# IMAGE STEGANOGRAPHY BASED CURVELET TRANSFORM

**AHMED FREIDOON FADHIL**

**amet83@yahoo.com**

**Engineering College, Kirkuk University**

## ABSTRACT

This paper proposes a new image steganography scheme in order to hide a secret data in cover image uses the transform domain to increase its robustness and security. Curvelet transform is the new member of the evolving family of multiscale geometric transforms. Since it represents edges better than Wavelet, Curvelet transform offers an effective solution to the problems associated with image steganography using Wavelets and DCT (Discrete Cosine Transform). In this paper we were testing four different steganographic methods. The Radon Transform used in this paper for encoding the secret image to increase security. The software used in this paper is (Matlab V 7.0.4). The results obtained are in accordance with the expected predictions of the existing theory of Curvelet transform.

# اخفاء المعلومات داخل الصور بالاعتماد على التحويل (CURVELET)

**أحمد فريدون فاضل**

**كلية الهندسة ,جامعة كركوك**

## الخلاصة

هذا البحث يقترح مخطط جديد لاخفاء البيانات السرية داخل الصور باستعمال تحويل المجال لزيادة المتانة والأمن. التحويل (Curvelet) عضو جديد للعائلة الناشئة للتحويلات الهندسية متعددة القياس . ولان التحويل (Curvelet) تقوم باسترجاع الحافات افضل من ال(Wavelets) فانها تعرض حل فعال للمشاكل المرتبطة بفن اختزال الصور باستعمال التحويلات (Wavelets) والتحويل (DCT). هذا البحث يختبر اربعة طرق مختلفة لفن الاختزال. ان التحويل (Radon) ايضا استخدم في هذا البحث لتشفير الصورة المراد اخفاءها لزيادة الامن. ان البرنامج المستعمل في هذا البحث هو (Matlab V 7.0.4). ان النتائج التي تم الحصول عليها جاءت متطابقة مع التنبؤات المتوقعة لنظرية التحويل (Curvelet) الحالية.

**Received 12/3/2009**



**Accepted 14/2/2009**

## 1. INTRODUCTION

In the present erea of computers and fast communication, one needs to protect communicated information (message or plain text) from unauthorized user, while sending it through any electronic media. One such technique to protect the data is Steganography. Data hiding is also known as Steganography (from the Greek words stegano for "covered" and graphos "to write"). The Steganography consists of techniques to allow the communication between two persons. It hides not only the contents but also the existence of the communication in the eyes of any observer [1].

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data [2].It represents a method of sending a message to someone else in secret by hiding the message in contrast to cryptography, where the message is visible, but scrambled in such a way that only a recipient with proper knowledge (encoding method and a key) can recover the message. The two methods can be combined by encrypting the message and then hiding it using Steganography, so even if the hidden message is discovered, its meaning can remain secret [2].

Image steganographic techniques can be divided into two groups [3] the Spatial Domain technique group, and the Transform Domain technique group. The Spatial domain technique embeds information in the intensity of the pixels directly, while the Transform domain technique embeds information in frequency domain of previously transformed image [4]. The proposed scheme is a kind of the frequency domain techniques.

## 2. IMAGE STEGANOGRAPHY TECHNIQUES

### 2.1 Simple LSB Method

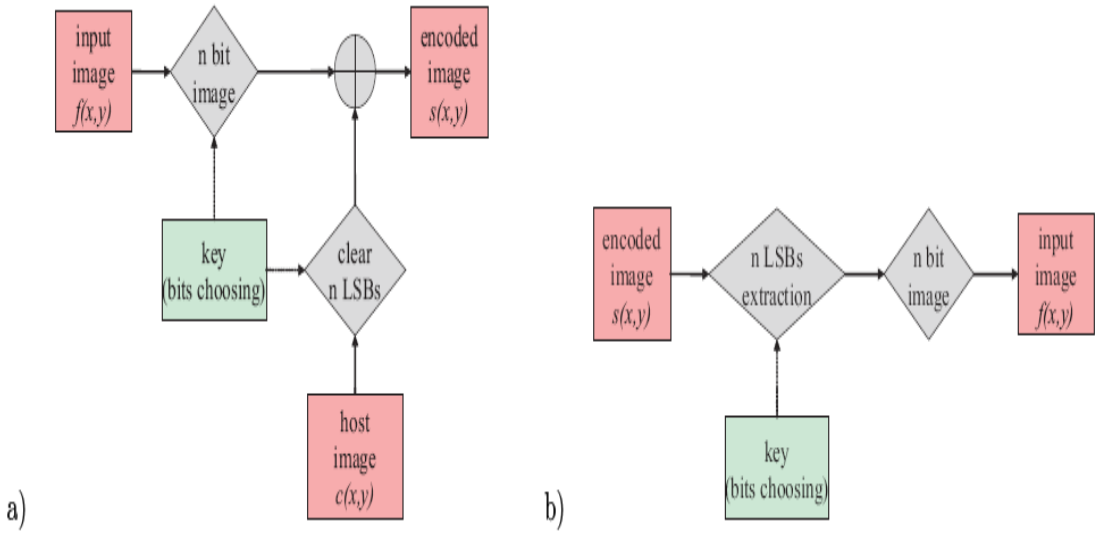
The first and most simple digital method uses less significant bits (LSB) to encode hidden data. The hidden message f(x,y) is divided into one, two or more LSBs of bytes describing each pixel. These bits of host image c(x,y) are replaced with bits from the message (Fig.1). Thus the hidden image is located in the domain of image and must possess several times less information pixels than the host image [5].

If input image is sufficiently smaller, it can be hidden in host image in a more sophisticated way. Only some pixels can be used for writing such data. The method of choosing these pixels can ensure additional security as it can be treated as a key without which decoding is impossible.

In Fig.1(a), The input image *f*(*x*,*y*) is changed into n bits per pixel of host image in the positions described by a key and n LSB bits in appropriate pixels of host image *c*(*x*,*y*) are cleared, next these two images are combined together into encoded image *s*(*x*,*y*).

In Fig.1(b), n LSB bits are extracted from appropriate pixels of encoded image *s*(*x*,*y*) defined by a key and next folded into decoded image *f*(*x*,*y*).

**Fig. (1):**




**Scheme of LSB method (a) Encoding (b) Decoding**

### 2.2 DCT Method

This method is closely connected with one of the most popular image formats in the internet (The JPEG standard and its lossy compression algorithm [6]). Decomposed image may not be the same as image before compression and changes in LSBs are expected. Therefore it is unlikely that LSB encoding would work with any lossy algorithm. In this method the whole host image c(x,y) is divided into blocks of n × n pixels (in basic version n=8). Each of them is transformed by using DCT. After that we get a block of n × n transformation coefficients they should be quantized by dividing them by a pre-defined (in JPEG standard) quantization matrix. Next, two of them: $C_{ij}$ and $C_{kl}$ are compared and their values are exchanged or not. If we want to put 0 in such a block and $C_{ij} < C_{kl}$ or if we want to put 1 and $C_{ij} > C_{kl}$ then we exchange the values of these coefficients. Otherwise we do not make any changes. It also possible to hide information f(x,y) by replacing the LSB of the quantized coefficients with the bit to be hidden in an image as in steganographic tool. After the completion of this process all blocks should be transformed by using inverse DCT obtaining encoded image s(x,y) (Fig.2). In this method the hidden image is located in the domain of transformation [2].

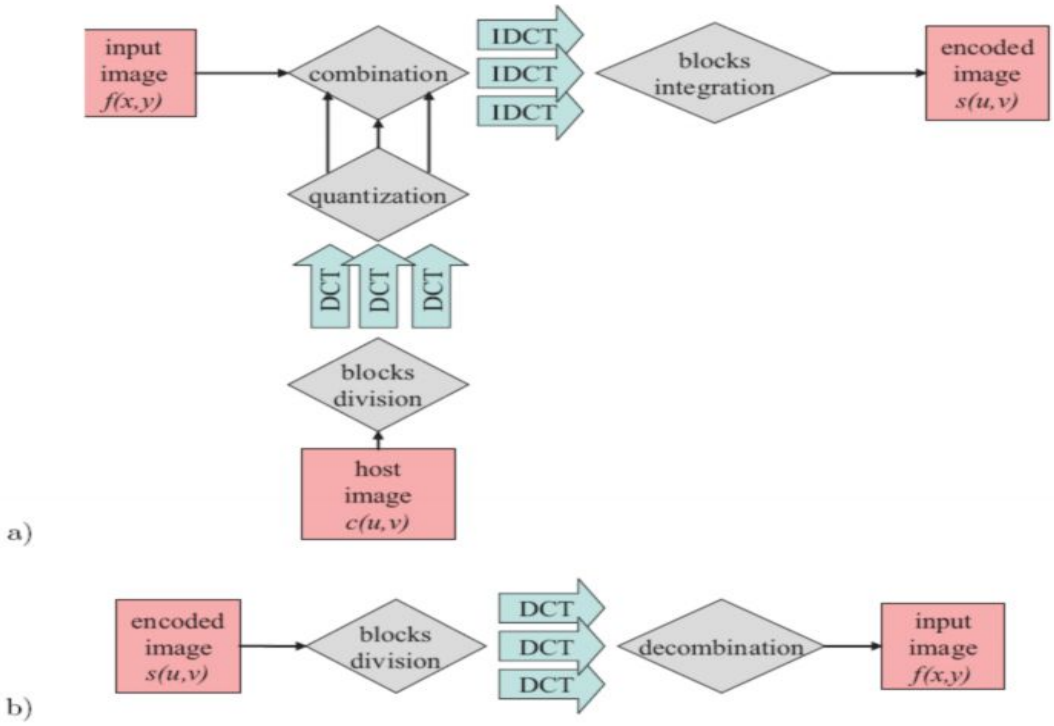



**Fig. (2): Scheme of DCT method (a) Encoding (b) Decoding**

### 2.3 Wavelet Method

Wavelet transform is used to convert a spatial domain image into frequency domain. It provides the time-frequency representation. The wavelet transform is created by repeatedly filtering the image coefficients on a row-by-row and column-by-column basis. The usefulness of wavelets in image steganography lies in the fact that the wavelet transform clearly separates high-frequency and low-frequency information on a pixel-by-pixel basis. The cover image is passed through wavelet filter bank. Image convolved with wavelet low pass filter gives smooth version of the input image and that with high pass filter results in the detail band. This decomposition can be carried up to $\log_2$(min (height, width)). The low pass coefficients of final level decomposition of the image constitute approximation band [7].

Haar Wavelet Transform is used here. It is the only quadrature mirror filter having a finite impulse response. The low-frequency wavelet coefficients (approximation band coefficients Ai) are generated by averaging the two pixel values as given in equation (1) and the high frequency coefficients (detail band coefficients Di) are generated by taking half of the difference of the same two pixels as given in equation (2).

$$A_i = \frac{P_{2i-1} + P_{2i}}{2} \quad (1)$$

$$D_i = \frac{P_{2i-1} - P_{2i}}{2} \quad (2)$$

Where $P_i$ is the ith pixel value in the input spatial domain signal sequence.

A cover image is decomposed into various wavelet sub-bands, shown in (Fig. 3), such as Approximation band, Vertical Detail bands, Horizontal Detail bands, and Diagonal Detail Bands. The Approximation band consists of the low frequency wavelet coefficients, which contains significant part of the spatial domain image. A detail band consists of high frequency coefficients, which contains edge details of spatial domain image.

The secret image is converted to 1D bit stream and embedded to the least significant bit (LSB) of the wavelet transform detail bands starting from Diagonal Detail Bands, Horizontal Detail Bands, and Vertical Detail Bands depending on data length.

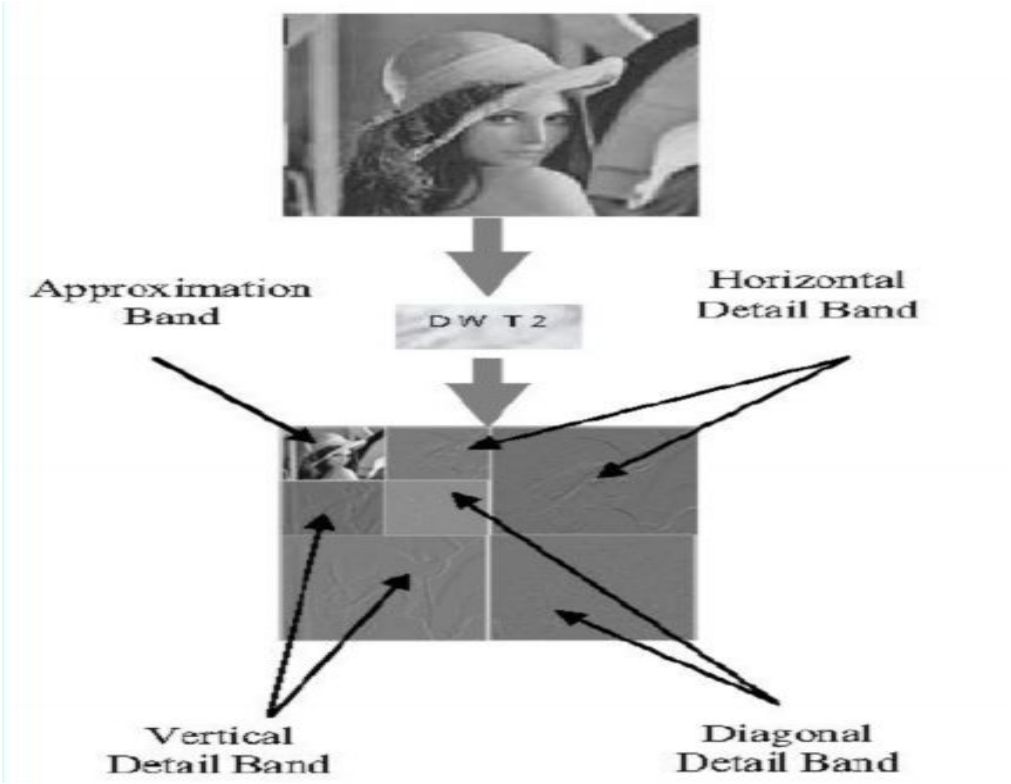



**Fig. 3: Wavelet Transform Subbands**

### 2.4 Curvelet Transform Method

The discrete curvelet transform for a 256 × 256 image is performed as is shown in (Fig. 4). The discrete curvelet transform can be performed in three steps [8]:

1) The 256 × 256 image is split up in three subbands.

2) Tiling is performed on subbands Δ1 and Δ2.

3) Discrete Ridgelet transform is performed on each tile.

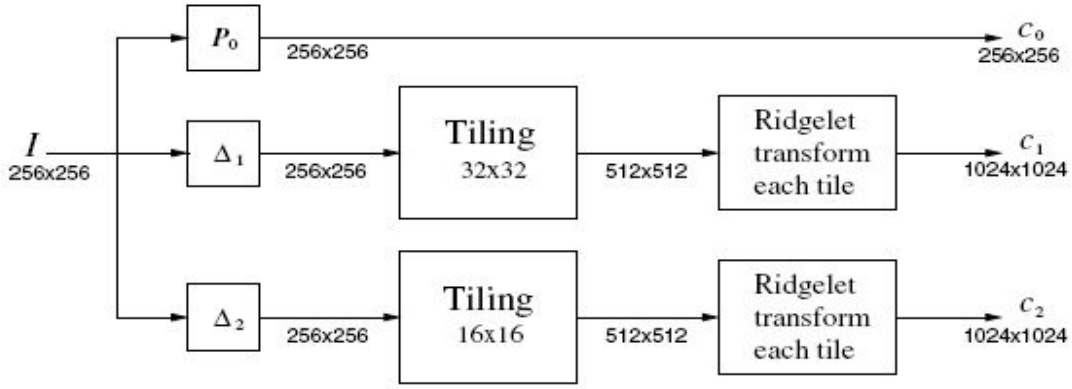



**Fig. (4): Flowchart of the discrete curvelet transform**

**A. Subband Filtering**

The subband filtering for a 256 × 256 image *I* is done as follows. The image is split up in three subbands *P*0, Δ1 and Δ2. Undecimated discrete wavelet transformation is used to implement the subband filtering. The 6-tap Daubechies undecimated discrete wavelet transform is used. *P*0*I* is the basis subband of image *I* calculated by zeroing all coefficients that stand for frequency larger than $\pi/16$ in the wavelet domain. Δ1*I* is the bandpass subband of *I* calculated by zeroing all coefficients that stand for frequency smaller than $\pi/16$ and larger than $\pi/4$ in the wavelet domain. Finally, Δ2*I* is the highpass subband of *I* calculated by zeroing all coefficients that stand for frequency smaller than $\pi/4$ in the wavelet domain. As an example, the Lena image *I* is split in the basis subband *P*0*I*, and bandpass subband Δ1*I* and highpass subband Δ2*I* as shown in (Fig. 5). Note that, the relationship between the Lena image I and its subbands is given by

$$I = P0I + \Delta 1I + \Delta 2I \qquad (3)$$

**B. Tiling**

The Ridgelet transform was designed to code linear singularities well but it does not handle curved edges nearly as well [8]. This is why the subbands Δ1 and Δ2 are tiled because by zooming well enough into the image, some curved edges will become linear singular. The tiling for the 256 × 256 subbands Δ1 and Δ2 are decomposed into overlapping blocks of side length 32 and 16, respectively.

**C. Ridgelet Transform**

To complete the Curvelet transform, the Ridgelet transform is used [8]. The standard 2D Ridgelet transform is described below:

1. Compute the 2D Fourier transform.
2. Extract lines going through the origin in the frequency plane.
3. Compute the 1D inverse Fourier transform of each line. We get the Radon transform.
4. Compute the 1D wavelet transform of the lines of the Radon transform.

The size of each subband after applying the Ridgelet Transform will be 512 × 512.

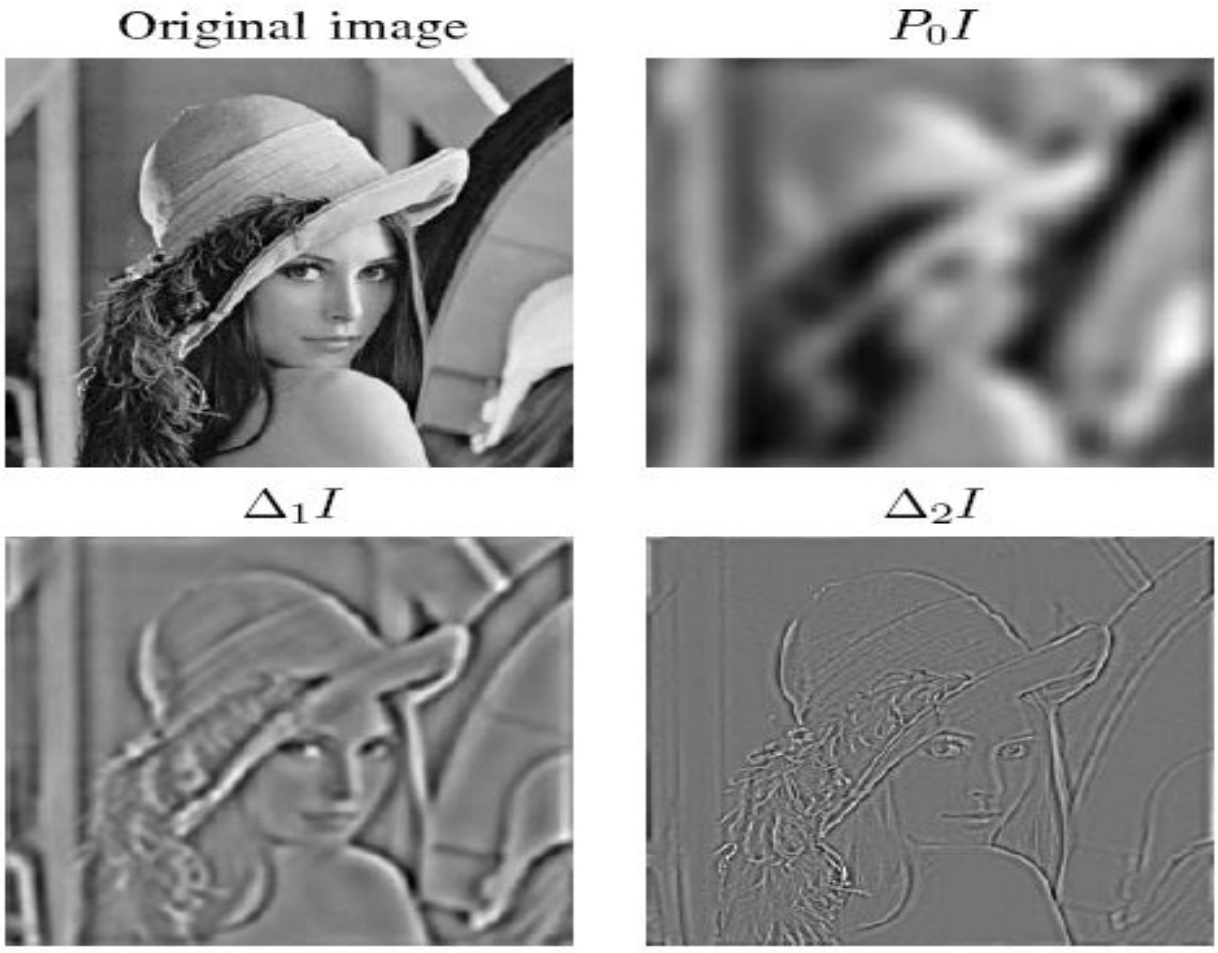



**Fig. (5): Lena image I and its subbands**

## 3. ALGORITHM FOR EMBEDDING DATA IN CURVELET TRANSFORM

The embedding process can be summarized step-by-step as follows:

**Input:** A cover-image of size $w \times w$ and secret-image of size h × h.

**Output:** A stego-image of size $w \times w$.

**Step 1:** Select a cover-image of size $w \times w$ and secret-image for hiding of size h × h.

**Step 2:** Radon Transform for secret-image is used to increase security of embedded image. The Radon Transform will randomly permute the data so that nobody can read the secret image without taking the inverse Radon Transform. Also nobody can guess the generated Radon sequence without

knowing the secret key. This ensures that only recipients who know the corresponding secret key will be able to extract the message from the stego image.

**Step 3:** Decompose the cover-image by using the Curvelet transform.

**Step 4:** Convert the secret-image into a 1D bit stream.

**Step 5:** The data sequence should be inserted into the least significant bit (LSB) of the Curvelet subbands starting from $\Delta 2I$, $\Delta 1I$, *and* $P0I$ according to data length, since the receiver must know the data length in order to extract the data. So we insert not only the data sequence but also the data length sequence N.

**Step 6:** After the embedding process ends. The stego image is generated by applying the Inverse Curvelet Transform on the modified coefficients.

## 4. ALGORITHM FOR EXTRACTING DATA IN CURVELET TRANSFORM

The extracting phase is similar to the embedding phase. The process can be summarized step-by-step as follows:

**Input:** A stego-image of size $w \times w$.

**Output:** A secret-image of size h × h.

**Step 1:** Decompose the image by using the Curvelet transform.

**Step 2:** The original cover-image is not needed to recover the embedded secret message from the received stego-image since the data length sequence (N) can be extracted from the Curvelet coefficients.

**Step 3:** Extract the embedded data bits from the N LSB's of the Curvelet transform.

**Step 4:** The proposed scheme is considered secure. That is; without knowing the stego-key a passive warden can't extract the secret image. In addition, without knowing the decryption key cannot retrieve the information bits. The inverse Radon transform with the secret key used to extract the secret-image.

## 5. OBJECTIVE MEASURES

The commonly used objective measures are the peak signal to noise ratio (PSNR), and the Correlation test (COR).

The peak signal to noise ratio (PSNR) is used in this paper to evaluate the image quality. The PSNR of a gray-level image is defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{MSE} \quad \mathrm{dB}. \tag{4}$$

The mean square error (*MSE*) for an N×N gray-level image is defined as follows:

$$MSE = \frac{1}{N^2}\sum_{r=1}^{N}\sum_{c=1}^{N}\left[X(r,c) - \overline{X}(r,c)\right]^2 \quad (5)$$

Here X denotes the original image, and $\overline{X}$ denotes the mean value of the corresponding image.

The closeness between two images can be quantified in terms of the correlation function. The correlation coefficient ranges from –1 to +1. A correlation coefficient value of +1 indicates that the two images are highly correlated, i.e., very close to one another. A correlation coefficient of –1 indicates that the two images are exactly opposite to each other [9]. The correlation coefficient is computed from:

$$Corr(I,X) = \frac{\sum_{r=1}^{N}\sum_{c=1}^{N}\left(I(r,c)-\overline{I}\right)\left(X(r,c)-\overline{X}\right)}{\sqrt{\left(\sum_{r=1}^{N}\sum_{c=1}^{N}\left(I(r,c)-\overline{I}\right)^2\right)\left(\sum_{r=1}^{N}\sum_{c=1}^{N}\left(X(r,c)-\overline{X}\right)^2\right)}} \quad (6)$$

Where I is the original image, X is the Embedded image, $\overline{I}$ and $\overline{X}$ stand for the mean values of the corresponding data set, and N×N is the image size.

## 6. EXPERIMENTAL RESULTS

The secret Arabic image shown in (Fig. 6 (a)) is used to be embedded in gray-level image (Lena image) shown in (Fig. 6 (b)).


*(a)* *(b)*

**Fig. (6): Original images (a) secret Arabic image (b) Cover image (Lena image)**

The Resultant images (Extracted secret image and Stego Lena image) from the Curvelet method are shown in (Fig. 7)


*(a)* *(b)*

**Fig. (7): Resulted images (a) Extracted secret Arabic image (b) Stego Lena image**

The proposed method is tested using six different grayscale images as shown in (Fig. 8). The expermintal results show that the stego image cannot be distinguished inside the cover image for all the different grayscale images. Only the results for the standard Lena image are given in this paper.

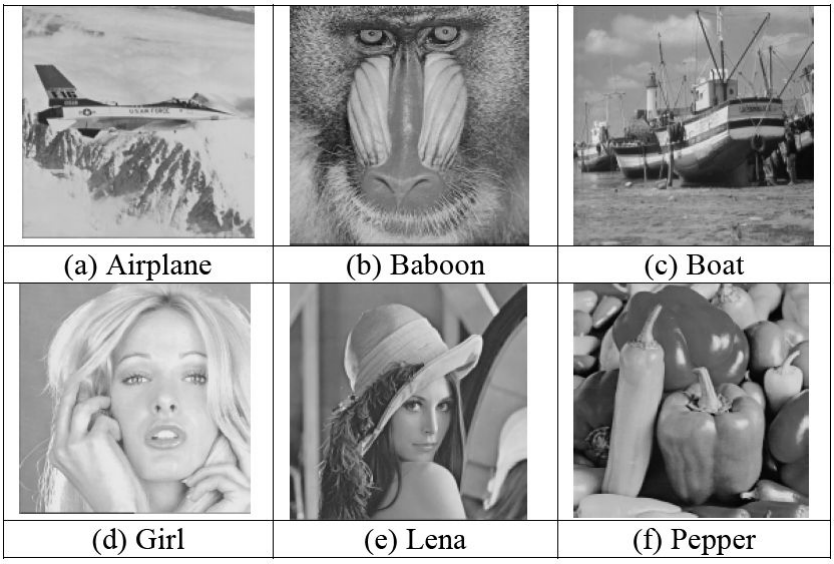



**Fig. (8): Original cover images**

**Table 1: Comparisons between the original cover image and the stego image**

| Stego Methods | PSNR /dB | Correlation |
|---|---|---|
| LSB Method | 47.1 | 0.9898 |
| DCT Method | 47.3 | 0.9948 |
| Wavelet Method | 47.4 | 0.9970 |
| Curvelet Method | **47.6** | **0.9998** |

**Table 2: Comparisons between the secret image and the extracted secret image**

| Stego Methods | PSNR /dB | Correlation |
|---|---|---|
| LSB Method | 20.9 | 0.9770 |
| DCT Method | 18.1 | 0.7685 |
| Wavelet Method | 20.2 | 0.8997 |
| Curvelet Method | **21.1** | **0.9999** |

## 7. DISCUSSION

The size of the resultant secret image and the experimented stego image are both 256 × 256 pixels, as shown in Fig. 7(a), Fig. 7(b) respectively.

In LSB and DCT methods, the size of the cover image must be at least twice the size of the secret image. Here the cover image resized to 512 × 512 and the secret image resized to 128 × 128, So that only 2 LSB used.

In Wavelet method, the size of the cover image must be twice the size of the secret image. Here the cover image resized to 512 × 512 size.

The secret image is embedded in the cover image using the four steganographic methods described above. Table (1) shows the results of the PSNR and Correlation values between the original cover image and stego image for the proposed method. It also shows results of Simple LSB, DCT, and Wavelet methods. Table (2) shows the results of the PSNR and Correlation values for the different methods between the secret Arabic image and the resulted one.

In all cases it was found that the Curvelet transform dominates the wavelet transform in terms of PSNR and Correlation test. The Curvelet steganographic image appears closer to the original image than the other methods. Since the Cuevelet Transform represents edges better than Wavelet, It

provides high PSNR values, high correlation values than Wavelet, DCT, and LSB methods. Also the resulted secret image appears the same as the original secret image. While other method extracts the image with lower resolution than Curvelet method.

## 8. CONCLUSIONS

This paper presents a new and simple algorithm for hiding binary secret images in gray level images. The secret image and the cover image both of the same size, while in old methods the secret image must be at most half the size of the cover image. The proposed method results a stego image and extracted image closer to the original images than the other methods. The Curvelet Transform represents edges better than other Transforms. Since edges play a fundamental rule in image understanding, one good way to enhance spatial resolution is to enhance the edges. It is clearly shown that the Curvelet steganographis method results better embedded and extracted secret image from the other methods.

For the sake of security, the embedded image should look intact to the human eye. Even though the hackers know that something is hidden in the image, they still cannot recover the secret image because this method randomly permuted the data by using Radon transform and a secret key.

## 9. REFRENCES

[1] A. Kumar and N. Rajpal "Application of T-Code, Turbo Codes and Pseudo-Random Sequence for Steganography" Journal of Computer Science 2, Vol .2, PP. 148-153. 2006.

[2] N. F. Johnson, Z. Duric, and S. Jajodia "Information Hiding: Steganography and Watermarking Attacks and Countermeasures" Published by: Kluwer Academic Publisher, 2001.

[3] H. Kharrazi and N. Memon "Image Steganography: Concepts and Practice". Published by: WSPC, 2004.

[4] J. G. Yu, E. J. Yoon, S. H. Shin and K. Y. Yoo "A New Image Steganography Based on 2k Correction and Edge-Detection" IEEE 5th International Conference on Information Technology: New Generations, 2008.

[5] M. K. Olszewski and K. Ch. Macukow "Optical steganography: a snapshot of the present" Proceeding of the Symposium on Photonics Technologies for the 7th Framework Program, 2006.

[6] G. Wallace, "The jpeg still picture compression standard" IEEE Transactions on Computer Electronics, Vol. 38, PP. 13-34, February 1992.

[7] K. B. Raja, Vikas , K. R. Venugopal, and L. M. Patnaik “High Capacity Lossless Secure Image Steganography using Wavelets” IEEE International Conference on Advanced Computing and Communications, Surathkal , 2006.

[8] J.L. Starck, E. Candes, and D. Donoho “The Curvelet Transform for Image Denoising“ IEEE Trans. Image Processing , Vol. 11, PP. 670- 684, June 2002.

[9] A. Eskicioglu , P. Fisher "Image quality measures and their performance” IEEE Transactions on Communications, Vol. 43, No.12, PP. 2959-2965, 1995.