International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 4 (March 2013), PP. 65-73

A Novel Steganography Method for a Secret True Image

Dr.Bahija khudaier shukur[1], hiba Mohammed jafaar[2], Anwar Jaafer Moosa[3]
[1]Assist. Prof., Iraq, Hilla, Babylon University
[2,3]Lecturer, Iraq, Hilla, Babylon University

Abstract:- Steganography is an ancient art or conveying messages in a secret way that only the receiver knows the existence of a message, most these methods suffer from number of problems which effect on its performance and implementation.In this paper, a novel mechanism using mathematical modulus to incorporate the secret true image into a cover-image to overcome most of these problems .This proposed method aims to meet most the requirements of any steganography system (like capacity, security and un detectability) ,where the mathematical modulus merging the secret data (the true image after compressing it by using wavelet Daubechies filter and ciphering it using strong key consist two stage the first stage generating pseudo random binary bit and xor it with the byte of the resulted image the second stage consist the rotate operation to satisfying the confusion and diffusion conditions) , that modulus is a threshold value that determines how the embedded file is incorporated into the cover-image. This method has a higher security since the secret information added to the cover image and the hiding data cannot be reconstructed unless we knowing the hiding algorithm and if we know the reconstructed algorithm then the hiding data cannot be constructed unless we know the decompression algorithm. In addition to that the knowing of the sharing secret information between the sender and the receiver which is the seed of the pseudo number generator (Sk) ,series number(S), the number of the hiding bits (m_l,m_u) and the threshold value (T) ,also the using of random style making the reaching process to the hiding image is difficult. The compressing and ciphering the embedded file used in order to reduce the size of it and increase the security. Furthermore, the quality of stego-image measured by PSNR is acceptable to human vision system and stable for diverse cover-image processes.

Keyword: Steganography, pseudo number generator, mathematical modulus

I. INTRODUCTION

Steganography can be defined as the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Though the concept of steganography and cryptography are the same, but still steganography differs from cryptography. Cryptography [1] focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated the strength of steganography can thus be amplified by combining it with cryptography. The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications.

Furthermore cryptography (from Greek kryptós, "hidden", and gráphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. The art of protecting information (plain text) by transforming it (encrypting it) into an unreadable format is called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography encrypts the actual message that is being sent. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key [2].

In addition to that steganography(from Greek Stegános, "Covered/hidden", and gráphein, "to write") is the art and science of communicating in a way which hides the existence of the communication [3].Steganography hides the very existence of the message by embedding it inside a carrier file of some type. An eavesdropper can intercept a cryptographic message, but he may not even know that a stenographic message exists. Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography, in contrast attempts to

prevent an unintended recipient from suspecting that the data is there. [4].Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable [5][6][7].

Steganography includes the hiding of media like text, image, audio, video files, etc in another media of same type or of different type. Later, the message hidden in the selected media is transmitted to recipient. At receiver end, reverse process is implemented to recover the original message.

II. WAVELET TRANSFORM

Wavelet transform (WT) is a linear transform developed from Fourier transform. However, unlike Fourier transform whose basis functions are sinusoids, wavelet transform is based on small waves, so-called wavelet, of varying frequency and limited duration so to obtain better resolutions along frequency scale [8], [9]. Wavelets can be used to solve very different problems that appear in many areas of electrical engineering, such as speech, audio and image coding, computer graphics, communications, numerical analysis, statistics, etc. [10]. Obviously a color image can be regarded as the change of discrete signal along a two-dimensional (2D) scale. Hence, a 2D discrete WT (DWT) was proved to be useful for signal or image processing and pattern recognition [11], [12]. Through decomposition of 2D discrete WT, which is implemented by consecutive low-pass (L) and high-pass (H) filtering through one-dimensional convolution, in this paper 2D wavelet transform is performed over these entered true images using Daubechies filter wavelet decomposition which can be divided into an approximation image (LL) and three detail images in horizontal (HL), vertical (LH), and diagonal (HH) orientations,.

III. THE STRUCTURE OF THE PROPOSED SYSTEM

Most researches are concerned on the LSB method for data hiding. This method, as explain previously, has many problems that effect on the performance of the embedding method. For this and to get a secure embedding, we proposed a new method that hiding a true color image in a BMP image file by using a mathematical modulus to incorporate the secrete true color image into a cover image . Its overcome LSB's problems and aiming to satisfy most the requirements of steganography system, especially the two main aspects (security and capacity), that affecting on the steganography and its usefulness.

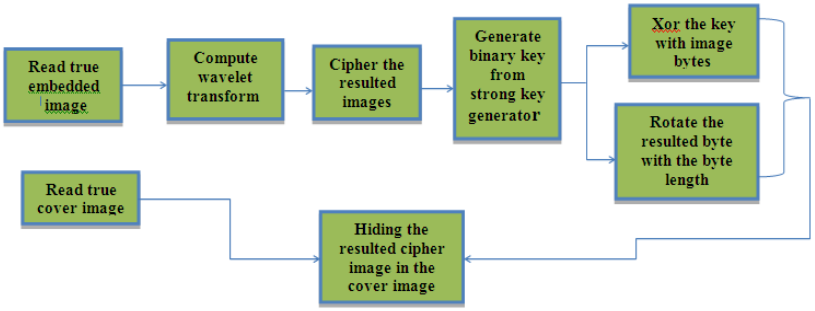


Figure 1: The cipher and hiding part

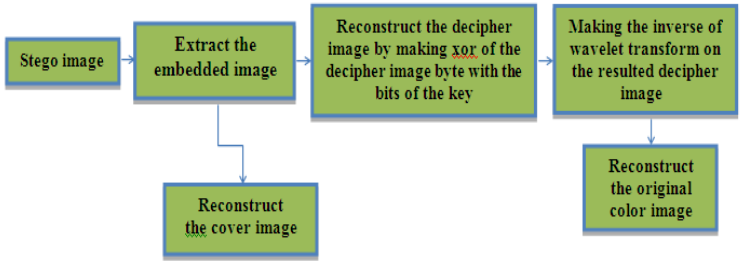


Figure 2: The decipher and reconstructed the original image part

3.1 Compute Wavelet

The main steps of this algorithm are:

Step 1: -Convolve the lowpass filters with rows and save the results.

Step 2: -Convolve the lowpass filters with the columns (of the result from step 1) and subsumable this result by taking every other values; this gives us the Lowpass -Lowpass **(LL)** subimage.

Step 3: -Convolve the result from step 1, the lowpass filtered rows, with the high Pass filter on the columns.by taking every other value to produce the Lowpass –Highpass **(LH)** Subimage

Step 4: -Convolve the original image with the Highpass filters on the rows and save the result.

Step 5: -Convolve the results from step 4 with the lowpass filter on the columns; Subsamples to yield the Highpass-Lowpass **(HL)** subimage.

Step 6: - To obtain the Highpass-Highpass **(HH)** subimage, convolve the columns of the Result from step 4 with Highpass filter

Step 7:-Go to step 1.

3.2 The inverse of wavelet transforms

In this stage to reconstruction the original image, where the reconstruction process started from the level that the analysis finished. The reconstruction process consist two main processes which are the convolution of the rows and columns with the filters and scaling ,the second process is the interpolation ,which consist the adding zeros between each two respective samples

The steps of this algorithm are:

Step 1:-Upsample the rows for each Subband **(LL, LH, HL, and HH)** by inserting zero between every two samples

where the Step 2:-Convolve the rows result from step 1 with low and high pass filter, and **(HL, HH)** with the high pass filter. Subbands **(LL, LH)** with low pass filter

Step 3:-Upsample the columns for the result from step2 by inserting zero between every two samples.

Step 4:-Convolve the result from step 3 with low pass and high pass filters, where the subbands **(LL, HL)** with **(LH, HH)** with high pass filters. the low pass filter and

Step 5:- Add the results from step 3 with the result from step 4 and save the result.

3.3 Cipher the Resulted wavelet image

The resulted wavelet matrix converted into a bit-string and then ciphers it as the following algorithm:

Read header of (resulted wavelet image)

While not end of file (resulted wavelet image)

Xor two byte from resulted wavelet image by two byte for strong key

Rotate the resulted two cipher bytes

End while

3.4 Hiding Ciphered image in the cover

After that the resulted ciphered wavelet matrix converting into a bit-string in order to embed by using modulo mechanism [13]. Assume that the color of one pixel p *a*t co-ordinates **(x,** *y)* is denoted by f(x, *y),* the eight-neighbors of p. For *p,* f (x**,** y) will be modified according to its embedding capacity, which depends on its color and the color variation of the upper and left neighbors. The advantage of using the upper and left neighbors to estimate the embedding capacity is that when or after the current pixel is processed, the colors of these upper and left neighbors will be never changed. Therefore the embedding module and extracting module arc synchronous when estimating the embedding capacity of each pixel [14]. Let

$$\begin{aligned}
&\text{Max}(x, y) = \max\{f(x-1, y-1), f(x-1, y), \\
&\qquad f'(x-1, y+I), .f(x, y-1)\} \\
&\text{Min}(x, y) = \min\{f(x-1, y-1), .f(x-1, y)), \\
&\qquad f(x-1, y+I), f(x, y-1)\} \\
&D(x, y) = \text{Max}(x, y) - \text{Min}(x, y)
\end{aligned}$$

Except for the boundary pixels in an image, the embedding capacity Kn(x, y) of each pixel (x, y) is defined as

$$\text{Kn}(x. y) = \log_2 \lfloor D(x, y) \rfloor$$

The embedding capacity should be limited by the color of current pixel. Here, an upper bound for embedding capacity at pixel (x, *y)* is defined as

$$U(x,y)=\begin{Bmatrix}4 & ,if\ \ f(x,y\le t\\ 5, otherwise\end{Bmatrix}$$

The next scheme describes the embedding algorithm:

Embedding Algorithm

Input: The cover-image and the embedding image message, the seed key and two modulus numbers m_u, m_l.
Output: The stego-image and secret key.

Step1: Find the workable pixel $p_c(i)$ in cover image C by using the pseudo-random number generator of seed sk .
Step2: Compressed the embedded-image
-Apply wavelet transform.
-Convert the coding matrix into bit-string B_s
Step 3: Set a threshold value T and the two modulus values m_l, mu. then compute a residue, $g_{remainder}$ and the possible capacity in a pixel, g_{eC} , as following form:

If $p_c(i) > T$, compute $g_{ec} = \lfloor Log_2^{m_u} \rfloor$, $g_{remaimder} = p_c(i) \bmod m_u$

Else, compute $g_{ec} = \lfloor Log_2^{ml} \rfloor$, $g_{remaimder} = p_c(i) \bmod m_l$

Where $p_c(i)$ denotes the intensity of the i-th. Pixel with order of top-down and left to-right in a cover-image C and $\lfloor\ \rfloor$ denotes the truncate value.

Step 3: Compute the absolute difference value, g_{dv}, such that

$$g_{dV=}|g_{remainder} - g_{ev}|$$

Where g_{ev} is a value, which is fetched sequentially from Bs with bits of g_{ec} -length.

Step 4: Embed g_{dv} into the pixel $p_c(i)$ (here, we define $p_s(i)$ as the intensity of the i-th pixel after embedding g_{ev})by performing the following Process:
Case I: $p_c(i) < T$

1. if $p_c(i) < \frac{m_l}{2}$, gain $p_s(i) = 0 + g_{ev}$.

2. $\frac{m_l}{2} < p_c(i) < T - \frac{m_l}{2}$

. if $g_{dv} > \frac{m_l}{2}$, gain an adaptable value, $Av = m_l - g_{dv}$.

. if $g_{remainder} > g_{ev}$, gain $p_s(i) = p_c(i) + Av$.

else , gain $p_s(i) = p_c(i) - Av$.

. if $g_{dv} \le \frac{m_l}{2}$, gain $Av = g_{dv}$

. if $g_{remainder} > g_{ev}$, gain $ps[I] = pc[I] - Av$.

3. If $(T - \frac{m_l}{2}) \le p_c(i) < T$, $gain\ p_s(i) = p_c(i) - g_{remainder} + g_{ev}$

Case II : $p_c(i) \ge T$

1. If $p_c(i) > (255 - \frac{m_u}{2})$, gain $p_s(i)=(255-m_u+1)+g_{ev}$

2. If $(T + \frac{m_u}{2}) < p_c(i) \leq 255 - \frac{m_u}{2} + 1)$

. If $g_{dv} > \frac{m_u}{2}$, gain $Av=m_u-g_{dv}$

If $g_{remainder} > g_{ev}$,gain $p_s(i)=p_c(i)+Av$
Else, gain $p_s(i)=p_c(i)-Av$

. If $g_{dv} \leq \frac{m_u}{2}$, gain $Av=g_{dv}$

If $g_{remainder} > g_{ev}$,gain $p_s(i)=p(i)_c-Av$
Else, gain $p_s(i)=p_c(i)+Av$

3. If $T \leq p_c(i) < (T + \frac{m_u}{2}), gain\ p_s(i) = p_c(i) - g_{remainder} + g_{ev}$

Step 5: Hide the embedded-header in the separated file .
Step 6: End.

The header part of the embedded image sending in a separated file.

In the stage of extraction, every bits of embedded image is extracted from the stego-image depending on the positions that stored using random number generated by seed key and two modulus numbers m_u, m_l .additionally the receiver must know the embedding algorithm and then decompress the extracted bits. The receiver cannot able to extract the embedded-image without know the embedded positions; therefore this method is more secure. The next scheme describes the extracting algorithm:

Extracting Algorithm

Input: The stego-image, the seed key and two modulus numbers m_u, m_l.
Output: The embedded-image.

Step1: Extract the embedded header of image.
Step 1: Find a workable pixel p_s (i) in stego-image s by using the
Pseudo-random number generator of seed Sk.
Step 2: Compute the embedded information as following
Case I: ps (i) <T:

$$g_{remaimder} = p_s(i) \bmod m_l$$
$$g_{ec} = \lfloor \mathrm{Log}_2^{m_l} \rfloor$$

Case II: $p_s(i) \geq T$:

$$g_{remaimder} = p_s(i) \bmod m_u$$
$$g_{ec} = \lfloor \mathrm{Log}_2^{m_u} \rfloor$$

Step 3: Translate the $g_{remainder}$ into the bits representation to recover the
embedded information, the bit-length for each $g_{remainder}$ is
Determined by the computation of g_{ec} .
Step 4: Decompress the embedded information
- Apply inverse wavelet transform.
Step 4: Recover the embedded-header from the separated file.
Step 5: End.

IV. THE PERFORMANCE MEASUREMENTS

To measure the performance of the proposed method, two different image files with different sizes are applied. Also, we are used true color images. The method emphases in selecting the image files that its sizes larger as four times than the image files. In order to explain how the proposed method have high-capacity

feature. We are used subject and object criteria as measures of stego-image and restored message quality. In object criteria, the following formulas are used:

i) Root mean square error (**RMSE**[*]).

$$RMSE = \sqrt{\frac{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2}{(M \times N)}} \quad ,(2)$$

ii) Peak signal to noise ratio (**PSNR**[*]): Here we are used two different formulas, one for images as following:

$$PSNR = 10 \log_{10} \frac{(L-1)^2}{\frac{1}{M \times N}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2} \quad ,(3)$$

Where L represents the number of gray levels $\hat{I}$ is the stego-image, and I is cover-image with size (MxN). Whereas, for measuring the quality of restored image, the following PSNR[**] formula is used:

$$PSNR = 10\log_{10} \frac{\sum_{n} x^2(n)}{\sum_{n}\left[x(n) - y(n)\right]^2} \quad ,(4)$$

Where x (n) represent sample of embedded image sequence and y(n) stand for sample of restored image sequence.

V. SATISFYING THE REQUIREMENTS OF CAPACITY, AND UNDETECTABILITY

In these experiments we attempt to embed an image message its size larger than the cover image. Also the modulus values m_u, ml are set of 32 and 16 respectively. In a sense the modulus 32 is set to accommodate the embedding of 5-bit pattern at the situation that the pixel of embedded image is greater than the threshold value T picked in our algorithm is empirically set the intensity value of 160.On the other hand, the modulus 16 is set to accommodate the embedding of 4-bit pattern at the condition that the pixel of embedded image is less than T. We have been tested the proposed method on a number of true color images with different size, to embed an image message its size as four times. The embedding capacity approximate restored message are given in table (1).

It can be seen from table 1 that the proposed algorithm with generally higher **PSNR** values for restored message. This indicates that the restored file is semi to the origin. Here we don't substitute the similar blocks in order to make the stego-image without distortion.

Also, the table 2 shows the results of **RMSE** and **PSNR** between the cover-images and stego-images.In such case, the embedding message is totally incorporated into cover-image. This indicates that all images less distortion and the attacker (steganalysis) can't easily detect the embedded message. This makes the mission of the attacker is more difficult. The **RMSE** and **PSNR** values for stego-images it's acceptable and the distortions are imperceptibility to human vision. It means such distortions will be less noticeable from the viewpoint of attacker.

Table 1: The results of RMSE and PSNR for the extract image massage.

Image	RMSE (image)	PSNR (image)
Image 2(b)	0.037	123.248
Image 4(b)	0.02	144.341
Image 6(b)	0.041	123.54
Image 8(b)	0.053	101.497

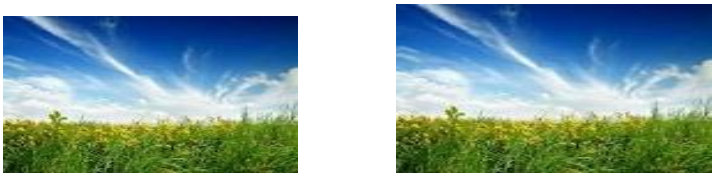
Table 2: The results of RMSE and PSNR for the stego-images

Image	RMSE (image)	PSNR (image)
Image1(b)	**0.01**	**95.504**
Image3(b)	**0.012**	**87.971**
Image5(b)	**0.013**	**85.884**
Image7(b)	**0.014**	**80.493**

VI. THE RESULT FOR THE IMPLEMENTATION OF THE PROPOSED SYSTEM

(a) (b)

Figure (3): image1 (a) cover-image, (b) stego-image



(a) (b)

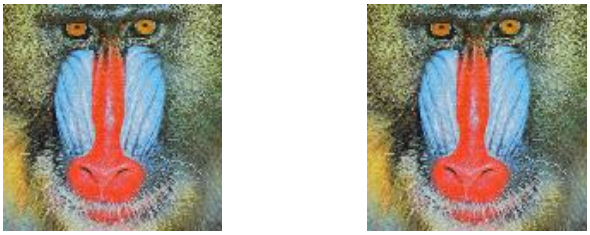
Image2 (a) embedded-image, (b) extract -image

(a) (b)

Figure (4): image3 (a) cover-image, (b) stego-image

(a) (b)

Image4 (a) embeded-image, (b) extract -image



(a) (b)

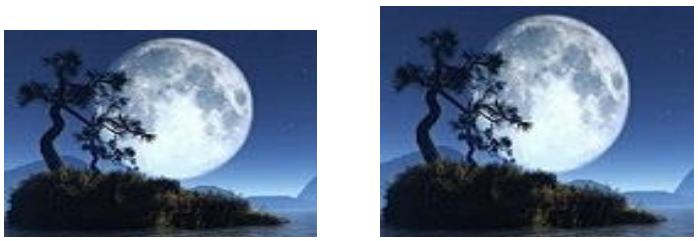
Figure (5): image5 (a) cover-image, (b) stego-image

(a) (b)

Image6 (a) embedded-image, (b) extract -image

(a) (b)

Figure (6): image7 (a) cover-image, (b) stego-image



(a) (b)

Image8 (a) embedded-image, (b) extract –image

VII. CONCLUSIONS

This paper emphases the most application requirements of any success steganography system like (capacity, invisibility, security, and undetectability and advanced the relation of one to one.

The process of compression gives as the ability to hide data its size larger than the cover data. Thus, we can hide a message its size larger than the size of cover-media and make the size of message less limited in some size. At this point, here is the powerful of the proposed method by increasing the capacity of cover-media and reducing the limits of size that facing most data hiding techniques. We find from experiments that the increased size of message have no much effects on the quality of stego-image and still imperceptible. Additionally, the compression process add another layer of protection for secrete message.

Also, after the embedding stage is completed, the stego-image less distortion or distortion-free depending on the values of **RMSE** and **PSNR** as we see in tables (1, 2), respectively. This is because the change in the values of data of cover-image is not found or not perceptual and the quality of stego-image still good. These results

reflected the ability of human visual system. This point will reflect on the steganalysis, and makes the process of analyzing the produced steganography very difficult.
For the security requirement, the algorithm produces a sequence of secret key that send independently to increase the difficulty of steganalysis on these stego-images. The receiver can extract the embedded message by using that secret key only.

REFERENCES

[1]. X. Luo, F. Liu and P. Lu. A LSB Steganography Approach Against Pixels Sample Pairs Stegonalysis. International Journal of Innovative Computing, Information and Control, Vol. 3, No. 3, pp. 575-588, June 2007.
[2]. William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.
[3]. M. Vetterli and J. Kova˘cevi´c. Wavelets and Subband Coding. Prentice Hall, 1995.
[4]. M. A. B. Younis and A. Janta. A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of computer science and network security, vol.8, no.6, June 2008.
[5]. C. C. Lin, and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," Journal of Systems and Software, 73(3):405-414, December 2004.
[6]. Kafa Rabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) -2004.
[7]. [2] S. Lyu and H. Farid. Steganalysis Using Higher-Order Image Statistics. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 111-119, March, 2006.
[8]. B. K. Alsberg, A. M. Woodward, and D. B. Kell, "An introduction to wavelet transforms for chemometricians: a time-frequency approach", Chemometrics and Intelligent Laboratory Systems,Vol 37, No. 2, pp. 215-239, 1997.
[9]. R. C. Gonzalez, and R. E. Woods, Digital Image Processing, 2nd Edition, Prentice-Hall, Inc., 2002.
[10]. A. N. Akansu and M. J. Y Smith. Subband and Wavelet Transforms: Design and Applications Kluwer Academic Publishers, 1996.
[11]. M. K. Bashar, T. Matsumoto, and N. Ohnishi, "Wavelet transform-based locally orderless images for texture segmentation", Pattern Recognition Letter, Vol. 24, No. 15, pp. 2633-2650, 2003.
[12]. H. G. Hwang, H. J. Choi, B. D. Kang, H. K. Yoon, H. C. Kim, S. K. Kim, and H. K. Choi, "Classification of breast tissue images based on wavelet transforms using
[13]. discriminant analysis, neural network and SVM", Proceedings of the 7th International Workshop on Enterprise Networking and Computing in Healthcare Industry, Busan
[14]. , Korea, pp. 345–349, 2005.
[15]. S.Wang and K.Yang, a Scheme of High Capacity Embedding On Image Data
[16]. using Modulo Mechanism, WISA, Souel, Korea, (2001).
[17]. Y.K.Lee and L.H.Chen, high Capacity Image Sreganographic Model, IEE
[18]. proceeding Vision, Image and Signal Proceeding, 147, 3, 288,(2000) .