AN ADAPTIVE IMAGE STEGANOGRAPHY COMPRESSION METHOD BASED ON DWT

Saleh.M. Ali, Saif.B. Al-khoja and Nabeel.J. Tawfeeq

Remote Sensing Research Unit, College of Science, University of Baghdad, Baghdad- Iraq.

Abstract

Steganography is the art of hiding messages in an unsuspected cover. The aim of this paper is to hide larger number of multi messages inside one cover image depending, using the low-low-block-features **LLBF** of wavelet transformation. The method of embedding messages based on Least-Significant-Bit (**LSB**) of cover image. The imperceptibility of the messages and cover images is assessed by using the Mean- Square-Error (**MSE**), the peak signal to noise ratio (**PSNR**) and the image histogram.

طريقة ضغط وإخفاء مطورة للصور تعتمد التحويل المويجي

صالح مهدي علي، سيف بشير الخوجة، نبيل جميل توفيق.

وحدة الاستشعار عن بعد، كلية العلوم، جامعة بغداد. بغداد – العراق.

الخلاصة

إن علم الاختزال هو فن إخفاء الرسائل في وعاء بعيد عن الشك. الهدف من البحث هو إخفاء أكبر عدد من الرسائل داخل صورة واحدة اعتمادا على تبني معاملات الترخيم الواطئة للتحويل المويجي. أما طريقة التضمين للرسائل فكانت باستعمال تقنية الحشر Least Significant Bit ، كما أستعمل معيار معدل مربع الخطأ و معيار نسبة قمة الإشارة إلى الضوضاء فضلا عن المخطط التكراري للصور.

Introduction

Stenography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of Stenography is to hide the *presence* of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the *content* of a message. A famous illustration of the Stegano- graphy is the Simmons' "Prisoners' Problem" [1]: Alice and Bob are in jail, locked up in separate cells far apart from each other, and wish to devise an escape plan. They are allowed to communicate by means of sending messages via trusted couriers, provided they do not deal with escape plans. But the couriers were agents of the warden Eve (who plays the role of the adversary here) and had leaked all communication to her. If Eve detects any sign of conspiracy, she would spoil the escape plans by transferring both prisoners to high security cells. Alice and Bob were well aware of these facts, so that before getting locked up, they had shared a secret codeword that they were going to exploit for embedding hidden information into their seemingly innocent messages. Alice and Bob succeed because they exchanged information allowing them to coordinating their escape and Eve does not become suspicious [2].

Steganography and Wavelet Transform

Wavelets are mathematical functions that cutup data into different frequency components, and then study each component with a resolution matched into its scale. They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes [3]. The Wavelets have been developed independently in the field of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields have guided to new applications; e.g. image compression, turbulence, human vision, radar, and earthquake prediction [4].

Image compression based on wavelet transform has given more attention in the recent years, especially for the data compression because of its superiority over the existing methods; i.e. high compression efficiency, the ability to handle large images, and progressive image transmission [5]. JPEG 2000, is one of the important attacks against image Steganography because it produces little degradation on stego-image at high compression ratios while its effects on the embedded image remains noticeable [6].

Understanding the types of attack that can be executed against Steganography led to discovering countermeasures to those attacks. The purpose of the countermeasure is to prevent a successful attack. Such countermeasures are useful for creating more robust Steganography [7]. Possible countermeasures to deter the effect of applying JPEG 2000 to the stego image may include the use of the wavelet transform itself to embed data in perceptually more significant parts of a cover image to make the removal of the embedded data more difficult. In addition to this advantage, the multi-resolution aspect of wavelets helps in managing a good distribution of the data in the cover in terms of robustness versus visibility [6]. However, it is expected that the next few years will witness the more attentions that would be given to wavelet transform as a tool in the image Steganography.

Least Significant Bit

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bit/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components.The simplest Steganography techniques embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence as shown in figure(1). Modulating the least significant bit does not result in a human-perceptible difference because the amplitude of the change is small other techniques "Process" the message with a pseudo-random noise sequence before or during insertion into the cover image. The advantage of LSB is embedded in its simplicity and its high perceptual transparency. However, there are many expected weaknesses when robustness, tamper resistance, and other security issues are considered; LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling rotation, cropping addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (Zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [8].

Quantization

It is a non-reversible mapping process, returns an approximated values. By this process, the wide range of real numbers is mapped to a small set of integers which require less number of bits in representation. Quantization can be performed by[10]:

$$f_q(r,c) = (f(r,c) - f_{\min}).\frac{255}{f_{\max} - f_{\min}} \quad \ldots (1)$$

Where: f(r, c) is the image before the quantization and fq(r , c) is its quantized version, fmax and, fmin are the maximum and minimum values of the original image. As mention before, this process affects the embedded image because many grey levels of the attenuated version of this image will be merged in one level depending on the attenuation factor.

Measures of image quality

Comparing restoration results requires a measure of image quality. Two commonly used measures are the Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), adopted here and given by[9]:

$$MSE = \frac{1}{MxN}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}(I(x,y) - I^{'}(x,y))^2 \quad (2)$$

$$PSNR = 20 \times \log_{10}(\frac{(255)}{\sqrt{MSE}}) \quad \ldots\ldots (3)$$

Where: I(x,y) is the original image, I'(x,y) is the corresponding values of the reconstructed image, and M and N are the height and the width of the image, respectively.
For colored images, the PSNR is computed as an average value of the Red, Green, and Blue bands.

Experimental Work and Results

This section explains the stego work, using steganography traditional method and steganography compression method. The samples of images shown in Figure.(4); i.e. Lena, Vista and MelG are used as cover images, while those illustrated figure.(5); i.e. Kids, Lily, Camera Man and Finger used as messages (they will be converted into gray tone images). Figures. (6, 8, and 10) clarifies the cover, quantize and stego images, their histograms, and the achieved MSE and PSNR for each stego image. Figures(7, 9, and 11)demonstrate the messages after the extraction process, and their MSE and PSNR values. The Conceptual models for these methods are illustrated in figure.(2) and figure.(3). Finally, the achieved quality measure results are listed in Table1 and Table 2.

Steganography Traditional Method

In this method the process consists at first quantize the cover image to 128 color in each band then generate two subsets {C1,C2…, C(sm)} from the cover image {M1,M2…,M(sm) } from the secret or message image where sm is the number of bits in the message (sm=xm×ym×8), next performing the substitution operation Ci↔Mi, which exchanges the LSB of the Ci by Mi ,where Ci each byte from a pixel of the cover image. As shown in figure.(2), their results clarified in Table1.

Adaptive Steganography Compression Method

This section explains LSB substitution with compression method which is illustrated in figure.(3). At first taking Lena's image and quantize it using 7 bits i.e 128 color, then up to 6 messages can be hide, while in traditional method only one message can be hide. Applying DWT to each message, then taking, LLBF, coefficients and storing them in Lena's image with eliminating remain coefficients. Finally, extracting messages, from Lena's image then calculation MSE and PSNR for each message which clarified in figure.(7)
and Table2. In order to check Steganography compression method figure.(8), figure.(9) clarifies the method on Vista cover image and figure.(10), figure.(11) clarifies the method on MelG cover image.

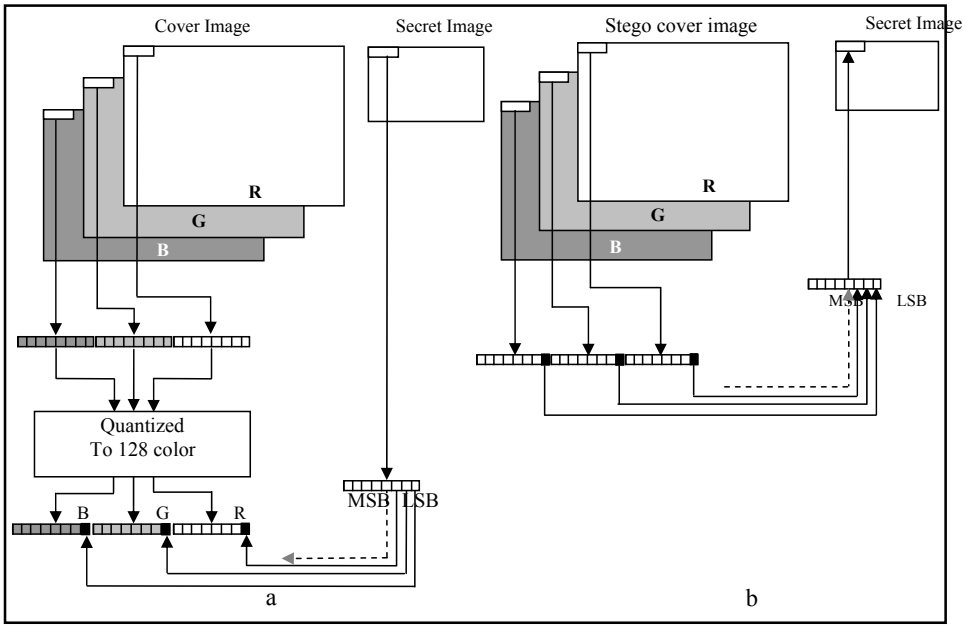

Figure 1: LSB Process a- The embedding algorithm b- The extracting algorithm

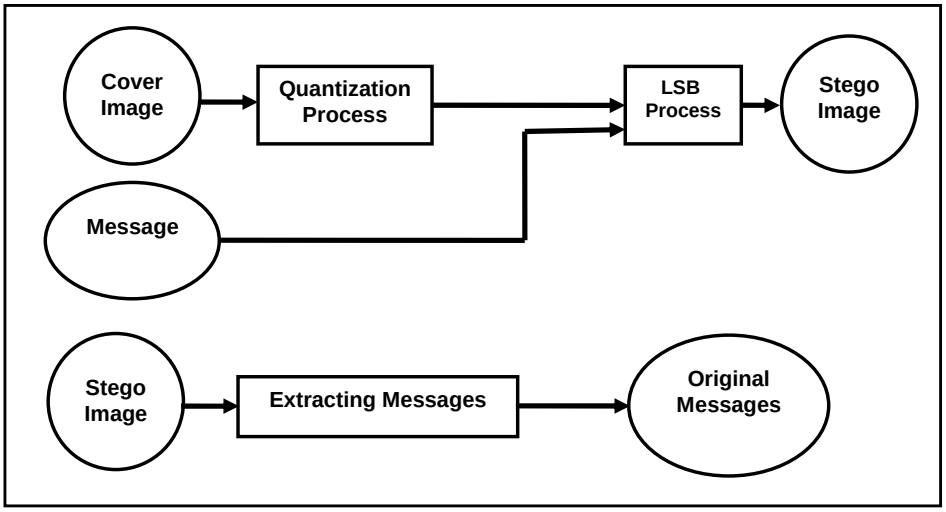

Figure 2: Traditional method system (Forward, Backward).

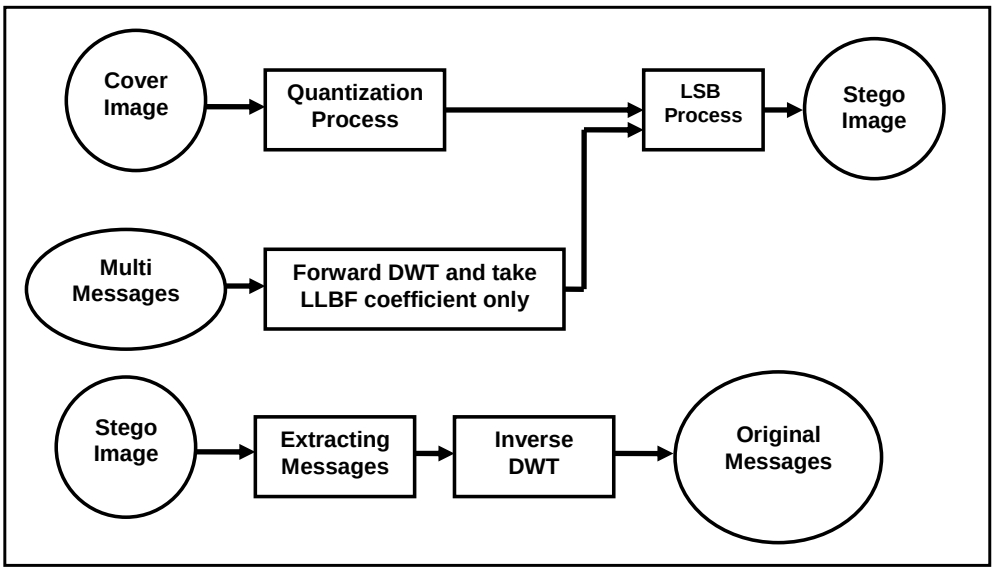

Figure 3: Steganography Compression method system, (Forward, Backward).

Conclusions

In this paper, an adaptive, useful, link between image hiding and image compression. The method provided additional security to the hided messages by reducing their required saving bits. In the recovering process, the number of saved messages is required. More security would be achieved if we encrypting the messages before inserting them in the cover. More image data compression may be required to increase the compression factor and remaining the output image quality unchanged.

Figure 4: Cover Images. (256× 256 Pixels)

Figure 5: Original Messages (128× 128 Pixels)

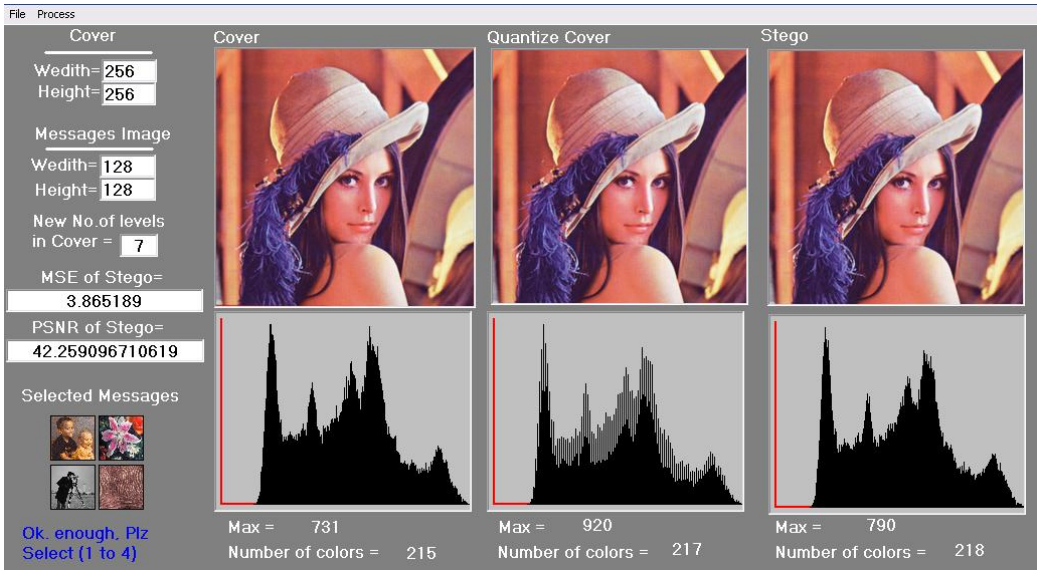

Figure 6: Lena cover image with the MSE, PSNR and its Histograms.

Figure 7: Recovered messages from the cover Lena image.

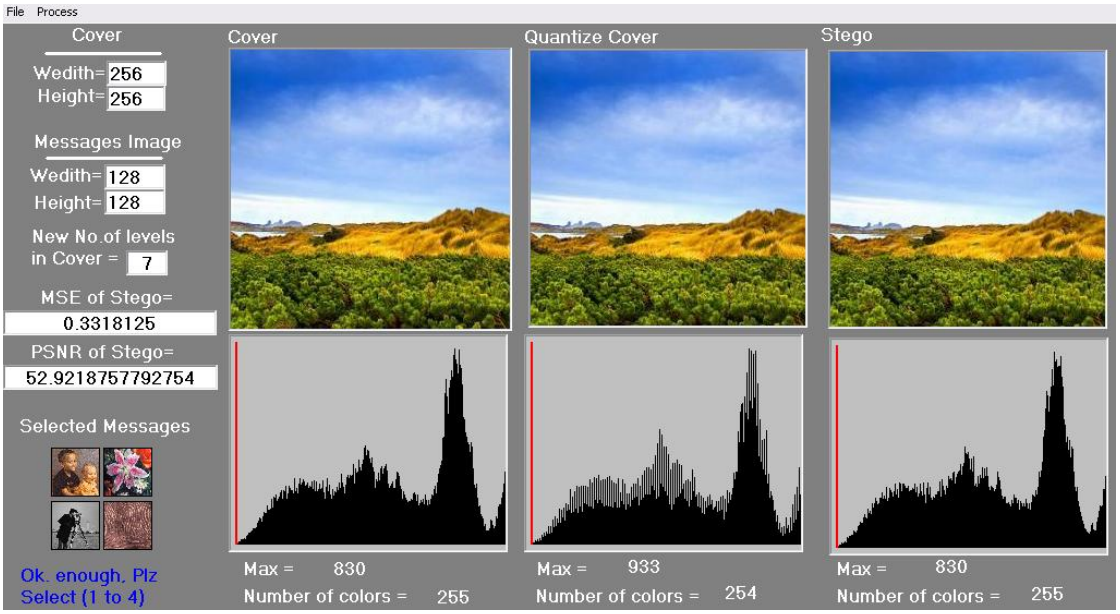

Figure 8: Vista cover image with the MSE, PSNR and its Histograms.

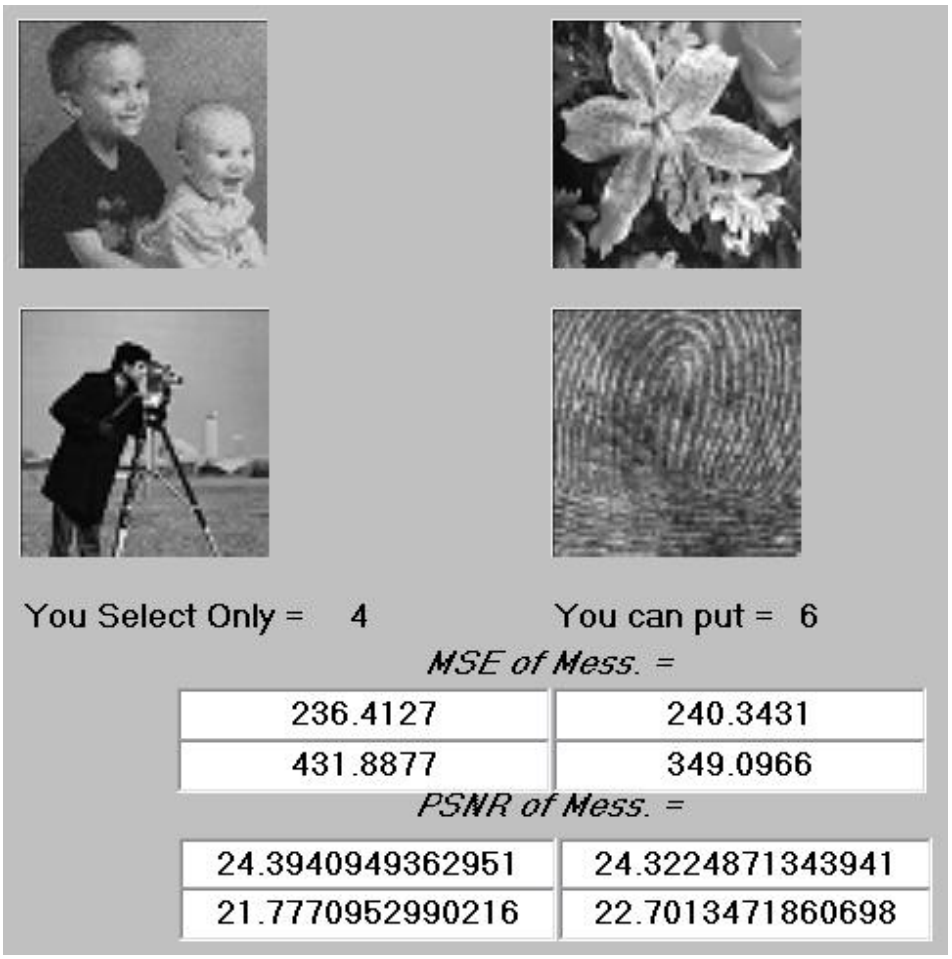

Figure 9: Recovered messages from the cover Vista image.

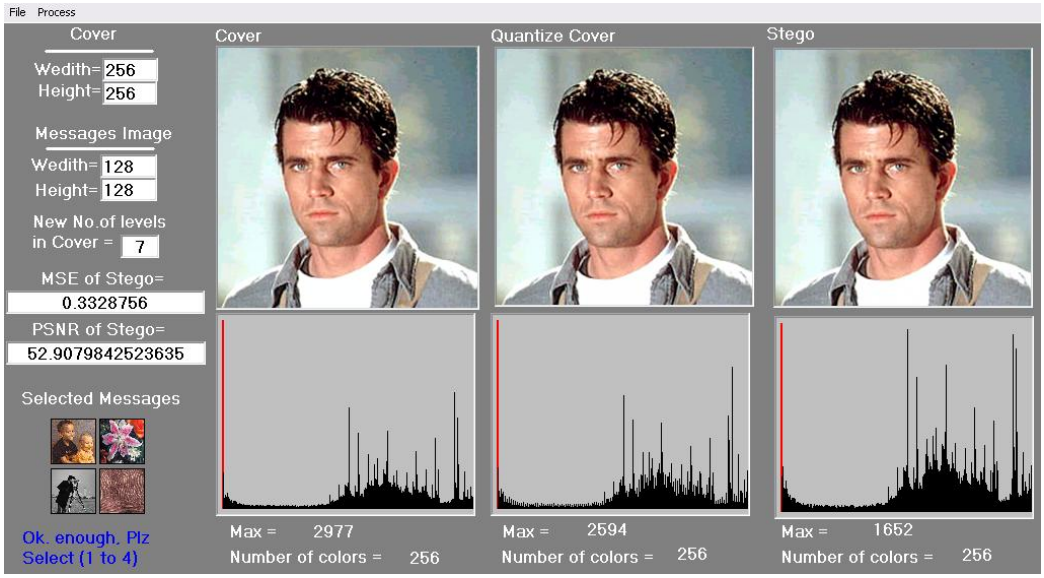

Figure 10: MelG cover image with the MSE, PSNR and its Histograms.

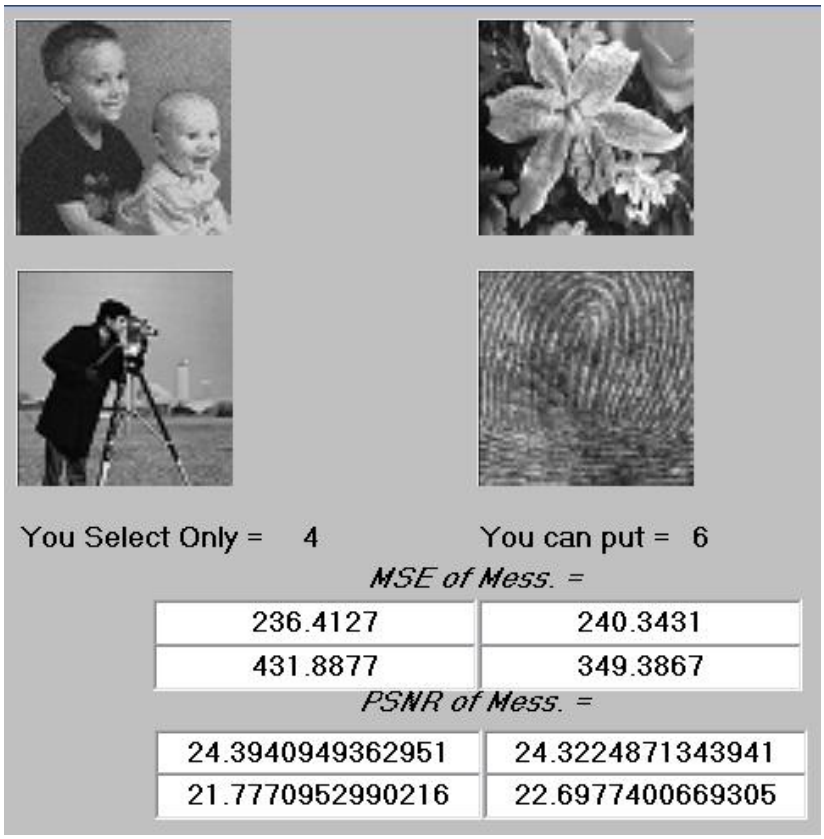

Figure 11: Recovered messages from the cover MelG image.

Table 1: Traditional Method Results.

Cover Image	MSE	PSNR	Message Image	PSNR
Lena	0.989	48.177	Kids	58.488
Lena	0.974	48.247	Lily	59.439
Lena	0.988	48.184	Camera Man	Infinity
Lena	1.020	48.047	Finger	60.125
Vista	0.332	52.925	Kids	58.488
Vista	0.330	52.944	Lily	59.439
Vista	0.332	52.924	Camera Man	Infinity
Vista	0.332	52.917	Finger	60.125
MelG	0.331	52.928	Kids	58.488
MelG	0.332	52.922	Lily	59.439
MelG	0.331	52.929	Camera Man	Infinity
MelG	0.331	52.930	Finger	60.125

Table 2: Adaptive Method Results.

Cover Image	MSE	PSNR	Message Image	PSNR
Lena	3.865	42.259	Kids	24.394
			Lily	24.322
			Camera Man	21.777
			Finger	22.688
Vista	0.332	52.922	Kids	24.394
			Lily	24.322
			Camera Man	21.777
			Finger	22.701
MelG	0.333	52.908	Kids	24.394
			Lily	24.322
			Camera Man	21.777
			Finger	22.698

References

1. Simmons, G. J. **1984.** The prisoners problem and the subliminal channel, in advances in cryptology: *Proceedings of Crypto 83 (D. Chaum, ed.*), 51–67, Plenum Press.
2. Pfitzmann, B. **1996.** *Information Hiding Terminology*, LNCS **1174.**Verly, Berlin, pp.347–350.
3. Graps, A. **1995.** An introduction to wavelets, *IEEE Computational Science and Engineering*,**2**(II):1-18.
4. Vetterli, M. and Kovacevic, J. **1995**. *Wavelets and Subbands Coding. Englewood Cliffs*, New Jersey, Prentice Hall.
5. Strack, J. L.; Murtagh, F. and Bijaoui, A. **1998.** *Image Processing and Data Analysis, The Multiscale Approach*., cambridge University press.
6. Katzenbeisser, S. and Petitcolas F .A .P. **2000.***Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, London.
7. Johnson, N. and jajodia, S. **1998.** *Steganalysis Of Images Created Using Current Steganography Software*. LNCS **1525.**Verly, Berlin, pp.273-289.
8. Johnson, N. F.; Duric, Z. and Jajodia, S. **2001.** *Information Hiding: Steganography and Watermarking*, kluwer academic publishers.
9. Satish,K.**2003**. An introduction to image compression. http://www.debugmode.com /imagecmp/ index.htm
10. Gonzalez, R . C . **2002**. *Digital Image Processing*. 2nd Edition, Prentice Hall.