Hiding Three Images at one image by Using Wavelet Coefficients at Color Image

Haidar M. Abdul-Nabi ; Emad S. Al-Shawi and Hussain L. Hussain

Dept. of Computer Science, College of Science, University of Basrah, Basrah ,Iraq

Abstract:

Information hiding is a general term that can be implemented using several techniques that should insure that concealed data would be invisible to the naked eye. Nowadays, two science of data hiding have been emerge, *steganography* and *watermarking*.

The proposed method deals with hiding information (three images) in other media (one image) using frequency domain by the wavelet coefficients.

Keywords: Image, Watermarking, Steganography, Frequency Domain, Wavelet.

1.Introduction:

Color images can be modeled as three-band monochromes image data as show in figure (4), where each band of data corresponds to different color [1]. The `actual information stored in the digital data is the brightness information in each spectral band. It is easily understood that placing a watermark imperceptibly insignificant components of an image causes imperceptible distortions to the watermarked image. The watermark should be integrated with the image content, so it cannot be removed easily without severely degrading the image. The watermark can be made invisible to the human eye, but still readable by computer. [2]

2.Aim of Research:

The aim of the research is to design a new method to hiding information (3 images) in one image, and the human eye cannot recognize them by using the intermediary coefficients of frequency domain. The proposed method deals with black and white images and color images.

3. Basic Concepts:

Wavelet Transform:

The wavelet transform is really a family of transforms that satisfy specific conditions. It can be described as a transform that has basis functions that are shifted and expanded versions of them.

The wavelets transform breaks an image down into four sub sampled or decimated images. They are sub sampled by keeping every other pixel. The results consist of one image that has been high pass filtered in both the horizontal and vertical directions. [3]

Wavelet Analyses

Intruder to perform the wavelet Analyses, a numerous filters can be used to implement the wavelet transform by first convolving them with the rows and then the columns by doing the following as shown in figure (1)

1. Convolve the low pass filter with the rows and save the results.

2. Convolve the low pass filter with the columns (of the results from step1) and sub-sample this result by taking every other values; this gives us the lowpass-lowpass version of the image .

3.Convolve the result from step1, the lowpass filtered rows,with the highpass fi

4. lter on the columns . Subsample by talking every other values to produce the lowpass- highpass image .

5.Convolve the host image with the highpass filter on the rows and save the result .

6.Convolve the result from step (4) with the lowpass filter on the columns ; subsample to yield the highpass-lowpass version on the image .

7.To obtain the high pass-high pass version, convolve the columns of the result from step (4) with the high pass filter. As an image, is shown in figure (1&2) [4, 5]

Figure (1): Wavelet Segments for Image

LL **(Low-Low)**	**HL** **(High-Low)**
LH **(Low-High)**	**HH** **(High-High)**

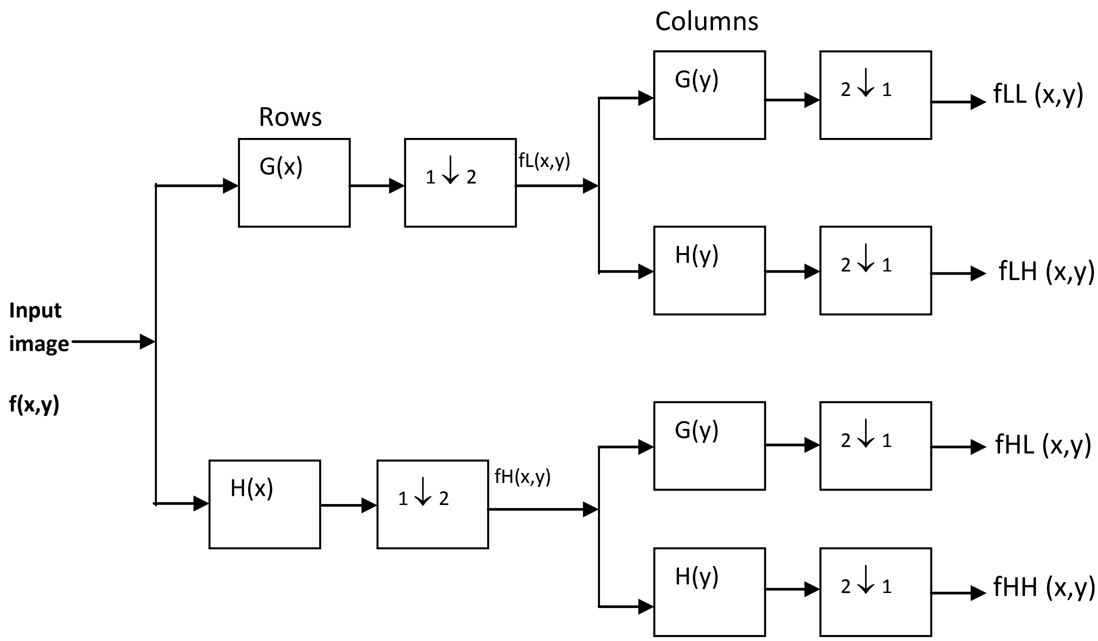


Figure (2): Wavelet Analyses for Image

Hiding Information:

Features :

Data-hiding techniques should be capable of impending data in a host signal with the following restrictions and features:[6]

1-The host signal should be none objectionally degraded and the embedded data should be minimally perceptible.

2- The embedded data should be directly encoded into the media, so that the data remain intact across varying data file formats.

3- The embedded data should be immune to modifications ranging from international and intelligent attempts at removal to anticipated manipulations, e.g. filtering, resembling, encoding and analog-to-digital (A/D) conversion, etc.

4-Asymmetrical coding of the embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access.

5- Error correction coding should be used to insure data integrity. It's inevitable that there will be some degradation to the embedded data when the host signal is modified.

6- The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered when only fragments of the host signal are available.

Applications:

Placing data in images is useful in a variety of applications. We highlight below the most important application its digital watermark. The objective of digital watermark is to place an indelible mark on an image. Usually, this means encoding only a handful of bits, sometimes as few as one. This "signature" could be used as means of tracing the distribution of images for an on-line service and four photographers how are selling their work for digital publication. [7]

Watermarking system deals with two steps:

Hiding Image Embedding Process:

The input hiding process consists of a hidden images (or encrypted images) and cover media. The embedded hidden images must be invisible to human eyes and robust to most images processing operations. To meet these requirements, a pixel value (0 or 1) is embedded in a block of the image. Before insertion, the host images is decomposed into N*N blocks. Depending on the contrast of a block, pixels in the block are adaptively modified to maximize robustness and guarantee invisibility. [8]

Hiding Image Extraction Process:

The extraction of a hidden image is similar to embedding while in a reverse order. The extraction of a hidden image must make reference to the original host image. [8]

4. The proposed Technique:

The Embedding Algorithm:

1. Read the original image, or host image (H), and read the hidden images (A1, A2, A3).

2. Divide the Host image (H) into blocks of N*N pixels.

3. Divide the hidden images (A1, A2, A3) into blocks of N*N pixels.

4. Transform the host blocks into frequency domain using wavelet method.

5. Chose the intermediary wavelet coefficients and then replace it with the pixel values of the hidden image blocks values.

6. Transform the host blocks from frequency domain to the spatial domain.

7. Assemble the host blocks to produce an image with hidden image (HA) as shows in Figure (5).

The Extraction Algorithm:

1. Read the image (HA) produced from the embedding algorithm. And Read the original image or host image (H).

2. Divide the image (HA) into blocks of N*N pixels.

3. Divide the original Image (H) into blocks on N*N pixels.

4. Transform the image (HA) blocks into frequency domain using wavelet transform method .

5. Transform the original Image (H) blocks into frequency domain using wavelet transform method.

6. Take the chosen intermediary frequency coefficients from the Image (HA) and intermediary frequency coefficients from the Image (H) to produce the original hidden Images (A1, A2, A3). As shown in figure (6).

7. Assemble the hidden images (A1, A2, and A3) blocks to produce the hidden image (A1, A2, A3). As shown in figure (6).

5. Experimental Results:

Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a reconstructed image with the original image. For an 8-bit grayscale image, the peak signal value is 255. Hence the PSNR of an M×N 8-bit grayscale image x and its reconstruction $\hat{x}$ is calculated as [9]

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad \text{…… (3)}$$

where the Mean Square Error (MSE) is defined as:

$$MSE = \frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left[x(m,n)-\hat{x}(m,n)\right]^2 \qquad \text{…… (4)}$$

Figure (7) shows the host images and the hidden images using the proposed algorithm. Figure(8, 10, and 12) shows the experiments using the host images with three hidden B&W images and the PSNR that results from this experiments, while Figure (9, 11, and 13) shows the experiments using the host images with three hidden colored images and the PSNR that results from this experiments.

The Experiments:

The results of the experiments are showed as the following:

Experiment (1): Deals with embedding the black and white images (A1, A2, and A3) in the Host image (H1), and the result measuring using PSNR given in the table (1) as shown below.

Table (1) The Results of experiment(1)

Host Image No.	Hid Image No.	PSNR (dB)
H1	**A1(B&W)**	**65.4317**
	A2(B&W)	
	A3(B&W)	

Experiment (2): Deals with embedding the color images (C1, C2, and C3) in the Host image (H1), and the result measuring using PSNR given in the table (2) as shown below.

Table (2) The Results of experiment(2)

Host Image No.	Hid Image No.	PSNR (dB)
H1	**C1(Color)**	**42.1335**
	C2(Color)	
	C3(Color)	

- Experiment(3):

Table (3) The Results of experiment(3)

Host Image No.	**Hid Image No.**	**PSNR (dB)**
H2	**A1(B&W)**	**65.4134**
	A2(B&W)	
	A3(B&W)	

- Experiment(4):

Table (4) The Results of experiment (4)

Host Image No.	**Hid Image No.**	**PSNR (dB)**
H2	**C1(Color)**	**42.1195**
	C2(Color)	
	C3(Color)	

- Experiment(5)

Table (5) The Results of experiment(5)

Host Image No.	Hid Image No.	PSNR (dB)
H3	A1(B&W)	65.416
	A2(B&W)	
	A3(B&W)	

- Experiment(6)

Table (6) The Results of experiment (6)

Host Image No.	Hid Image No.	PSNR (dB)
H3	C1(Color)	42.1194
	C2(Color)	
	C3(Color)	

6. Conclusions:

The implementation of this method is applied on two types of images: Black and white images, and Colored image.

The experiments shows the ability of the proposed algorithm to embed the hidden image in an efficient manner by achieving the hiding information requirements that showed below, and the experiments explain the results for color image almost is rather similar to the result of the black and white images.

1. **Transparency**: The proposed algorithm provides a high degree of transparency that the HVS does not recognize the hidden images that embedded in the original image. And this can be achieved by choosing the embedded locations which are far from the low frequency locations (blocks energy).

2. **Capacity**: The proposed algorithm has a high capacity that can reach the quarter of the original image size because the method uses the wavelet that divide the image into four parts. The hidden images can be embed in the (4, 8, 16) locations at least in each block (8*8=64 locations).

3. **Security**: The important requirement that must be provided in the system by embed the hidden images in the appropriate frequency domain coefficients and produce an embed image with good PSNR value.

7- References

[1]:SCOTT.EUMBAUGH ,"Computer vision and image processing", Prentic Hall PTR,1998.

[2]:JIRI FRIDRICH and M. Goljan, "Comparing Robustness of watermarking Techniques", PIE security and watermarking of multimedia content. Sanjose, CA.

[3]:ROBI.POLIKAR ,"Fundamental concepts and an overview of the wavelet theory", second edition,1999.

[4]:AL-OBAIDI H. H. "Encryption Using Wavelet Code Image Data", M.Sc. Thesis, Computer Engineering department , College of Engineering , Basrah University, June 2004.

[5]:KJOELN, A., "Wavelet based compression of skin tumor images" ,Master's thesis in electrical engineering southern Illinois university at Edward Svill, 1995.

[6]:W.Bender, D.Gruhl, N. Monmoto, A. Lu, "Techniques for data hiding", IBM system journal, Vol 35, Nos 384, 1996.

[7]:A. T, S. HO, J. Shen ,and S. H. Tan , "Character embed watermarking algorithm using the fast Hadamard transfer for satellite images" , Procsplt 4293 , 2002.

[8]:COX, I. , M. Miller and J. Bloom , "Digital watermarking ", Morgan Kaufman ,publishers ,2001.

[9] M.Rabbani and P.W.jones, "Digital image compression Techniques", VolTT7,SPIE Optical Engineering Press, Bellvue, Washington(1991).

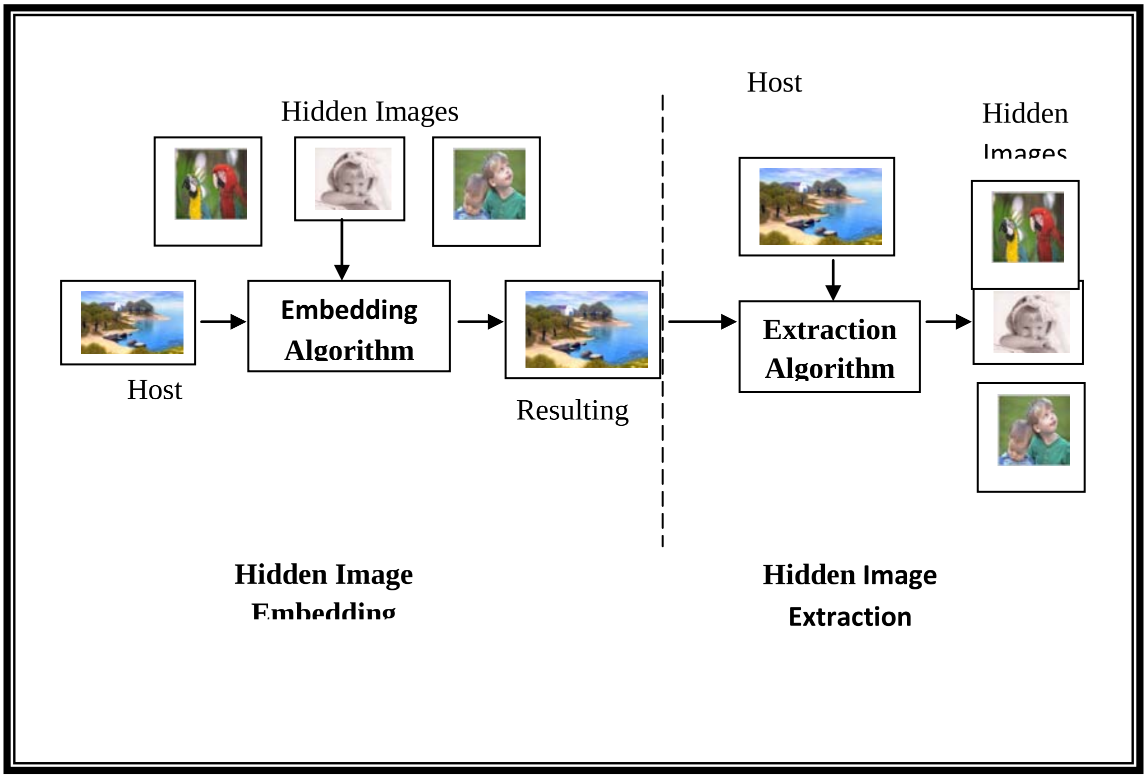


Figure (3): Embedding and Extraction Image

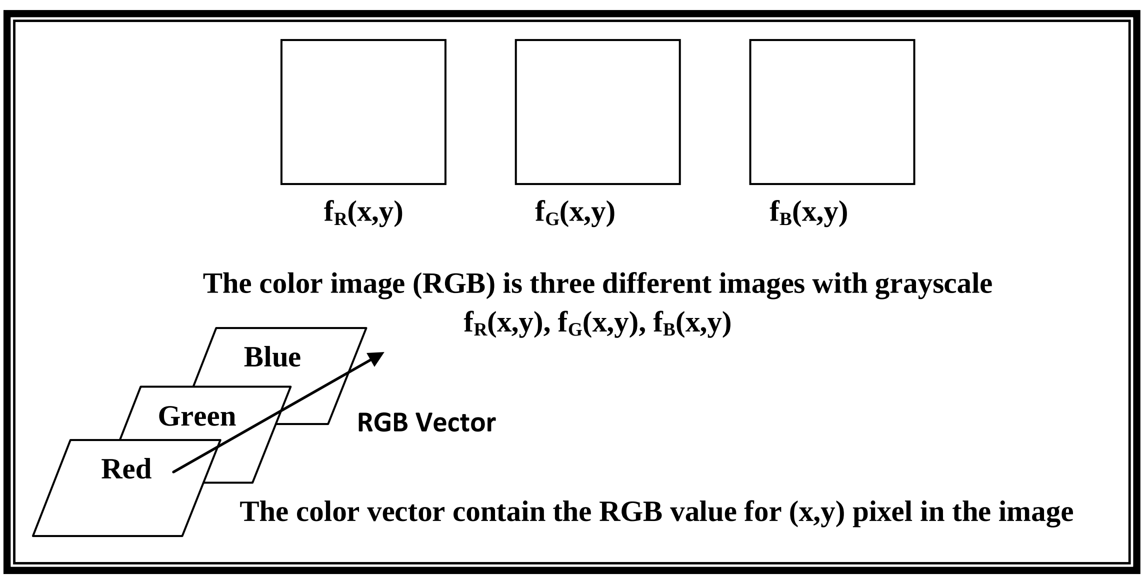
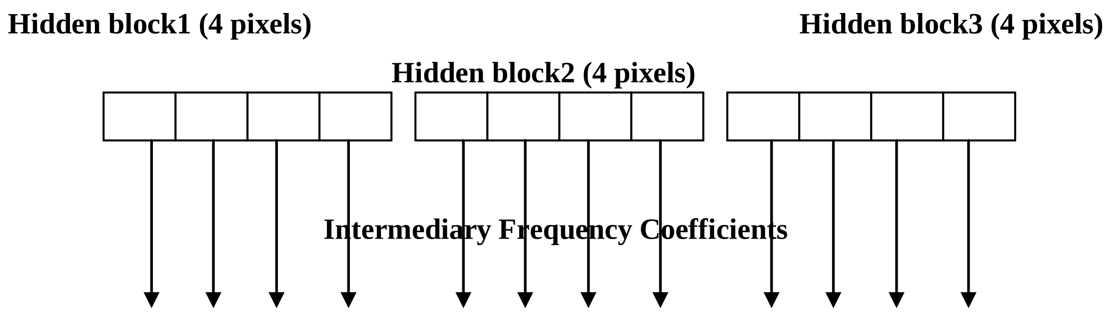


Figure (4): Representation of color image.



0	1	…	8	…	16	…	24	…	32	…	63	R
0	1	…	8	…	16	…	24	…	32	…	63	G
0	1	…	8	…	16	…	24	…	32	…	63	B

Figure (5): The Embedding Stage.

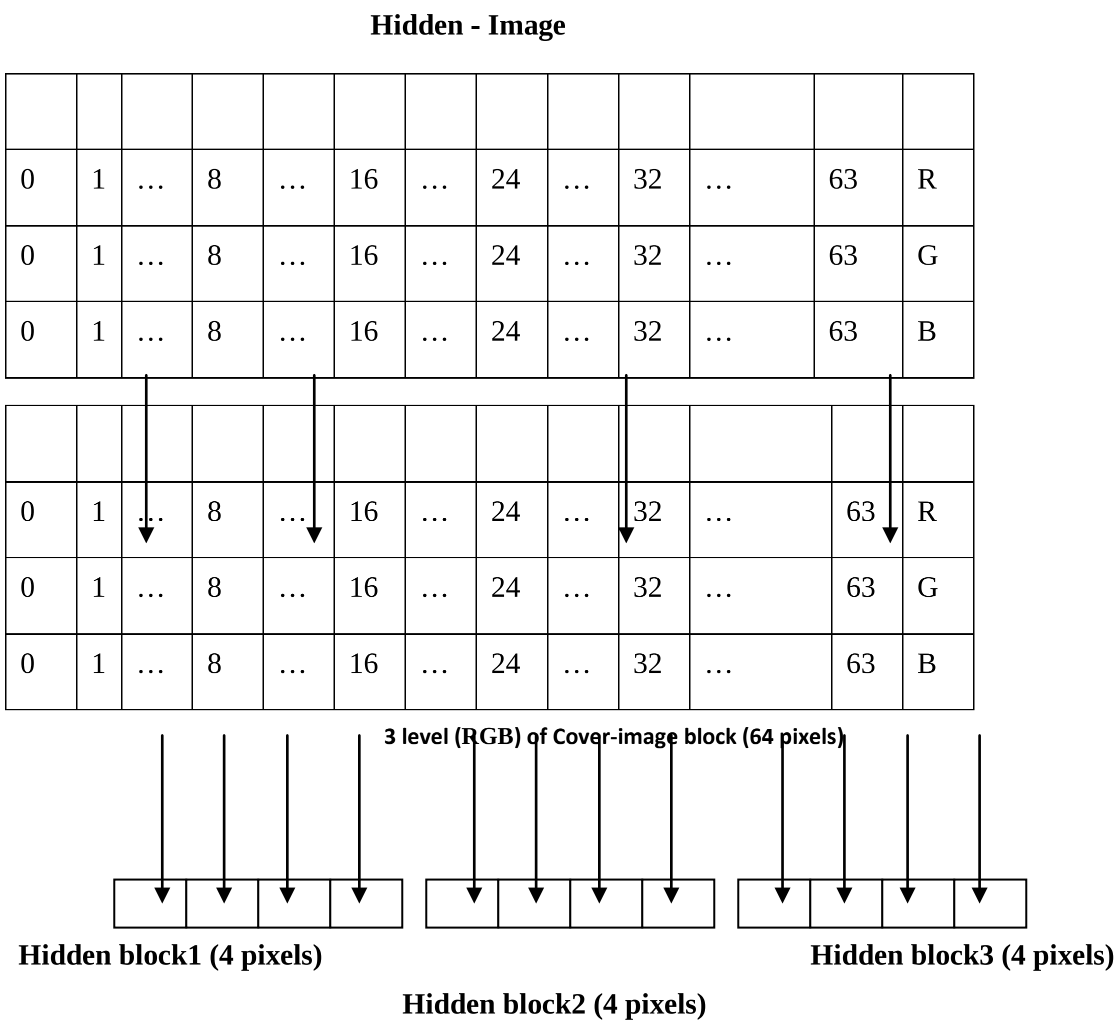
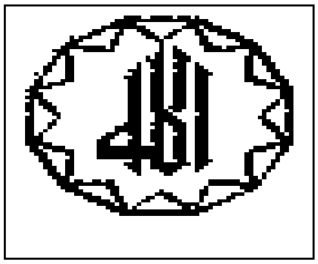


Figure (6): The Extraction Stage.

Host Image (H1) 1024*768

Host Image (H2) 1024*768

Host Image (H3) 1024*768



Hidden Image (A1) 128*128

Hidden image (A2) 128*128

Hidden image (A3) 128*128

Hidden Image (C1) 128*128

Hidden image (C2) 128*128

Hidden image (C3) 128*128

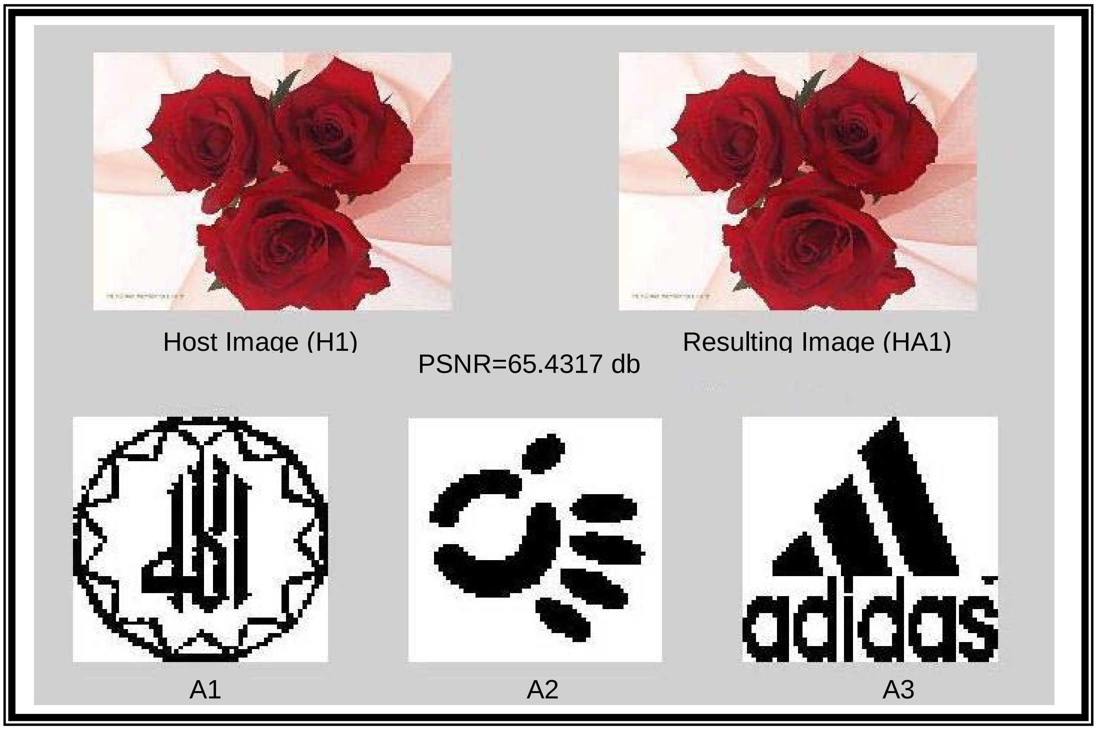


Figure (8): The Result of Experiment (1).

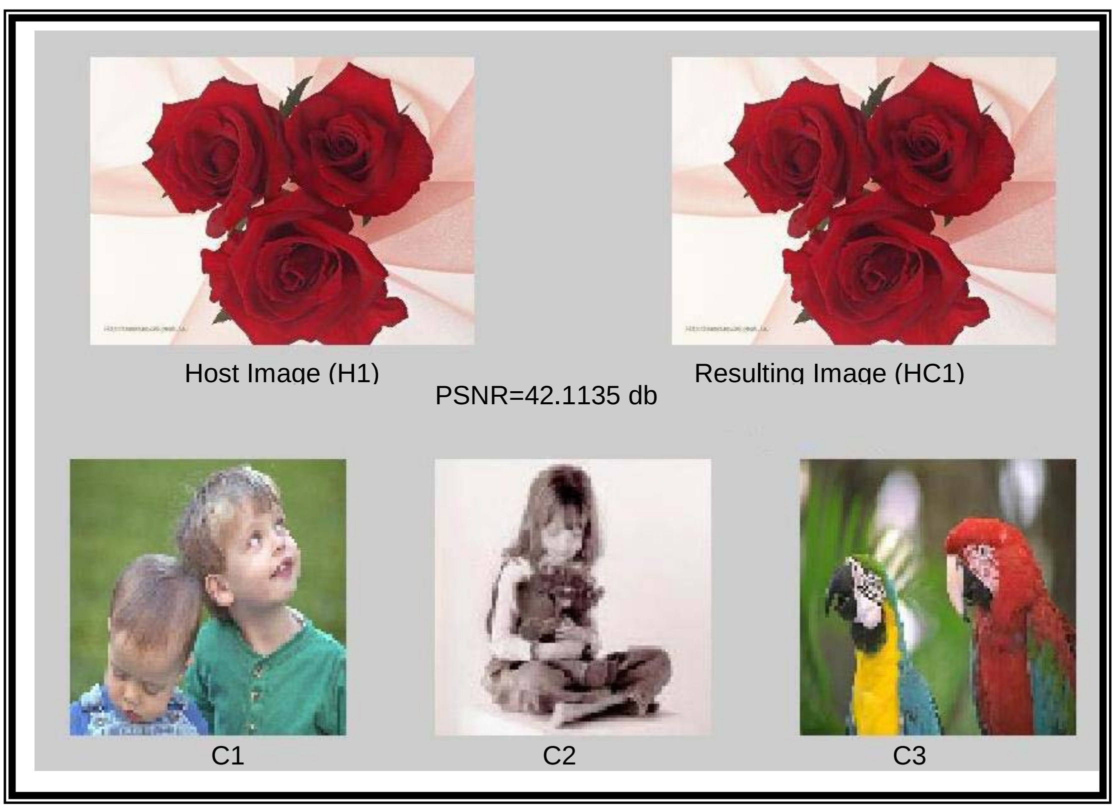


Figure (9): The Result of Experiment (2).

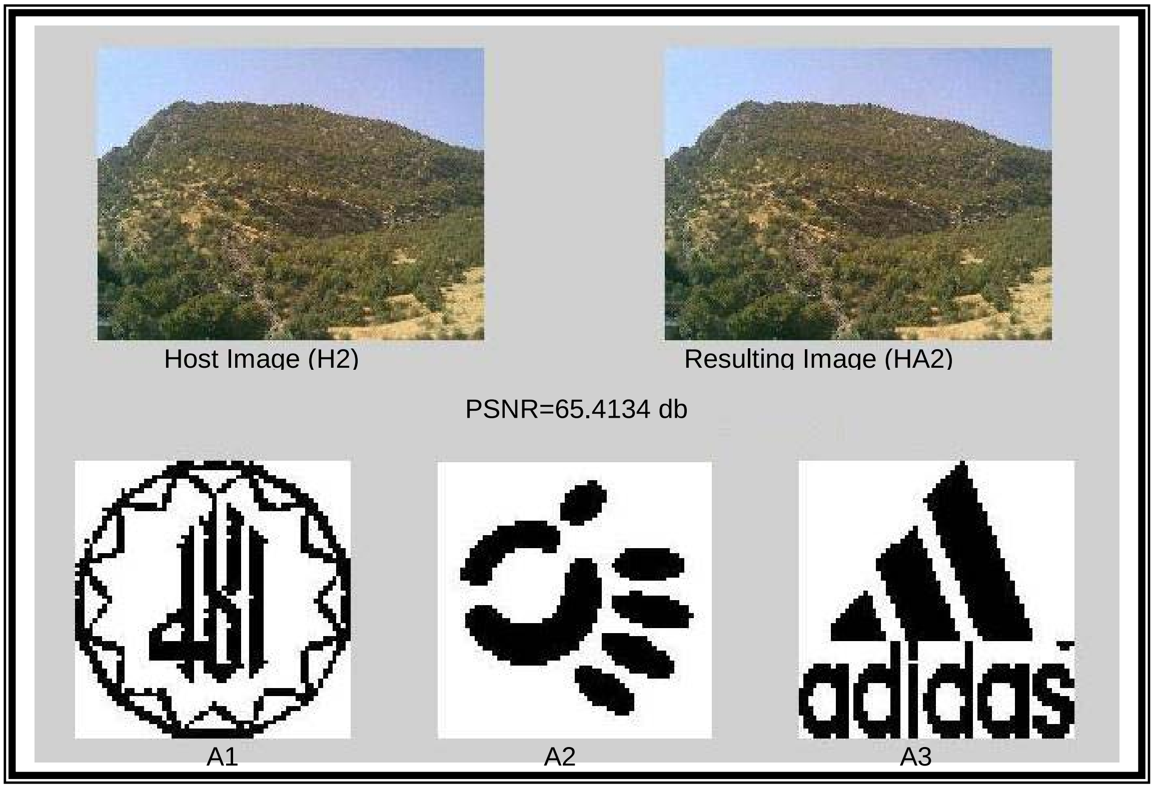


Figure (10): The result of experiment (3).

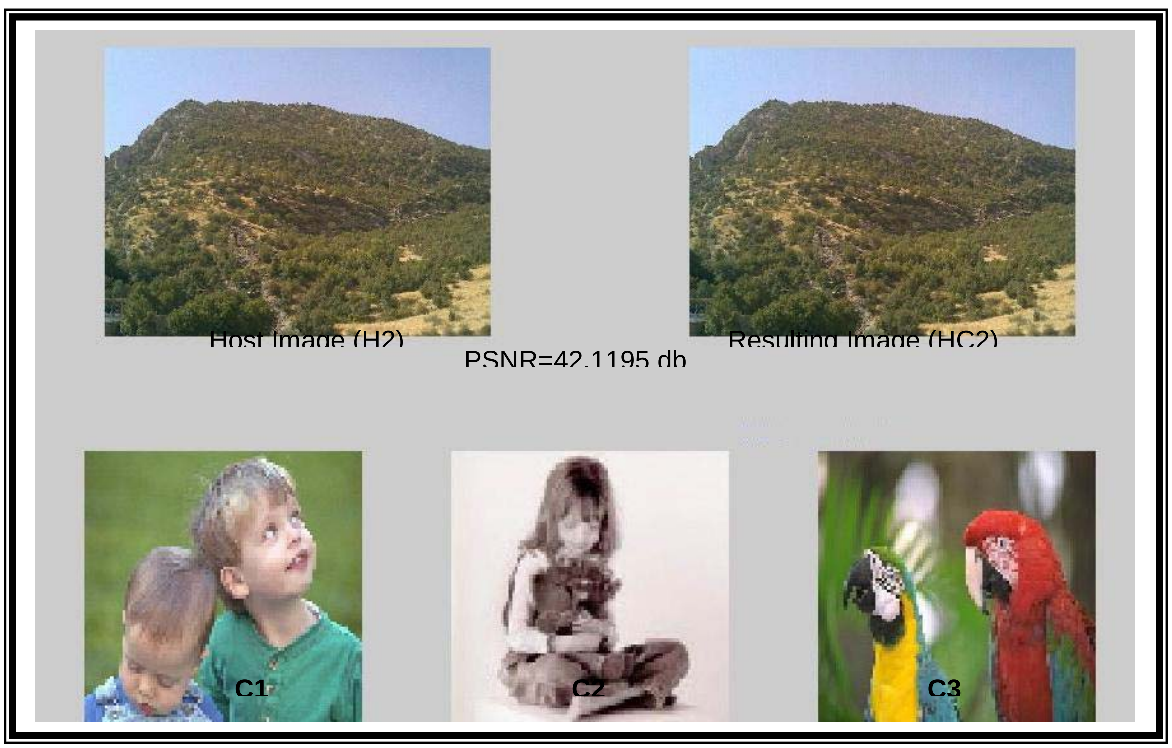


Figure (11): The result of experiment (4).

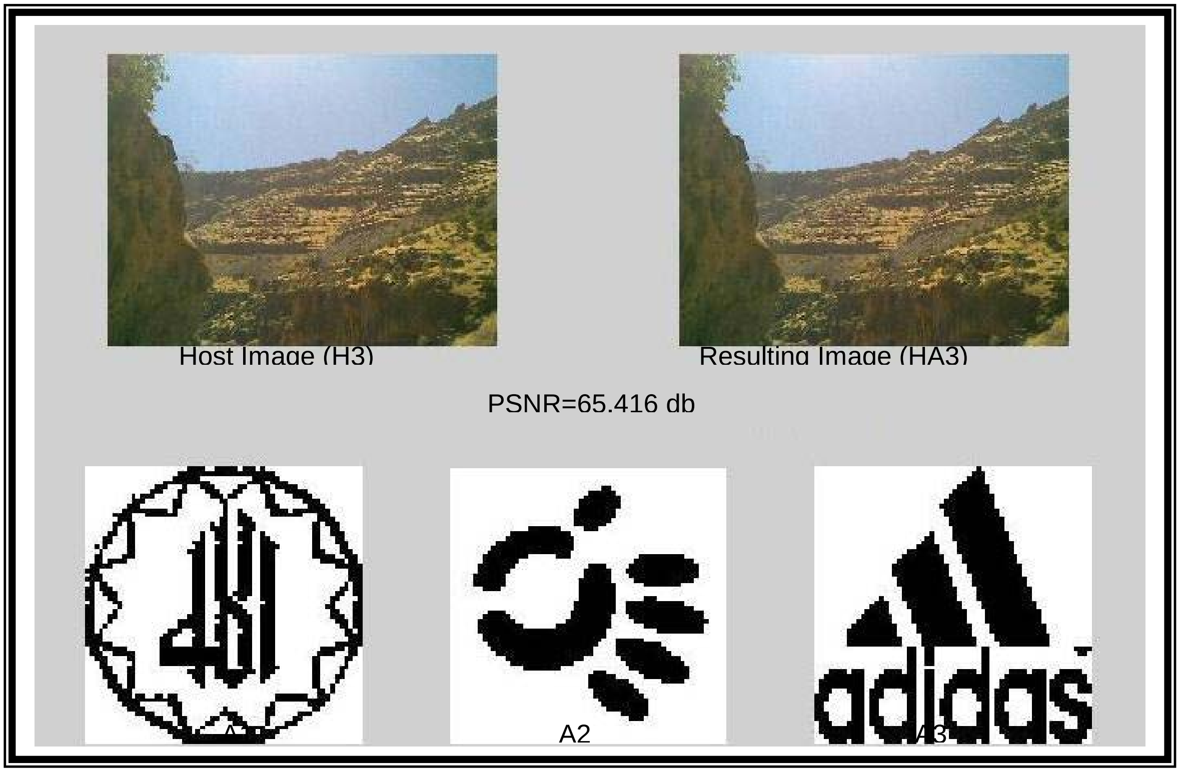


Figure (12): The result of experiment (5).

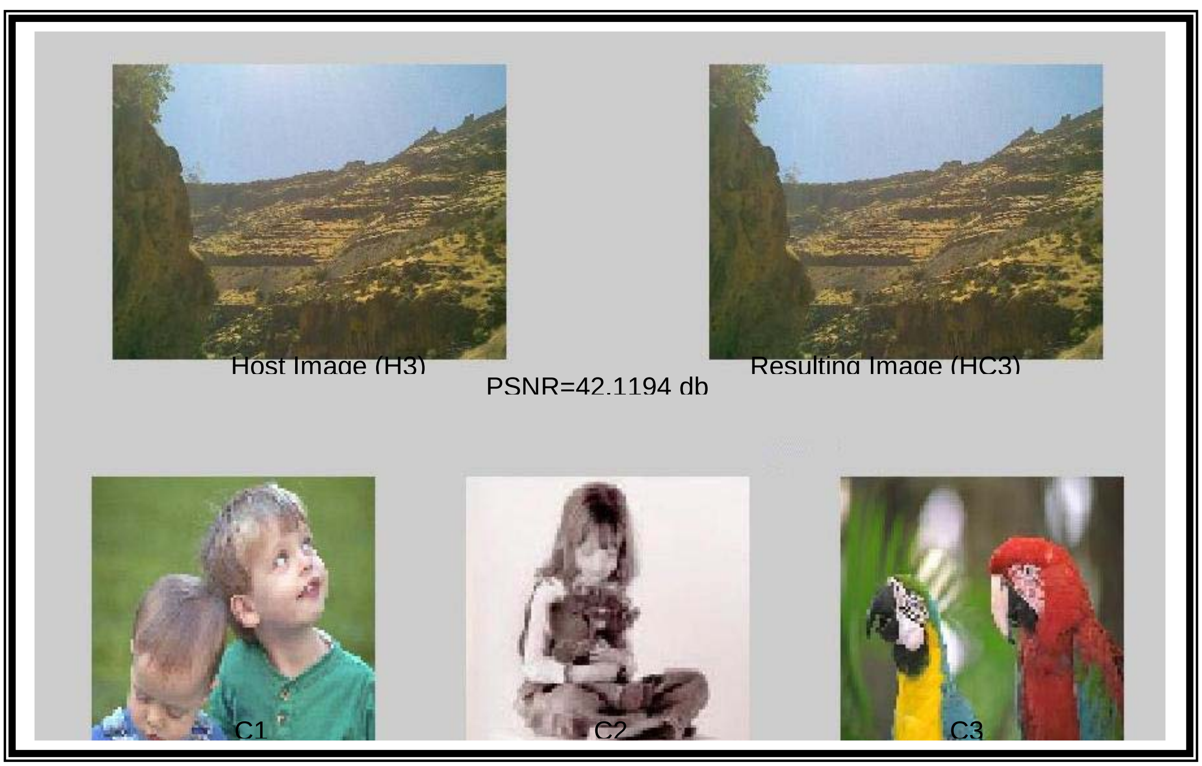


Figure (13): The result of experiment (6).

إخفاء ثلاث صور في صورة واحدة باستعمال التحليل المويجي للصور الملونة

حيدر محمد عبد النبي وعماد شعلان الشاوي و حسين لفته حسين

جامعة البصرة – كلية العلوم – قسم علوم الحاسبات – البصرة – العراق .

المستخلص

اخفاء المعلومات هو مصطلح عام يمكن ان يطبق باستعمال عدة تقنيات والتي تضمن إن البيانات المخفية يجب ان تكون غير مرئية للعين المجردة. في الوقت الحاضر تم التركيز على نوعين أساسيين من طرق اخفاء البيانات هما الكتابة المخفية Steganography والعلامة المائية Watermarking.

الطريقة المقترحة في بحثنا هذا تتعامل مع إخفاء المعلومات (ثلاث صور) في صورة ملونة واحدة باستعمال معاملات المجال الترددي.

الكلمات المفاتيح: صورة، العلامة المائية، الكتابة المخفية،المجال الترددي، التحويل المويجي.