Steganography System Using Wavelet Transform
(Image Inside Image)

Submitted by

Fatma Hassan Al-Rubbiay * **Raghad Mohammed Hadi****

Abstract

Steganography is allowing a user to hide large amounts of information within image and audio files. Steganography is still in an experimental phase and no general theory is available

This research suggests method of sub-image (secret image) hiding inside a covered image using discrete wavelet transform, in this method we hide secret image inside details information applied on a covered image.

In this way, sub image must be shrinked its values in order to accommodate high resolution details, after this process is accomplished we must try to re-arrange shrinked secret image in simple manner by changing row positions and then changing columns position which get hide secret image and then convert to the inverse discrete wavelet transform it.

The proposed system is tested using PSNR criteria and has proved that there are no tangible changes between the cover image and stego image

Key words (Steganography, Wavelet Transform).

* Management and Economey Collage / University of Al Mustansuraia

** Informatics Institute for Postgraduate Studies /Iraqi Commission for Computers and Informatics

الكتابة المخفية باستخدام طريقة التحويل المويجي

في الصور الرقمية

اعداد

فاطمة حسن الربيعي*   رغد محمد هادي**

الخلاصة

الكتابة المخفية تسمح للمستخدم بأخفاء كميات كبير من المعلومات في ملفات الصور والصوت. الكتابة المخفية لاتزال في مرحلة الاختبار ولاتتوفر نظرية عامة .

هذا البحث يقترح طريقة لاخفاء جزء من الصورة (الصورة المأمونة) في داخل الصورة الغطاء بأستخدام التحويل الموجي المتقطع، في هذه الطريقة نخفي الصورة المأمونة داخل المعلومات التفصيلية للصورة الغطاء.

في هذه الطريقة، الصورة المأمونة يجب تقليص قيمها لكي تستوعب التفاصيل بدقة عالية ، ولاكمال العملية يجب اعادة ترتيب الصورة المأمونة بصورة بسيطة بواسطة تغيير موقع السطر ثم تغيير موقع العمود لكي يحصل اخفاء الصورة المأمونة ثم يتم التحويل الى معكوس التحويل الموجي المتقطع.

تم اختبار النظام المقترح باستخدام معيار PSNR واثبت عدم وجود تغيير ملموس بين الصورة الغطاء والصورة بعد الاخفاء.

الكلمات المحجوزة (الكتابة المخفية ، التحويل الموجي)

* كلية الادارة والاقتصاد / الجامعة المستنصرية

*** معهد المعلوماتية للدراسات العليا/الهيئة العراقية للحاسبات والمعلوماتية*

1. Introduction

With the use of the internet for the distribution of multimedia data, steganography has become a topic of growing interest. A number of programs for embedding hidden messages in images and audio files are available and the robustness of such embeddings is a controversial issue. [1].

The LSB (Least Significant Bit) modification techniques are easy ways to embed information but they are highly vulnerable to even small cover modifications. An attacker can simply apply signal processing techniques in order to destroy the secret information.

The development of steganography systems that embedding information in frequency domain of a signal can be much more robust than embedding rules operating in the time domain [2].

2. Digital Steganography

Information hiding represents a class of processes used to embed data into various forms of media such as image, audio, video, and text or any unused area in the storage media. The embedded data should be invisible and inaudible to a human observer [3].

An important subdiscipline of information hiding is Steganography. While cryptography is about protecting the content of messages, steganography is about concealing their very existence [2].

Steganography is the art and science of secret communicating. In contrast to cryptography, where the “enemy” is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem. The goal of steganography is to hide messages inside other “harmless” messages in a way that does not allow any “enemy” to even detect that there is a second secret message present[3].

Steganography has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks [4]. In figure (1) shows the image steganography system.

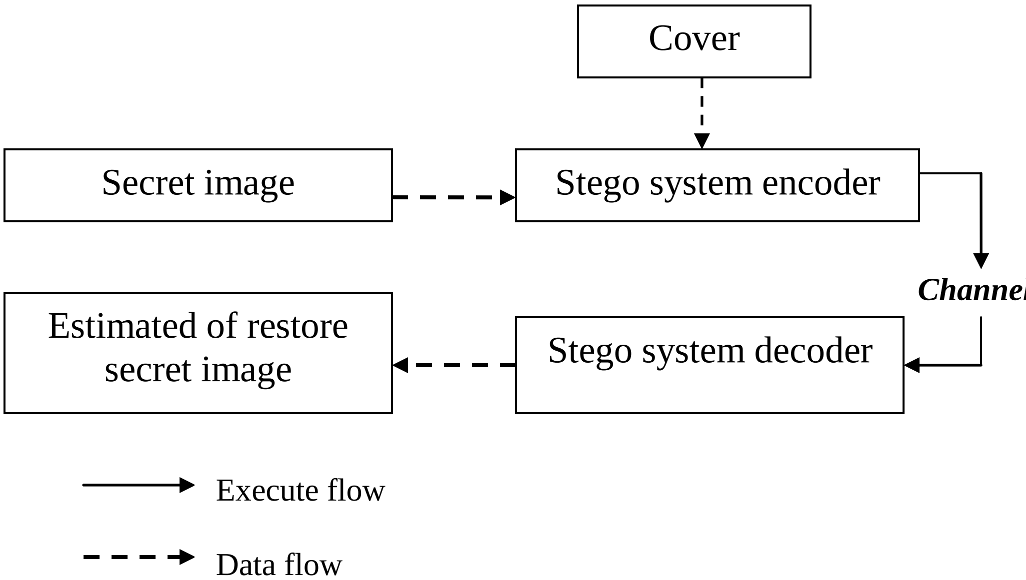

Figure (1) image steganography system (image inside image)

3. Steganography Features and Restrictions [5]

Steganography system should be capable of embedding data in a host signal (cover) with the following features and restrictions:

1. The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible.
2. The embedded data should be directly encoded into the media, rather than into a header or wrapper, so the embedded data will be compatible with different data formats.
3. The embedded data should be as immune as possible to modifications from intelligent attacks.
4. Some distortion or degradation of the embedded data that is expected at cover data makes it suffer from effects such as blurring.

4. Wavelet Transform (WT)

Wavelets are becoming a key technique in the ongoing source compression standard JPEG-2000. The multiresolution aspect of wavelets is helpful in managing a good distribution of the message in the cover in terms of robustness versus visibility [6]

The wavelet transform consists of multiscale spatial frequency decomposition of an image. Figure (2) shows the image decomposition with three scale factors. The lowest frequency band at the lowest scale factor is found in the top-left corner (LL_3). At the same resolution level, the block (HL_3) contains information about the highest horizontal and lowest vertical frequency band. Similarly, the block LH_3 contains information about the lowest horizontal and highest vertical frequency band at the lowest scale factor. The same process is repeated for the intermediate and highest resolution levels [2].

There are two types of analysis: the continuous and discrete time analysis. The distinction among the various types of WT depends on the way in which the scale and shift parameters [6].

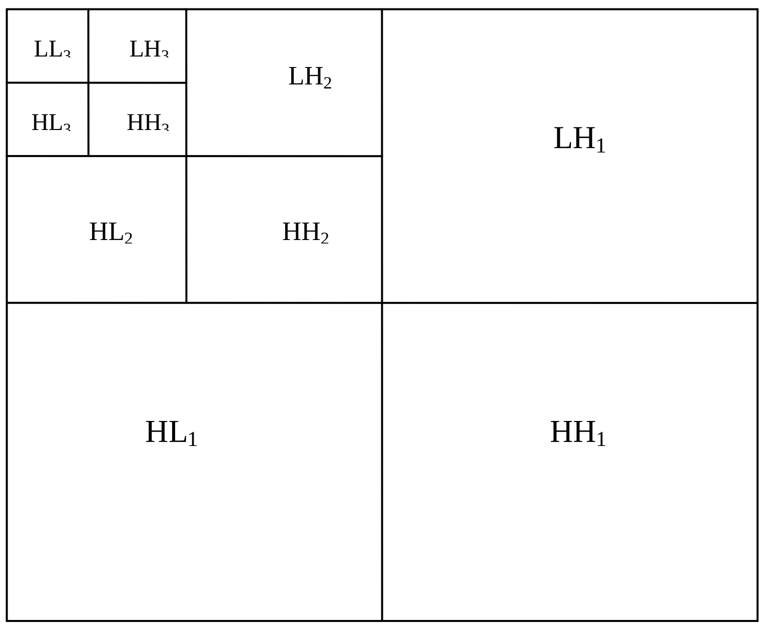

Figure (2) Multiscale decomposition [2].

1. Continuous Wavelet Transform (CWT)

The continuous Wavelet Transform was developed as alternative approaches to the short time Fourier transform to overcome the resolution problem [6].

The continuous Wavelet Transform is defined as follows:

$$CWT_x^{\psi}(T,S) = \psi_s^{\psi}(T,S) = \frac{1}{\sqrt{|S|}}\int x(t)\psi^*\left(\frac{t-T}{S}\right)dt \text{..(1)}$$

As seen in the above equation, the transformed signal is a function of two variables, *T* and *S*, the translation and scale parameters, respectively. Psi(t) is the transforming functions, and it is called the mother wavelet. The term mother wavelet gets its name due to two important properties of the wavelet analysis.

The term wavelet means a small wave, the smallness refers to the condition that this (window) function is of finite length (compactly supported).

The wave refers to the condition that this function is oscillatory. The term mother implies that the functions with different region of support that are used in the transformation process are derived from one main function, which is called the mother wavelet [7].

2. Discrete Wavelet Transform (DWT)

The wavelets are obtained from a single prototype function ψ(x) by scaling parameters 'a' and shift parameters 'b'. The discrete normalized scaling and wavelet basis functions are defined as,

$\varphi_{i,k}(l) = 2^{i/2} h_i(2^i l \,.\, k)$ …………………………….(2)

$\psi_{i,k}(l) = 2^{i/2} g_i(2^i l \,.\, k)$ …………………………….(3)

where i and k are the dilation and translation parameters and h_i and g_i are respectively the sequence of low pass and high pass filters. Thus 2-band discrete wavelet transform decomposes an image (two dimensional signals) into four sub bands namely LL (Low-Low), LH (Low-High), HL (High-Low) and HH (High-High). The decomposed sub bands correspond to the coarse approximation, horizontal, vertical and diagonal details of the image signal respectively. Multi resolution capability of wavelet transformation further decomposes each LL band into four previously specified sub bands [8].

The General equation of DWT as in the following:

$$g(t) = \sum_{k=-x}^{x} C_{j0}(k)\phi_{j0,k}(t) + \sum_{k=-x}^{x}\sum_{j=k}^{x} d(k)\phi_{j0,k}(t) \qquad (4)$$

The coefficient in this wavelet expansion is called DWT of signal g(t). These wavelet coefficients completely describe the original and can be used away similar to Fourier system (FS) coefficients for analysis, description, approximation, and filtering. If the wavelet system is orthogonal, these coefficients can be calculated by inner products. The DWT is similar to a FS but in many ways is much more flexible and informative. Unlike a FS it can be used directly no-periodic transient signals with excellent results [9].

5. Image Shrinking

Region growing and shrinking methods segment the image into region by operating principally in the rc-based image space. Some of the techniques used are local, in which small areas of the image are processed at a time; others are global, with the entire image considered during processing. Methods that can combine local and global techniques, such as split and merge, are referred to as state space techniques and use graph structures to represent the regions and their boundaries [10].

Various split and merge algorithms have been describe, but they all are most effective when heuristics applicable to the domain under consideration can be applied.

This given a starting point for the initial split. In general, the split and merge technique proceed as follows [10, 11]:

1. Define a homogeneity test. This involves defining a homogeneity measure, which may incorporate brightness, color, texture, or other application- specific information, and determining a criterion the region must meet to pass the homogeneity test.
2. Spilt the image into equally sized region.
3. Calculate the homogeneity measure for region.
4. If the homogeneity test is passed for a region, then a merge is attempted with its neighbor(s). If the criterion is not met, the region is split.
5. Continue this process until all regions pass the homogeneity test.

There are many variations of algorithm. For example, we can start out at the global level, where we consider the entire image as our initial region, and then follow an algorithm similar to the preceding algorithm, but without any region merging [11].

Algorithms based on splitting only are called multiresolution algorithms splitting. This merge-only approach will be quite similar, with the differences apparent only in computation time. Parameter choice such as the minimum block size all allowed for splitting, will heavily influence the computation burden as well as the resolution available in the result.

The user-define homogeneity test is largely application dependent, but the general idea is to look for features that will be similar within an object and different from the surrounding objects. In the simplest case we might use gray level as our feature of interest. Homogeneity test that required the gray level variance within a region to be less than some threshold. These are define gray –level variance [10]

$$\frac{1}{N-1} = \sum_{(r,c)=REGION} [I(r-c) - I]^{-2} \qquad (5)$$

$$I = \frac{1}{N} \sum_{(r,c)=REGION} I(r-c) \qquad (6)$$

6. The proposed system of Image Steganography Using Wavelet Transform

Image Steganography is trying to hide secret image inside a cover image in specific manner that doesn't change the viewing of cover image to everyone.

Now, if we want to apply image in a certain region of wavelet space of a cover image in some protocol that doesn't effect on reconstructed output. The results of zero equalized HH algorithm proved that this region of wavelet space contain doesn't effect hardly on the reconstructed image therefore we try to hide the secret image in the HH resolution in wavelet space image. If we make statistical study on the data point inside HH resolution, we find the band of data is very small and limited in a very narrow band, therefore the first problem we must solve it is trying to make matching between the data point inside HH resolution and the data point of secret image. The proposed system is use the below equation to calculate maximum Peak Signal to Noise Ratio (PSNR) between the cover image and stego image as follows:

$$PSNR = XY \max_{x,y} P^2_{x,y} / \sum_{x,y} (P_{x,y} - P_{X,Y})^2 ....(7)$$

This statistical test can expose abnormalities in an image that are not visible by the human eyes. This process compared between the original image and stego image.

The following algorithms show the steps of transmission and reception.

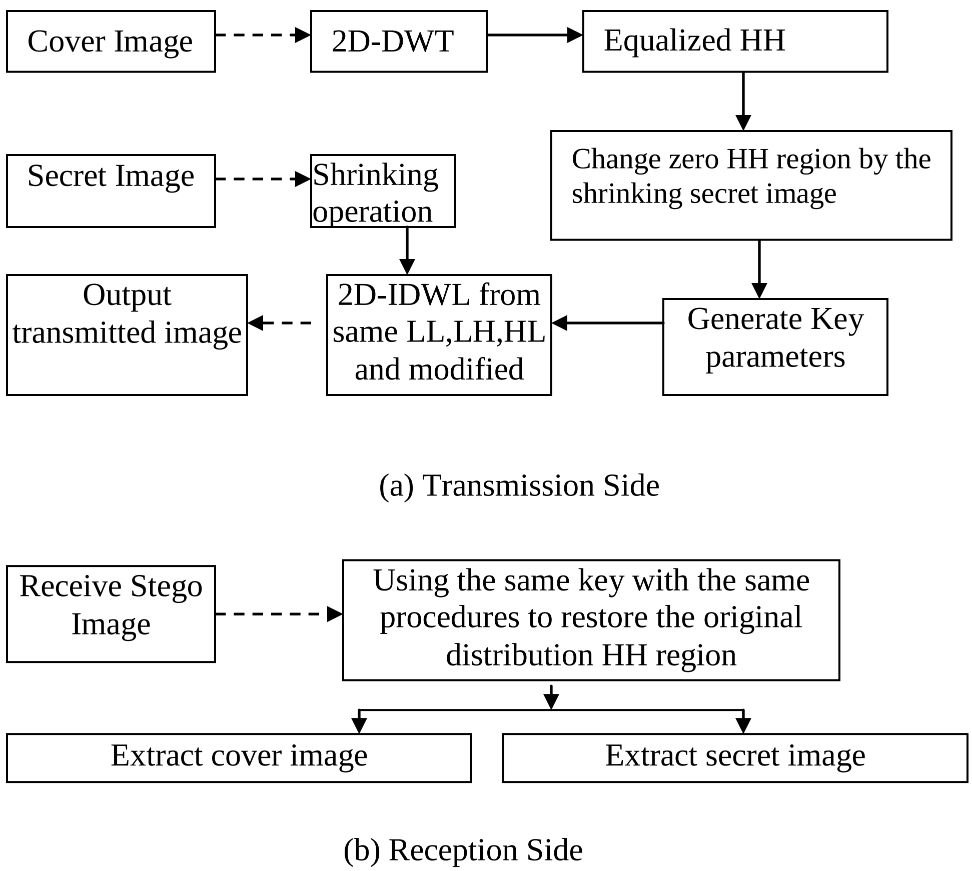

Figure (3) the proposed system which hides image inside image

The proposed system applied on different color images of size (640*480) pixels as a cover image and different images of size (256*256) pixels as secret image. This system applied on two types of image format (BMP and GIF) images.

From figure (3) we can see the image steganography takes two sides of work. The first is transmission side and the second for reception.

These algorithms are explained below:

6.1 Algorithm(1) { Transmission Side}

Input: secret image.

Output: the stego image.

Step 1: start

Step 2: Select a cover image with size N*N

Step 3: Select a secret image with size (N/2*N/2) at maximum.

Step 4: take two dimensional of discrete wavelet transform using specific wavelet filter of cover image.

Step 5: apply zero equalized algorithm on HH region of wavelet space as we explained in previous section.

Sep 6: apply shrinking on secret image in order to compress the band of its data point in to every narrow band to match the original data inside HH region of wavelet space by using equation (6) which explained in section (5).

Step 7: replace empty HH region of wavelet spaces by the image generated from the previous step.

Step 8: evaluate key parameters of steganography by using the secret key generation $K=[K_0,K_1,\ldots,K_{n-1}]$

Step 9: apply IDWL on the wavelet space of the same (LL, LH, Hl) resolution and update HH resolution.

Step 10: transmit the result image.

Step 11: end

6.2 Algorithm(2) {Reception Side}

Input: the stego image.

Output: the reconstructed original image and the secret image

Step 1: start

Step 2: receive the work image containing secret image.

Step 3: take 2D-DWL of the working image using specific wavelet filter.

Step 4: Separate the image result in HH region as single image.

Step 5: use the same key which is used in the transmission algorithm in a reverse direction in order to restore secret shrinking image.

Step 6: apply stretching on image of previous step in order to restore the original secret image.

Step 7: view the resulted secret image.

Step 8: end.

7. The results and Conclusions

1. The implementation of the suggested approach in transmission region is a signal modified image of original cover image and the success is get the higher degree of similarity between the modified and original cover image and compared the result by using PSNR test as show in table (1).

Image samples	Image type	PSNR of cover image	PSNR of stego image
S1	BMP	49.3	48.6
S2	BMP	49.6	47.9
S3	BMP	45.1	44.8
S4	GIF	44.6	44.3

Table (1) the result of PSNR testing

2. The implementation of suggested approach in reception region is an image stretching expand the band of the image to fit the full band of colors therefore the contract between colors of image are increased. Finally the resulted secret image must be similar to the original one. The success of our proposed work must offer high degree of similarity between the resulted secret image and the original one.
3. The high degree of similarity between resulted secret image and the original one that provide resistant against some type of attacks.

In the figure (4) shows example of the image steganography system with two sides of work first is transmission side and second for reception.

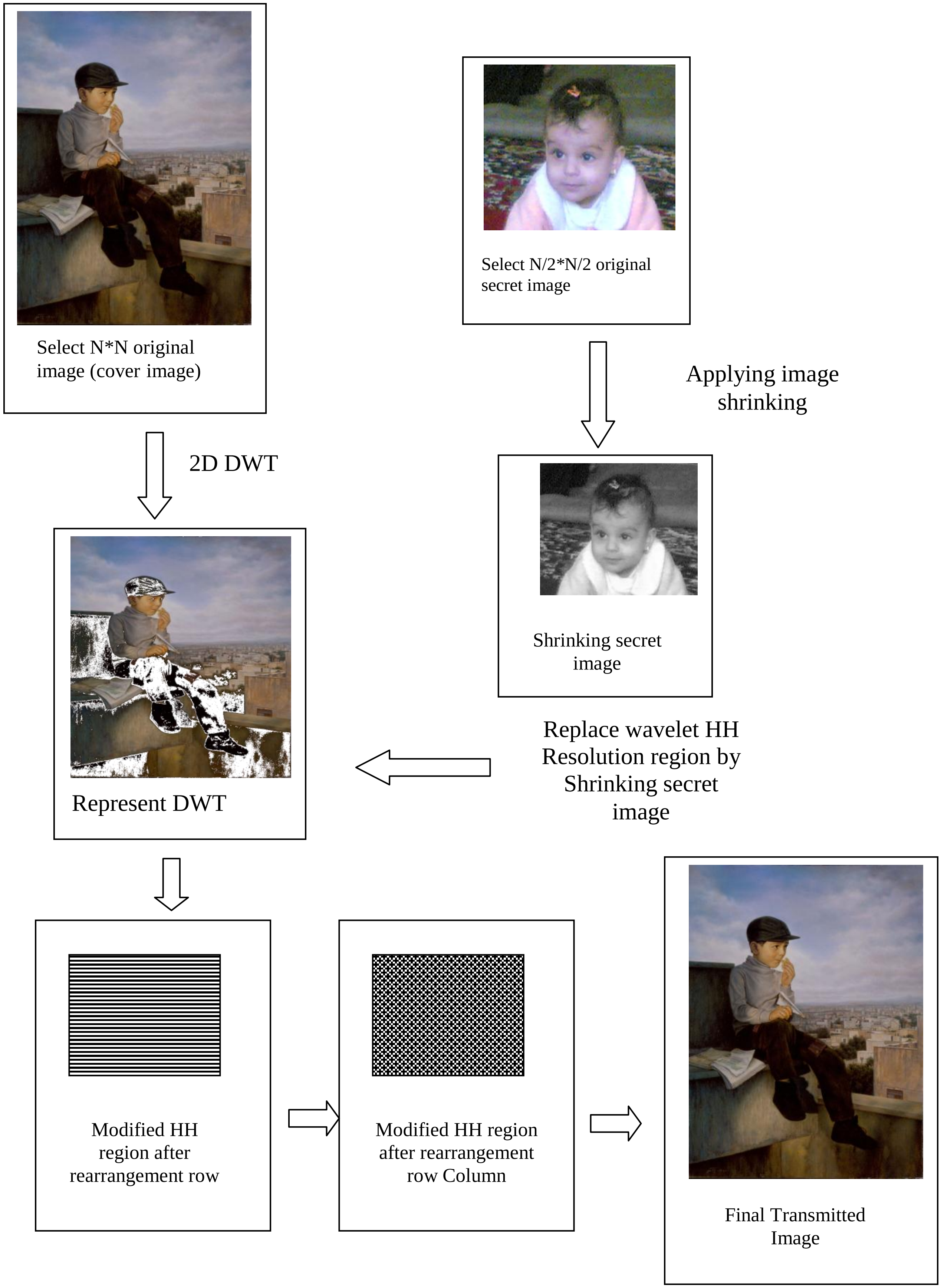

Figure (4.a) Example of the proposed system (Transmission side)

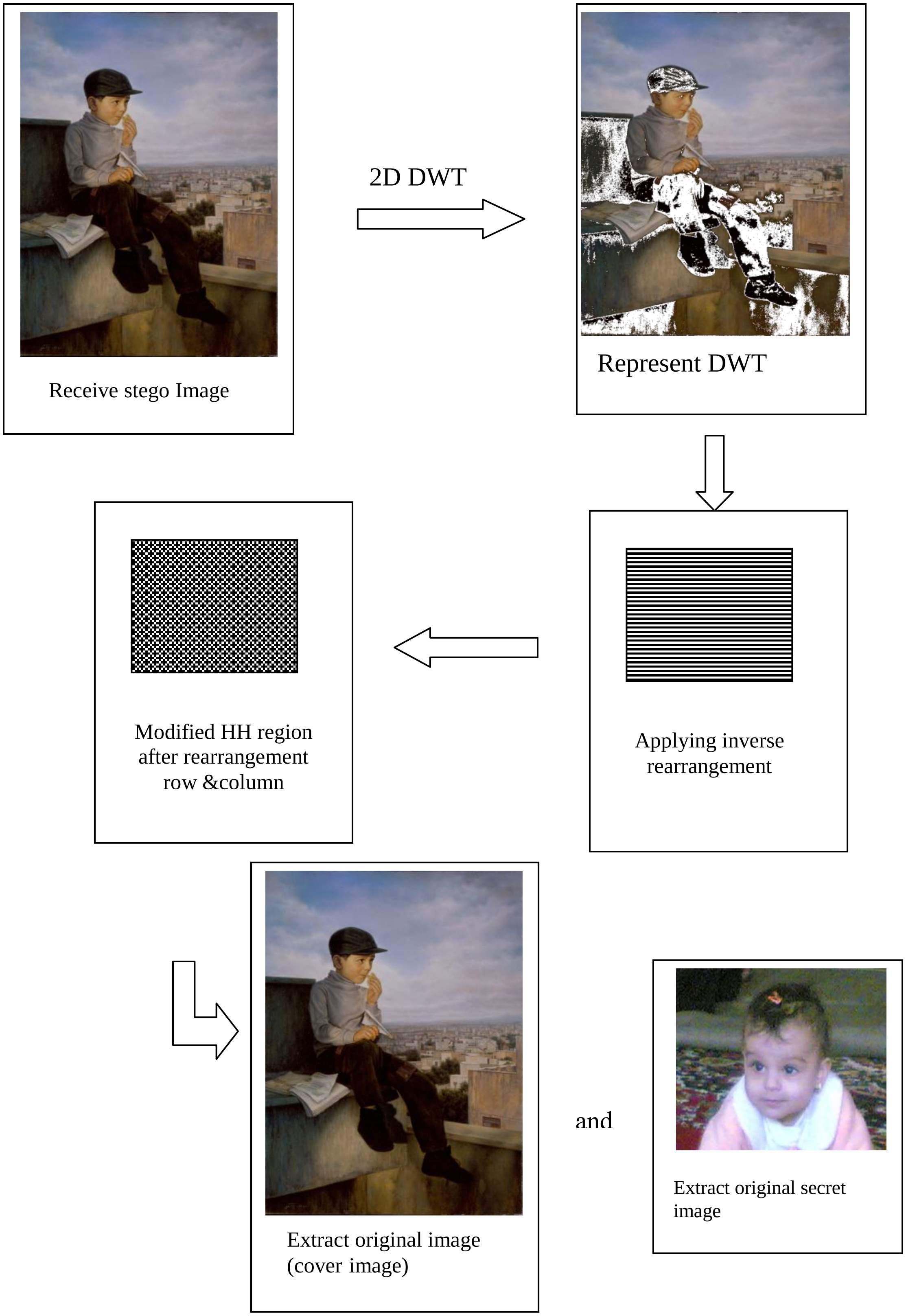

Figure (4.b) Example of the proposed system (Reception side)

8. Suggestions for Future Works

There are many suggestion points which can be given to enhance the work of the proposed system, theses are:

1. Improve the system to deals with animation images, video images, and audio.
2. Using another file format of the images that are not used in our system such as JPEG, TIFF, PCX and other formats.

9. References

1. Mittelholzer T., "An Information- Theatrical Approach to Steganography and Watermarking", Information Hiding, Third International workshop, Lecture Notes in computer since, pp.1-16, Springer, 2000.
2. Katzenbeisser S. and Petitcolas F., “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House pub., USA. http://www.ifi.unizh.ch/~oppliger/series editor.html, 2000.
3. Mahdi,S.R.., "Development of Text and Gray Image in Video Steganography Using MSB", M.Sc. thesis ,Iraqi Commission for Computer and informatics, Baghdad, Iraq, 2005.
4. Fabien, A. P., Petitcolas, Ross J., Anderson and Makus G. Kuhn, "Information Hiding : A Survey " , Proceedings of the IEEE, special issue on protection of multimedia content, July 1999.
5. Electronic Engineering: Technical seminar Topics, “Steganography – The Art of Hiding information”, julay 29 , 2008, www.bestneo.com
6. Polikar R., "The Wavelet Tutorial Part III: Multiresolution Analysis: The Continues Wavelet Transform", Dept. of Electrical and Computer Engineering, Rowan University, 1998, Web site, http://www.public.ee.iastate.edu.html
7. Valens, C., “ A Really Friendly Guide to Wavelets” , 1999, web site, http://www.preso.wandoo.fr/polyvalens/wavelets,html
8. Maity S.P., Nandy P. , Das T. S. , Kundu M. K., "Robust image watermarking using multiresolution analysis", Electronics and Telecommunication Engineering Dept., Bengal Engineering & Science University, Shibpur, Howrah, India 711103,2004.
9. Mallat, S.G,“A Theory for Multiresolution Signal Decomposition: The Wavelet Representation", IEEE transaction on Pattern Recognition and Machine Intelligence. No.7 ”,PP.67-693, July 1999
10. Umbaugh S.E., "Computer Vision and Image Processing”: A practical approach using CVIP tools “, Prentice Hall, 1998.
11. Gonzales, R.C., and Wintz, P., "Digital Image Processing", Addison Wesley publishing company 1992.