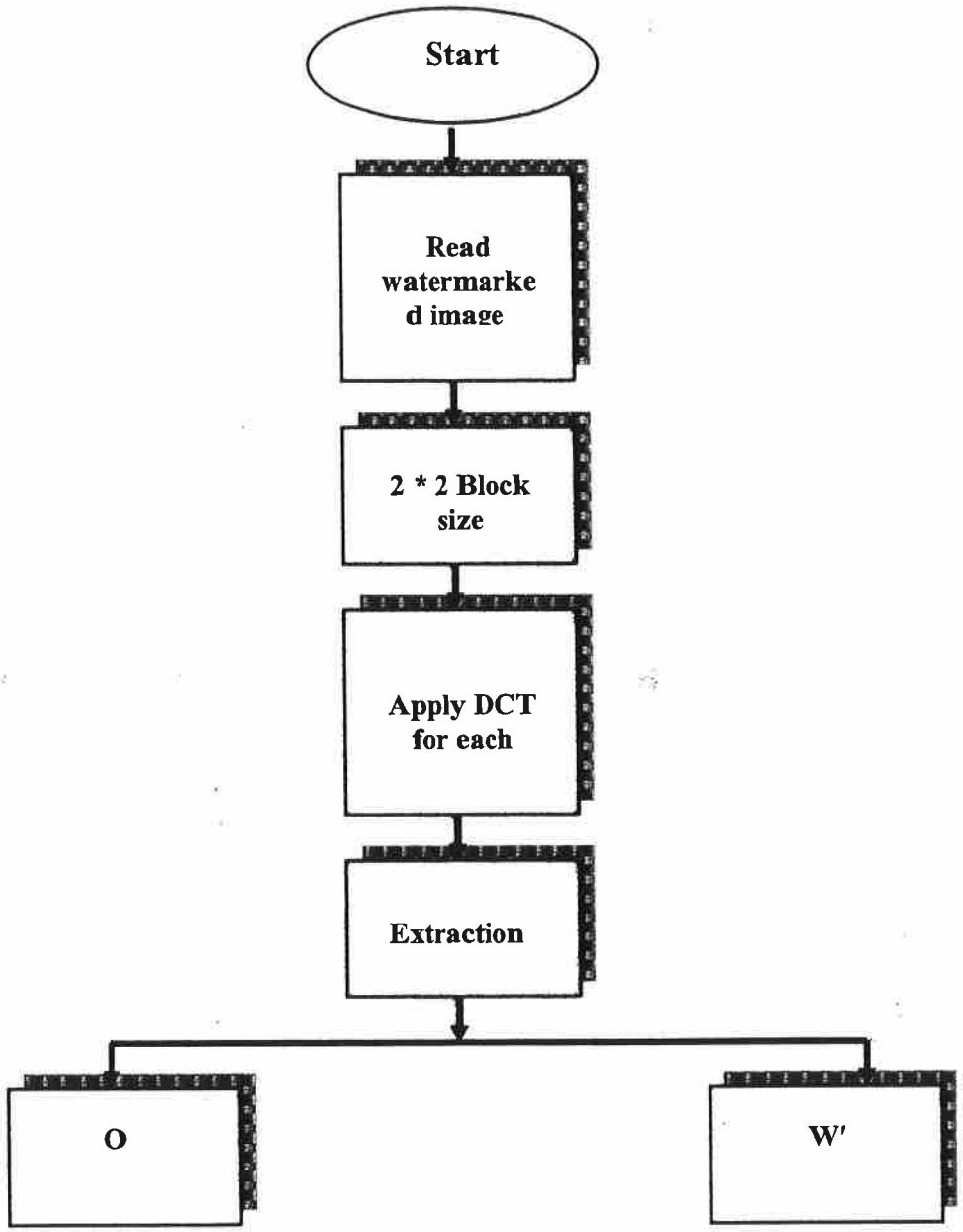

Figure (5) Flowchart for extraction process

After watermark recovered we calculated MSE from equation (1), between W and W′ to determine the value of MSE for W′ before any attack, this value is useful in the stunt comer latter with performance of proposed method, table (3) illustrate the value of MSE before attack between W and W'.

The reader should know that the image texture is effect on MSE value from one image to another. MSE value better if it is lesser, we found that the worst sample in this test is poor, but the value of poor sample accepted in general. We used the follow equation to compute the distortion in a recover watermark to determine MSE value before any attack to compare this value with new values that we well gain in the tests in the next comer latter.

$$MSE = \frac{\sum_{x,y} [O(x,y) - R(x,y)]^2}{W * H} \quad \text{----------} \quad (1)$$

Where $O(x, y)$ represents a pixel, whose coordinates are (x,y), in the original (undistorted image), and $R(x,y)$ represents a pixel, whose coordinates are (x,y) jn the reconstructed image, in the stego image. W and H represent the width and height of image respectively[11]

2.3 Tamper Detection Process

know we go to detect tampering with WI′ (if WI′ tamper with), by compared the recover watermark W′ with original watermark W, if they are identical then the corresponding block is authenticate otherwise it is unauthenticated (i.e. tampered with).The alterations in the authentication mark can be clearly identified, and the tampered area(s) is localized by using algorithm (2.3), tamper detection process illustrated in figure (6)

Algorithm (2.3) Tampers detection process

Input
Watermarked image as origin
Original watermark as W
Recover watermark as W'

Output
Tamper detection and localization

Remark
This algorithm is used for tamper proofing with a received or tampered image.

Procedure
Step: 1origin ← imread ('c:\ ewatermark.bmp'); // read a watermarked image (received image)

Step: 2 water ← imread (' c: \ watermark.bmp'); // read original watermark

Step: 3 nmark ← imread ('c: \ nmark.bmp'); // read a new recove watermark

Step: 4 great a new array that represent the differences between water and namrk arrays.

Step: 5 tamper detection process
For I ← 1: 256
For J ← 1: 256
if diff (I,J) equal to zero than tamper detection and localized

Else (if)
End;
End;
End;

Before we going fare-off with tamper detection with unintended attack those particularizations in the next presentation, we should know a technique that used for image authentication proofing, the next figure illustrate authenticate proofing operation:

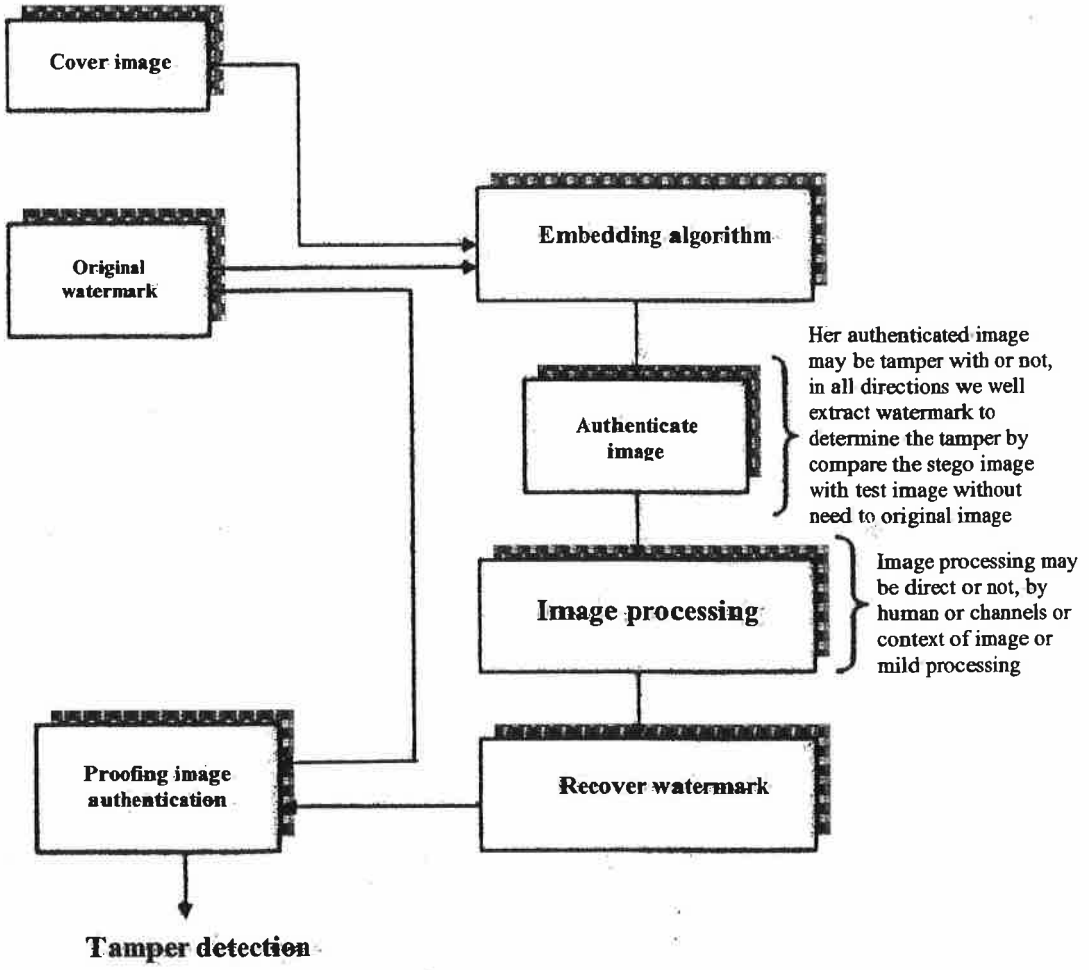

Figure (6) Tamper detection and authentication proofing

3. Results and Discussion

The method was tested using different natures (texture) of 24bits color 256 * 256 image (i.e. H=256, W=256).

3.1 Performance measures

The using of PSNR(peak signal to noise ratio) help us to asses the effect of proposed method on the objective quality for the watermarked image (WI), this function computed from the next equation:

$$PSNR = 10 \log_{10} \frac{(R)^2}{MSE} \quad \text{---------- 2}$$

When the value of MSE computed from the equation (1). In the previous equation, R represents the max. Flections in the input image data type. For example: if the input image has a double – precision floating data type then R is 1 , if it has an 8-bit unsigned integer data type (unite8) than R is 255,... Etc [12].

3.2 performances under no attack

Before any attack we computed the MSE function between W and W' to gain the value of it , for the samples that used in the proposed method, this value help us to determine the changing in it (WI) after attack, table(3) illustrate this state.

3.3 performances under attack

When the watermarked image is under attack, it will be affect by it, but there are differences between attacks or tamper types, such as intended or unintended.

The intended tamper will change the general features of the image to produced an authenticate image (illegal image or tampered image),

for example (when the user add or remove an features of original image), another intended attacks such as resizing, scaling, modify, change image color space,...etc. But an intended attack or tamper mean that the changing on the digital signal is not aimed to produce illegal or an authenticate image, but it occurred unintentionally direct or indirect, by human or program or under net channel effect. Therefore we should gain an idea that could distinction between intended and an intended attack, if it could do this function, then it will be a smi-fragile watermark, otherwise it will be a fragile watermark. This idea we will highlight it in the stunt comer later.

3.3.1 under intended attack

Intended attack mean all types of image processing that modify or change image features to produce an authenticate image called tampered image. The aim of this operation is illegal, it produced digital media different from original media (image). Therefore the needing for mechanism is now very important for tamper proofing and detection with localize a tamper area. The proposed method has ability to discover and localize any intended attack, the figures (9, 10) show us this state.

3.3.2 under unintended attack

We know the ability of proposed method for tamper proofing and detection, and then we know an idea about this ability for tamper detection. now we moved to a new and important stage of evaluation the performance of proposed system to be our guide about the watermark that used in the work if it is a semi-fragile watermark or not, through exposing them to several unintended attacks such as :-

1- Compression operation test, table (4) illustrates it.

2- Copy – past operation test, table (5) illustrate it.

3- Transmission test, table (6) illustrates it.
4- Convert file type operation test, table (7) illustrate it.

4. Results

The next presentations highlight the results that we gained after performed the proposed method, tables and figures illustrated all states for this proposed method, the details illustrate in the conclusion section.

Table (2) The value of PSNR after embedding operation

PSNR between original image and watermarked image 256*256/BMP color image	
Image name	PSNR
Lena	**51.1115 DB**
Child	**51.1197 DB**
Poor	**51.0695 DB**

Table (3) The value of MSE for test image before any attack

MSE between original watermark and recover watermark		
Image name	Image peculiarity	MSE
Lena	**Standard**	**0.0000**
Child	**Digital**	**0.0001**
Poor	**Painted**	**0.0055**

Table (4) The value of MSE after compression attack between W and W'

Image name	Compression type WinRAR	CR	MSE
Lena	Store	%100	0.0000
	Fastest	%71	0.0000
	Fast	%70	0.0000
	Best	%62	0.0000
Child	Store	%100	0.0001
	Fastest	%76	0.0001
	Fast	%75	0.0001
	Best	%50	0.0001
Poor	Store	%100	0.0055
	Fastest	%78	0.0055
	Fast	%76	0.0055
	Best	%50	0.0055

Compression ratio refers to the degree of image file size reduction due to compression process. This measure is determined as the ratio between the sizes of the original uncompressed image file to the size of the overall compressed data file [10].

$$C_r = \frac{uncompressedfilesize}{compressedfilesize}, \text{----------} \quad (3)$$

And it is often written as Size U: Size C. The (C_r) parameter is an indicator for the compactness ability of the compression process. The

other measures may be used to describe the achieved reduction in data size due to compression (compression factor, and bit rate). The next figure (7) show us the best sample in this test, we depend on MSE value from previous table that computed between W' and W.

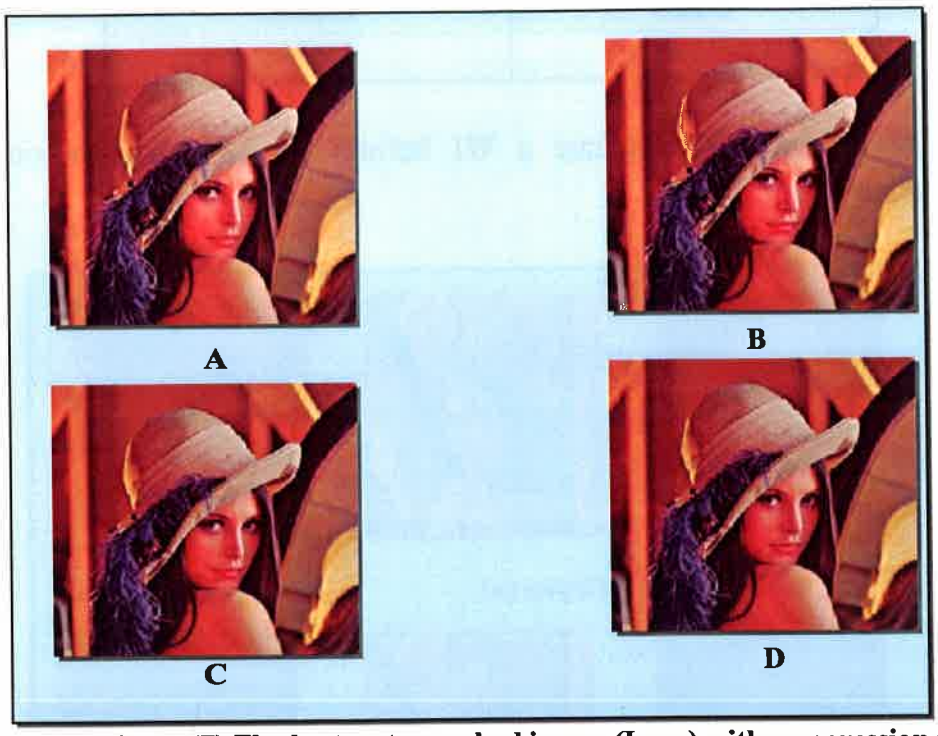

Figure (7) The best watermarked image (Lena) with compression test (A) Fastest CR, (B) Fast CR, (C) Store CR, (D) Best CR

Table (5) The value of MSE after copy – past attack between W and W′

Image name	MSE
Lena	0.0000
Child	0.0001
Poor	0.0005

Table (6) The value of MSE after transmissions attack between W and W′

Image name	MSE
Lena	0.0000
Child	0.0001
Poor	0.0055

The next figure (8) illustrate a WI before and after transmission operation:

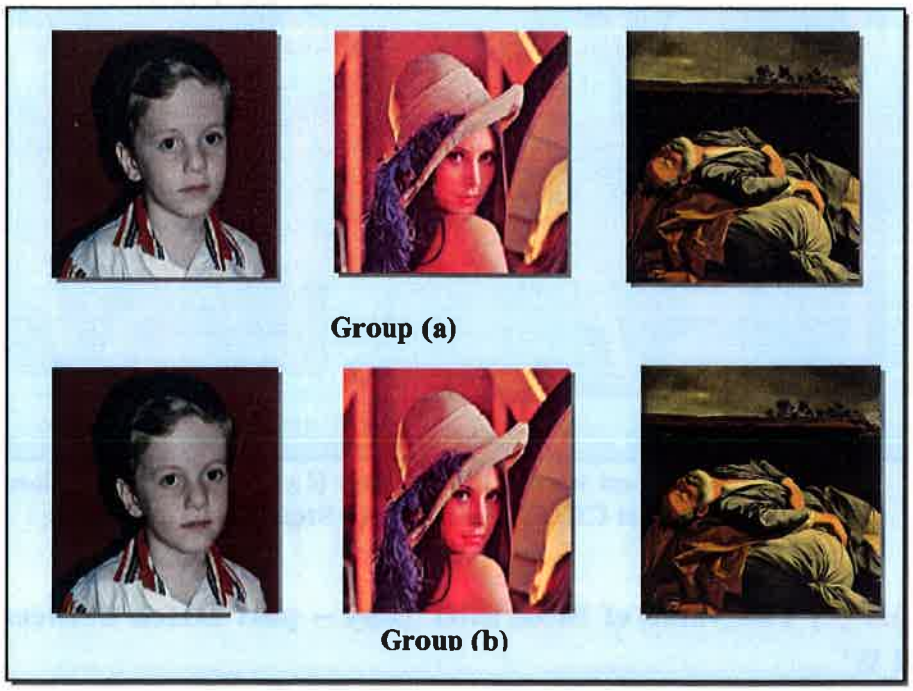

Figure (8) Transmission process
(a) Represent a watermarked image group before transmission
(b) Represent a watermarked image group after transmission

Table (7) The value of MSE after converting the watermarked image to other format between W and W'

Image name 192 KB	New format	Size in KB	MSE
Lena	JPEG	54.9	30.0509
	TIFF	201	0
	PNG	136	0
	GIF	24.4	99
Child	JPEG	48.6	29.136
	TIFF	177	0
	PNG	146	0
	GIF	17.4	99
Poor	JPEG	60.0	30.5975
	TIFF	189	0
	PNG	150	0
	GIF	24.4	99

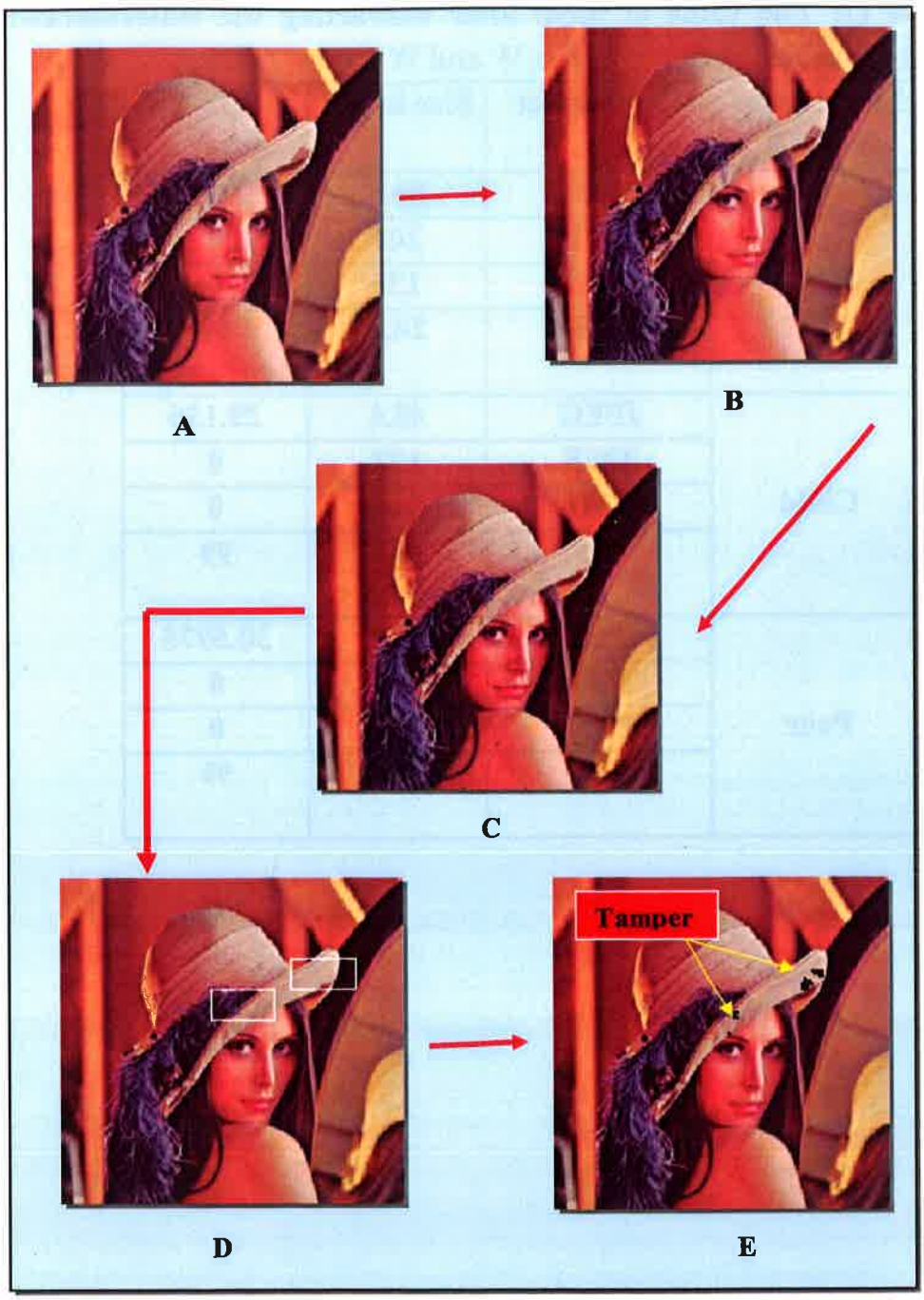

Figure (9) Tamper detection and localization with standard image (Lena)

(A)Original image (B) Watermarked image (C) Tampered image (D) Tamper localized (E) Tamper detection

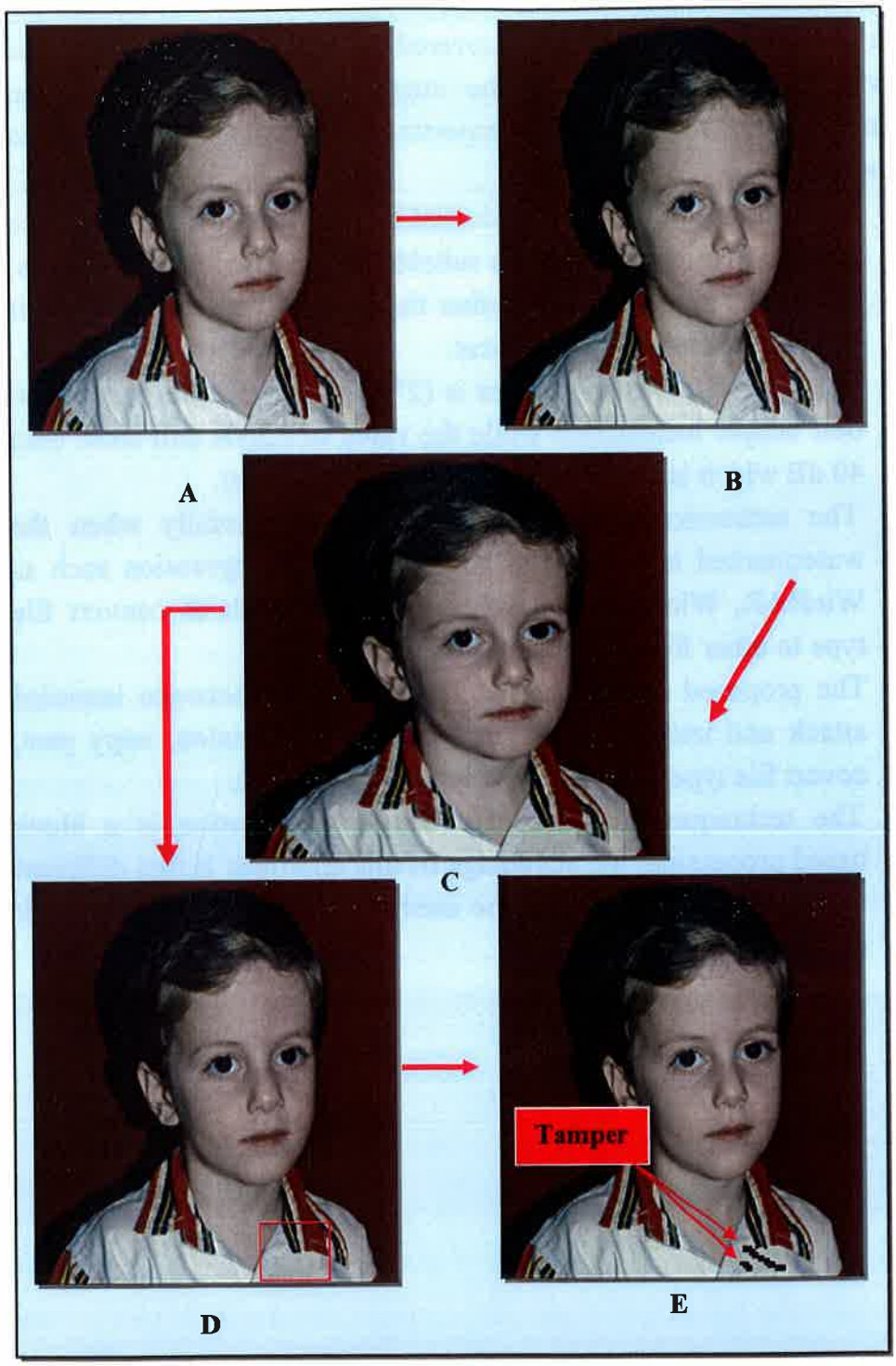

Figure (10) Tamper detection and localization with digital image (Child)
(A)Original image (B) Watermarked image (C) Tampered image (D) Tamper localize (E) Tamper detection

5. Conclusions

The previous discussions have covered some remarks related to the behavior and performance of the suggested image authentication system. A summary of some important conclusions could be the following:

1- The results of the tests, conducted in this work, confirm the idea that the frequency domain is suitable for watermark applications, like image authentication, rather than spatial domain, because, it make the watermark robustness.

2- The optimal partition number is (2*2) parts, because it gives the best tamper localization while the value of PSNR still more than 40 dB which is acceptable (image authentication).

3- The authentication mark is extracted successfully when the watermarked is exposed to some types of compression such as WinRAR, WinZip and another operations such as convert file type to other file type, transmission, copy-paste.

4- The proposed method has ability to disunite between intended attack and unintended attack such as transmission, copy past, covert file type to another file type, compression.

5- The techniques that used for tamper localization is a block based processing; the advantage of this approach is that different watermark information can be used for each block thus giving it more flexibility.

6. Reference:

[1]. C. S. Lu and H. Y. M. Liao, "***Multipurpose watermarking for image authentication and protection***," IEEE Transactions on Image Processing, 2001, 10(10), pp. 1579-1592

[2]. C. K. Ho and C. T. Li. "**Semi-*Fragile Watermarking Scheme for Authentication of JPEG Images***," International Conference on Information Technology: Coding and Computing (ITCC 04), vol. 1, 2004, pp. 7-11

[3]. M. Barni, F. Bartolini, V. Cappellini and A. Piva, "***A DCT-Domain system for robust image watermarking***," Signal Processing, 1998, 63(3), pp.357-372.

[4]. P. W. Wong and N. Memon. "***Secret and public key image watermarking schemes for image authentication and ownership verification***," Image Processing IEEE Transactions, 2001, 10(10), pp. 1593-1601.

[5]. X. Q. Li and X. Y. Xue, "***Fragile authentication watermark combined with image feature and public key cryptography***," 7th International Conference on Software Process (ICSP 04), Aug, 2004, pp. 2286-2289

[6]. C. T. Li, and F. M. Yang, "***One dimensional neighborhood forming strategy for fragile watermarking***," Journal of Electronic Imaging, vol. 12, No. 2, 2003, pp. 284-291.

[7]. C. T. Li, "***Digital Fragile Watermarking Scheme for Authentication of JPEG Images***," Proc. of IEE on Vision, Image and Signal Processing, vol. 151, 2004, pp.460-466

[8]. Z. M. Lu, C. H. Liu, D. G. Xu and S. H. Sun, "***Semi-Fragile Image Watermarking Method Based on Index Constrained Vector Quantization***," IEEE Electronics Letters, vol. 39, 2003, pp. 36-37

[9]. C. H. Lin, T. S. Su and W. S. Hsieh, "***Semi-Fragile Watermarking***

Scheme for Authentication of JPEG Images," Tamkang Journal of Science and Engineering, vol. 10, No 1, 2007, pp.57-66

[10]. Umbaugh, S. E, "***Computer Vision and Image Processing: A practical Approach using CVIP Tools***", Prentice Hall,1998, Inc. 1

[11]. Kutter, M., and Petitcolas, F, A., "A ***Fair Benchmark For Image Watermarking System*** ", Security and Watermarking of Multimedia Content, SPIE-3657 1999, PP. 226-239.

[12]. Matlab help.