International Journal of Applied Electromagnetics and Communication Systems
Volume 1, Issue 04, 2025

CHAOS AND CONTOURLET TRANSFORM-BASED HIGH CAPACITY STEGANOGRAPHY FOR HIDING MULTIMEDIA DATA

L.M. Pankatov
Nizhny Novgorod State University, 23 Gagarin avenue, Nizhny Novgorod, 603950, Russia

Research Article

Date of Submission: 29-08-2025 **Date of Acceptance: 26-09-2025** **Date of Publication: 19-11-2025**

ABSTRACT

Steganography is one of the most significant subdisciplines in the field of information concealment, which has proved successful in recent years. Numerous algorithms seemed to be focused on creating effective practical steganography systems. The study of steganography deals with concealing hidden information in various carrier media, such as images, audio, structured text, or video. The primary goal of this is to hide the presence of data itself. Here, we deal with steganography of images. This work presents image steganography techniques (both blind and non-blind) based on the chaotic system and the contourlet transform. The chaotic system is used for a number of reasons, the first of which is the use of a Modified Arnold Cat Map (MACM) to increase the key space, making it extremely difficult for the adversary to extract the secret message. This approach involves embedding in the Contourlet domain, which offers a huge embedding capacity. The proper embedding site is then carefully chosen to reduce the distortion on the cover picture and prevent this procedure from being detected. Experiments and comparative analyses demonstrated how well the suggested method produced stego pictures. Additionally, a comparison with a comparable wavelet-based steganography method demonstrates its superiority. PSNR, SNR, and correlation were used to gauge how similar the stego picture was to the cover image in order to determine the stego image's quality.

KEYWORDS: Contourlet Transform, Blind and Non-Blind Steganography, and Modified Arnold Cat Map.

1- INTRODUCTION

The ancient art of steganography has seen a resurgence in recent years. The term "steganography," which has Greek origins and literally translates to "covered writing," is often used to refer to the practice of concealing information between other pieces of information [1]. An ancient technique for transmitting messages covertly is steganography. The ancient Greeks were the first to use this technique of message masking.

Spies from both sides employed "invisible ink" during World War II [2]. Capacity, security, and resilience are the three most crucial requirements for a steganographic method [3].

-Capacity is the amount of information that a data concealing strategy can effectively embed in the tagged medium without causing any discernible distortion.

- Safety. If the embedded information cannot be eliminated beyond trustworthy detection by targeted assaults based on a thorough understanding of the embedding technique and detector, the embedding algorithm is considered safe.

-Sturdiness. If the embedded data can be consistently identified after the picture has been altered but not completely destroyed, it is considered resilient.

Digital steganography techniques are divided into two categories depending on the embedding domain: (i) spatial domain and (ii) frequency domain. By altering a pixel's value, the

secret message is immediately incorporated into the host picture using the spatial domain approach. Transform domain attempts to encode message bits in the image's transform domain coefficients. Transformed ones are more resilient than those in the spatial domain. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and others are examples of transform domain approaches. Because DWT performs better than other transform domain approaches, it is often utilized for digital steganography. DWT is a temporal frequency and multiresolution representation. It fails to capture smoothness along the contours and only records the discontinuities at the image's edges in three directions at each resolution. The Contourlet Transform (CT) has provided a solution to this issue.

Aperiodic long-term behavior in a deterministic system is called chaos. Chaos is formally described as "randomness" produced by basic deterministic systems; this randomness results from the sensitivity of chaotic systems to the starting circumstances. Lorenz (1963) pioneered the topic.A map that displays chaotic activity in order to boost security is called a chaotic map. Chaos's great sensitivity to beginning circumstances is its most alluring trait in the information concealing domain.

Each of the steganography approaches has been the subject of several studies, some of which are briefly described here:High capacity steganography techniques are offered in research studies [5–7], chaos-based steganography techniques are published in research studies [8–10], and steganography based on contourlet transform is presented in research studies [11–13].

Both kinds were used in this work: blind systems, which allow the receiver to extract hidden information without the original cover picture, and non-blind systems, which need the original cover image for comparison and secret information extraction. In order to reduce the distorting effect in the cover image, the cover was broken down into multiple levels using the contourlet transform (CT). The energy of the subbands was then calculated to conceal the information in the subbands with lower energy. The secret information was then embedded using a chaotic map, which was used to shuffle the secret information throughout the cover image.

2. PROPOSED APPROACH

2.1 CHAOTIC MAP

A map that displays some kind of chaotic activity is called a chaotic map. Discrete-time or continuous-time parameters may be used to parameterize maps. Iterated functions are often used to represent discrete maps [4]. A deterministic map is defined as an evolution equation given by a function f:M M mapping a space M to itself that results in a time series {x(i)} that satisfies the connection x(n + 1) = f(x(n)) = fn(x(0)).It is often taught how the map works on the unit square.

with a picture of a cat, which gave the map its name. The mathematical formula is [14]: C(x; y) = (x+y mod 1, x+ 2y mod 1)

$$= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1 \qquad (1)$$

where "a" mod 1 .means the fractional part of "a" for any real "a". Denoting the square 2×2 matrix as A .|A |is equal to 1. Equation (1) is one-to-one, each point of the unit square is uniquely mapped into another point in the unit square. The Lyapunov exponents of the Arnold cat map are calculated

by finding the eigenvectors of the matrix in eq. (1) [16] were: $\lambda 1 = \frac{3+\sqrt{5}}{2}$, $\lambda 2 = \frac{3-\sqrt{5}}{2}$, we see that λ1

>1 and λ2 < 1 , Hence, the Lyapunov exponents of eq. (1) are ι1=ln(λ1) ,ι2=ln(λ2).It is clear that one of the Lyapunov exponents, i.e., λ1, is positive

It can be easily seen that the original Arnold transformations given by equation (1) can be modified to produce a sequence of Arnold transformations ,and One way to generalize the above 2-D Arnold cat map can be achieved by introducing new parameters(a_1,b_1,c_1) to increase and ensure high security implementation a as follows [14],assume that we have an N × N image P. Arnold cat map is given as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & b_1 + c_1^2 \\ a_1 & 1 + a_1 b_1 + a_1 c_1^2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod N \qquad (2)$$

where a_1,b_1 and c_1 are positive control parameters ∈ R , (x' , y') are the coordinate values of the shuffled pixel.One can easily notice that ,|A |is equal to 1, which means that eq. (2) is one-to-one. Furthermore to find the LE of this matrix first we must find the eigenvalues of A .

i.e. ι1=ln(λ1) ,ι2=ln(λ2), we see that λ1 >1 and λ2 < 1 when we choose (a_1, b_1 , c_1) > 0 and (a_1, b_1 , c_1) ∈ R , one of the Lyapunov exponents is positive, so we use these parameters as control to increase the security.

2.2 THE CONTOURLET TRANSFORM

The contourlet transform is a "true" two-dimensional transform that can capture the intrinsic geometrical structure that is crucial in visual information. The limitations of widely used separable extensions of one-dimensional transforms, such as the Fourier and wavelet transforms, in capturing the geometry of image edges are well known. Similar to how wavelets were generated from filter banks, this discrete-domain multiresolution and multidirection extension makes use of nonseparable filter banks. The contourlet transform is the term given to this design because it produces a flexible multiresolution, local, and directed picture expansion utilizing contour segments [15].
The contourlet transform was created by Do and Vetterli based on an effective two-dimensional multiscale and directional filter bank that can handle smoothly contoured pictures. The contourlet transform is computationally efficient because it takes use of iterated filter banks; for an N-pixel picture, it needs O(N) operations [16].
The wavelet transform only offered the first three of these characteristics, but the contourlet transform had all of them [15]:

1) Multiple solutions. 2) Place. 3) Sampling critically. 4) Directionality. 5) Anisotrop

2.2.2 THE CONSTRUCTION OF THE CONTOURLET TRANSFORM

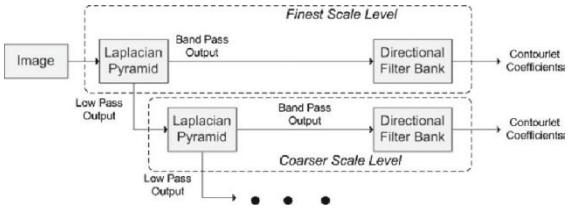
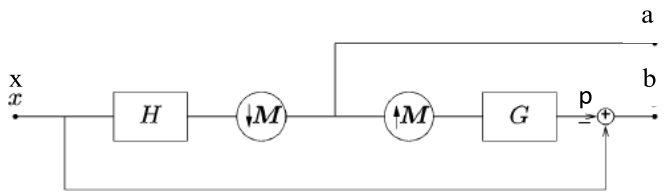


Figure (1) An illustration of Contourlet Transform

Figure(1) shows the construction of the contourlet transform.The contourlet transform is a combination of two transforms namely:
1) The Laplacian Pyramid (LP) with special filters and reconstruction scheme .For dividing the image into a low pass and a high pass subband.
2) A two dimensional directional filter bank for splitting the high pass subband into different spatial frequency orientations. The combined properties of these transforms provide us with the desired properties of a multi

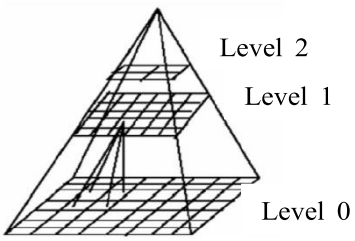
directional transform for digital images , and by successively applying the transform on the low pass image, we also achieve a multiresolution representation[16]. Figure (2) depicts this decomposition process, whereH and G are called (lowpass) analysis and synthesis filters, respectively, and M is the up or down sampling matrix. The process can be iterated on the coarse (downsampled lowpass) signal[15].



Figure(2) Laplacian pyramid (one level LP decomposition).

Where x : the original image, a : coarse approximation, b: the difference between the original x and prediction image p. For one level LP decomposition ,the Laplacian pyramid generates a down sampled low pass version of the original and the difference between the original "x" and the prediction "p", resulting in a bandpass image "b" (prediction error) see figure(2) [17].

By repeating these steps several times a sequence of images are obtained. If these images are stacked one above other ,the result is a tapering pyramid data structure as shown in figure(3).



Figure(3) Laplacian pyramid

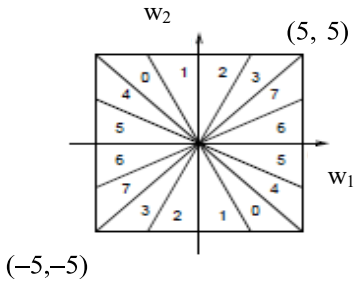


Figure (4) Directional filter bank frequency partitioning L= 3 and there are 23 = 8 real wedge-shaped frequency bands

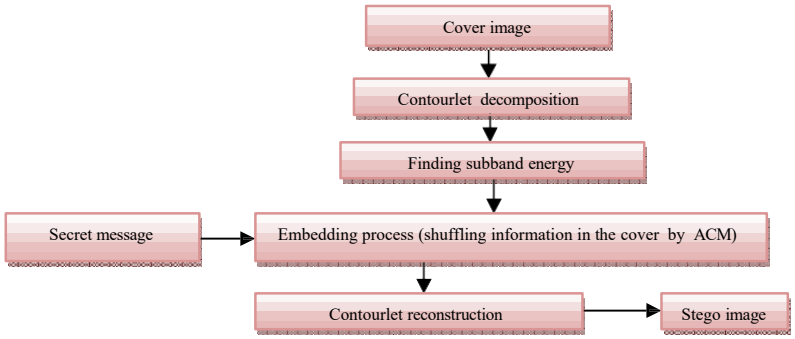
a 2-D directional filter bank (DFB) with flawless reconstruction and maximum decimation. As shown in figure (4), the DFB is effectively implemented by an L-level tree-structured decomposition that results in 2L subbands with a wedge-shaped frequency partition [16].

2.3 IMPLEMENTATION OF THE PROPOSED SYSTEM

This piece involves both text and visual concealment. In addition to the quality of the stego picture as compared to the original cover, we have shown interest in the extracted secret information quality in these methods.

2.3.1 THE TRANSMITTER SIDE

Every algorithm is used in both blind and non-blind systems. In all of these algorithms, the transmitter analyzes the cover (digital image) into multiple levels using contourlet transform CT (decomposition) and calculates the energy of the subbands to conceal the information in the subbands with less energy to reduce the distorting effect in the cover image. Next, we embed the secret information using a chaotic map (Arnold cat map), which was used to shuffle the secret information throughout the cover image. Finally, (ICT) performs the reconstruction to obtain the transmitter stego-image, as illustrated in figure 5.

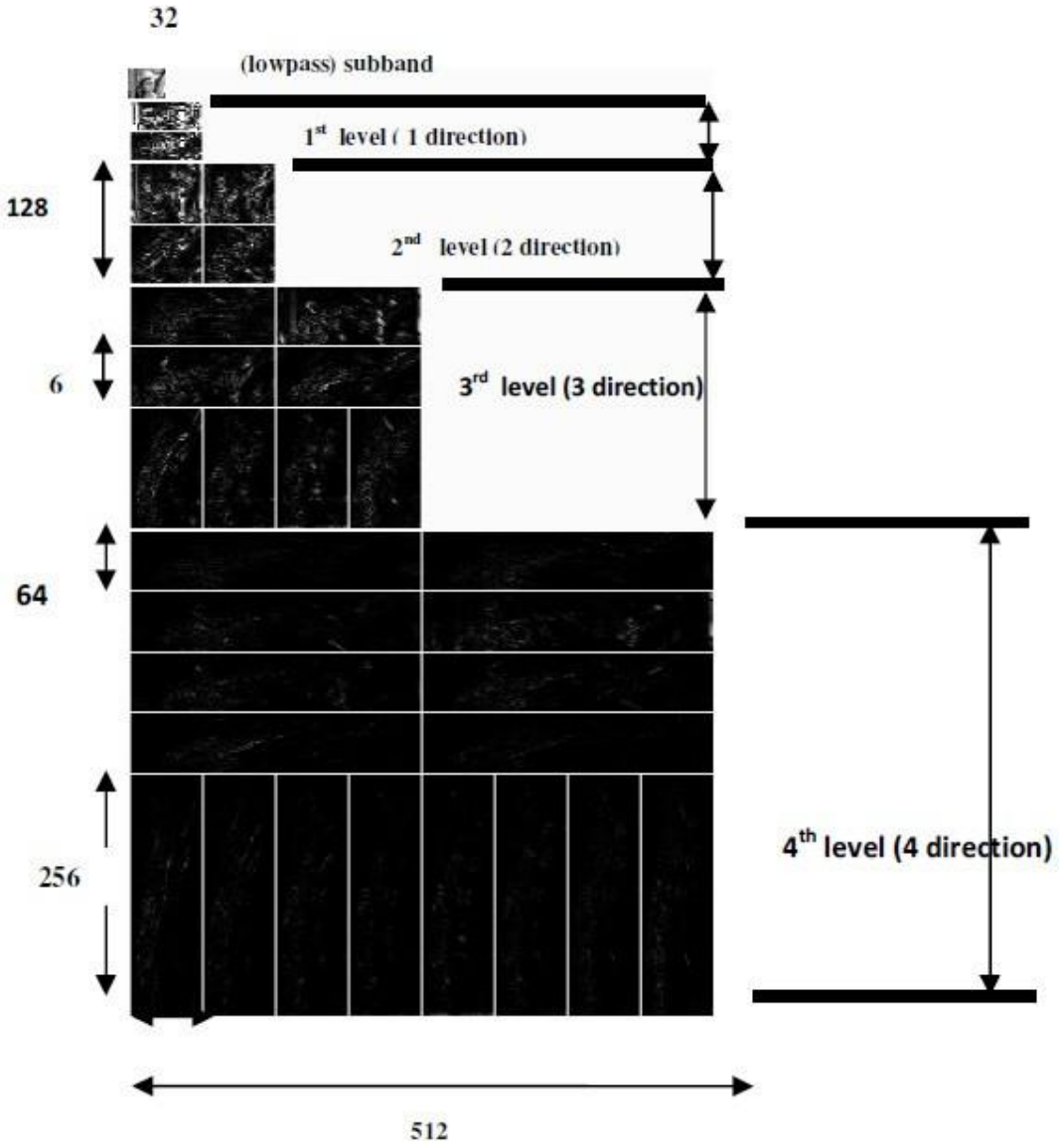


Figure(5) The main block diagram at the transmitter side

In these systems, the cover image should first be carefully chosen, such as a cover with low details, so that the contourlet transform (CT) can breakdown the cover picture when the high frequency is substituted with another piece of information. The first subband in this transform is the low pass region, which is created by applying Laplacian Pyramids (LP), which split the image into a low pass and high pass subband. If this process is repeated multiple times, the low pass subband is split at multiple levels. The high pass subband is then split using the directional filter bank (DFB).An m-level binary tree decomposition that results in 2m frequency partitioning is an effective way to construct the DFB. Let's use the following sequence to illustrate these steps:[L]=[ℓ_1 , ℓ_2, ℓ_3 , ℓ_4 , ... ℓ_m]

Where m: no. of level, and ℓ_i =number of directions of the ith level , up to 2^ℓ_m number of subbands . The dimension of the cover should be power of two (2n), where n:is an integer .

- If [L]=[1,2,3,4] ,the first level has 21=2 subbands, the second level has 22=4subbands ,the third level has 23=8 subbands, and the fourth level has 24=16 subbands as shown in fig.(6) where the dimension of the low pass subband is (32×32) only and all of the others are high frequency, the dimension of the high frequency subband for the first level is (32×64) for both of the subband, for the second level is (64×64) for all of the subbands, for the the third level is (64×128) for all of the subbands, and for the the fourth level is (64×256) for all of the subbands , adding together for all levels ,then we have: 32*32+(2*32*64)+(4*64*64)+(8*64*128)+(16*64*256)=349,184 coefficients



Figure(6) 4-level Contourlet decomposition

The information will now be included into the cover picture (let's say a 512 by 512 lena). Figure (6) illustrates the usage of a four-level decomposition of the contourlet transform in this study.The last stage would be the embedding process.The amount of the information to be contained in the highpass subband will define the number of directions in the final level. The location of the secret information will then be chosen based on the energy of the subbands.Equation (3) will be used to determine the contourlet coefficients' energy:

$$E = \sum i \sum j \left| s(i,j)^2 \right| \quad \ldots\ldots.(3)$$

Where $0 \leq (i, j) \leq N$, s(i,j):the value of the contourlet coefficient .

Then by aapplying Modified Arnold Cat Map(MACM) to an image the result becomes imperceptible or noisy ,where(a_1 ,b_1 and c_1) are positive control parameters as a secret key between

the sender and recipient . This operation will be used inside the embedding process to shuffle the secret information overall the intended subband. Let's consider a (4×4)block , then if (MACM) is applied on its pixels then new positions of each pixel as in figure(7).

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



16	2	8	10
9	15	1	7
6	12	14	4
3	5	11	13

Figure (7) Applying MACM to (4×4)block and(a_1=2,b_1=3,c_1=4)

2.3.1.1 EMBEDDING ALGORITHMS

2.3.1.1 A HIDING IMAGE IN IMAGE

The steps for this algorithms as shown in figure(8) are:

1- After preparation of the cover image(C)
2- Convert the secret image into vector(1-dimension)(SV1-blind)&(SV2-non-blind).
3- Multiply by a factor SV1'= SV1*α and SV2'=SV2* α.
4- Generate modified MACM.
5- If the system is blind then replace the value of coefficient S(i,j) by the value of SV1',else adding the value of SV2' to the original value of the coefficient in case the system is non-blind.
6- Reconstruct by(ICT)to give the stego Image.

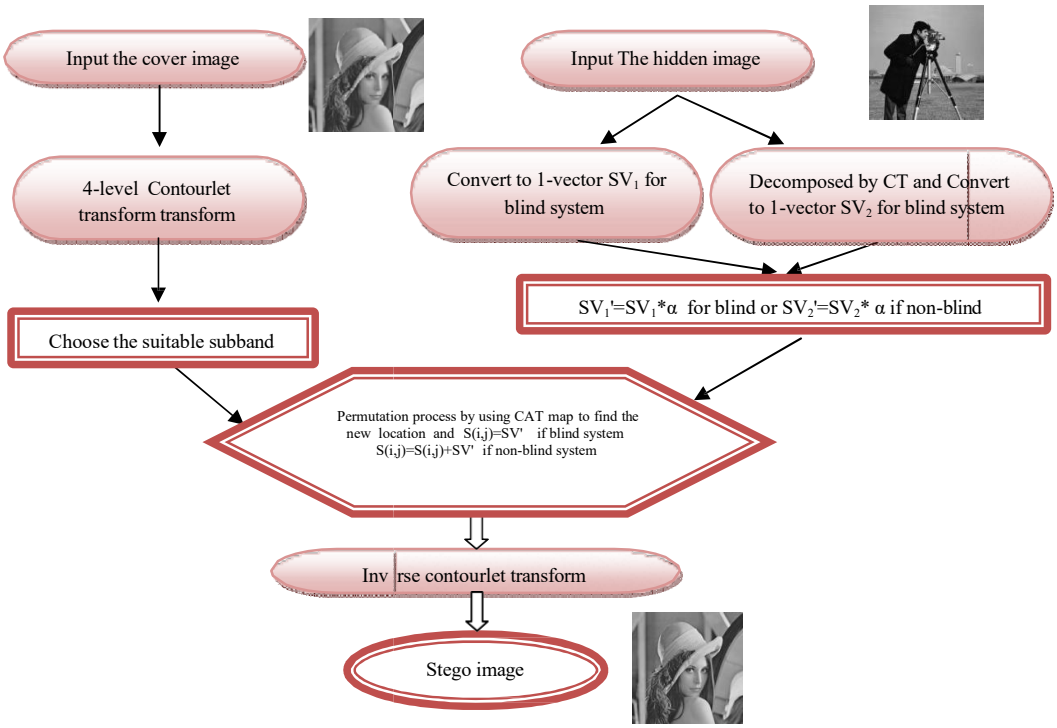


Figure (8): Block diagram of Hiding image in image

2.3.1.1 b: HIDING TEXT IN IMAGE

The steps for this algorithms as shown in figure(9) are:

1- After preparation of the cover image(C), the secret text message(S) of size M*N will be converted into jpeg image S2 and each pixel is represented by (8-bit/pixel).

2- Thresholding S2(i,j) to convert it into (1-bit/pixel) S2'(i,j) by using the mean(μ).

$$\mu = \frac{\sum_i \sum_j P(i,j)}{M \times N} \quad \ldots\ldots(4)$$

Where $0 \leq (i, j) \leq N$, P(i,j):the value of the pixel .

3- Generate modified MACM.

4- Replace the value of coefficient S(i,j) by the value of ± β if the system is blind else adding the ± β to the value of coefficient if the system is non-blind .

5- Reconstruct by(ICT)of the modified cover image(Stego Image)

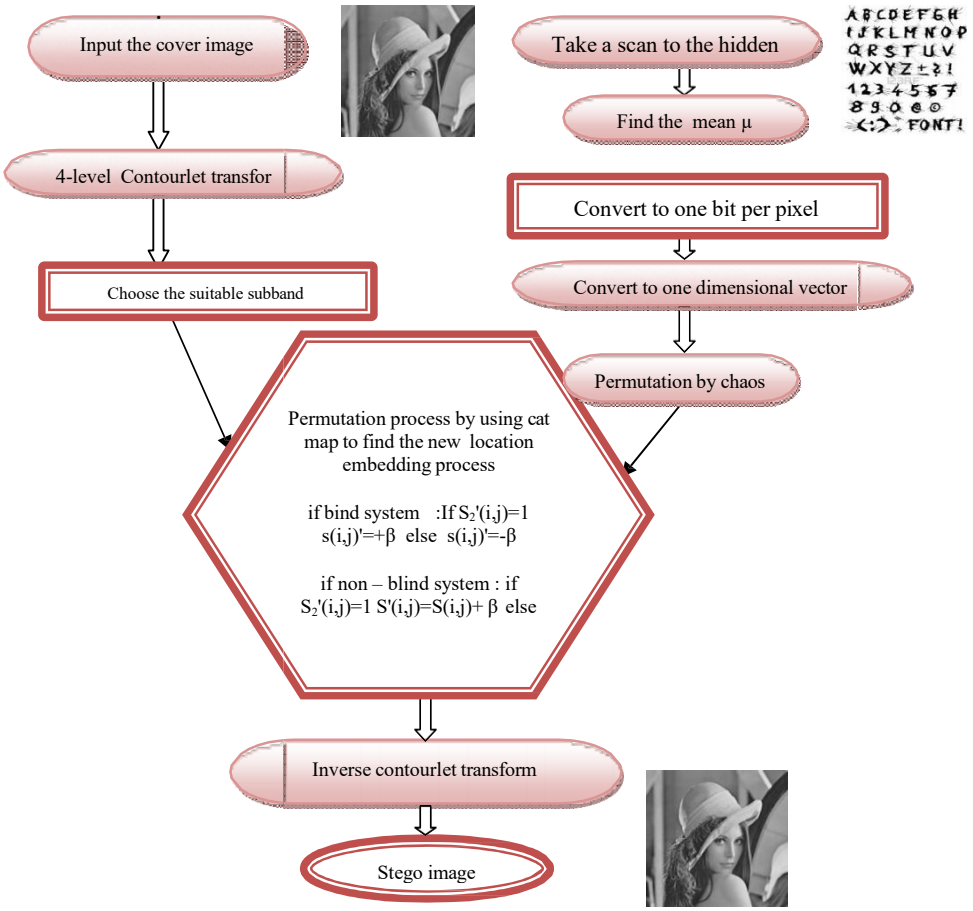


Figure (9) :Block diagram of Hiding text in image

2.3.2 EXTRACTING ALGORITHM AT THE RECEIVER SIDE

The MACM secret key (a1, b1, c1) must be known by the recipient. This key was used during the embedding procedure created using the Modified Arnold Cat Map. The values of (α,β,θ) were used to conceal text in the picture and images in the image, respectively. Using the same filters employed on the transmitter side, the 4-level contourlet transform breaks down the stego picture to identify which subband was utilized to contain the data. As was previously said, the extraction method is the opposite of the embedding algorithms.

3. EXPERIMENTAL RESULTS

The performance of the proposed algorithms is shown using experimental findings in this section. By concealing the secret data in higher contourlet coefficients, the suggested steganography method increases the embedding capacity and decreases the visual distortion of the stego image. In addition, we employ a chaotic map to boost security because, when a powerful algorithm is employed, the only way to break the system is to obtain the key. Matlab* (R2013a) is used to develop the suggested systems, and the testing were conducted on a personal computer with a 2.80 GH CPU (CORE i7).

3.1 MEASURING OF THE QUALITY

The quality of the picture may be assessed using a variety of techniques. First, it was discovered that the statistical characteristics of the cover image were unaffected by altering certain coefficients. Therefore, if the cover image's histogram is almost identical to the cover image's histogram, the suggested system was effective enough to evade the attackers. Additionally, the normalized correlation between the stego-image and cover-image was assessed. Therefore, the normalized correlation equals one when the stego-image and the original cover-image are perceptually comparable [2].

$$\mathrm{Cor} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\bar{C})(St(i,j)-\bar{St})}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\bar{C})^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(St(i,j)-\bar{St})^2\right]}} \quad (5)$$

where: i: row number, j: column number, M: No. of rows of the cover image, N: No. of columns of the cover image, C(i,j): cover image, St(i,j): stego image, $\bar{C}$: the mean of C(i,j) and $\bar{St}$: the mean of St(i,j). And PSNR is usually measured in dB and given by:

$$\mathrm{PSNR} = 10\log_{10}\frac{(L-1)^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(St(i,j)-C(i,j))^2} \quad (6)$$

Typical PSNR values range between 20 and 40 dB [2]. And the last test is Signal-to-Noise-Ratio (SNR),This is given in dB by :-

$$\mathrm{SNR} = 10\log_{10}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j))^2}{} \quad (7)$$

3.2 KEY SPACE AND KEY SENSITIVITY ANALYSIS

A safe system should have a key space big enough to prevent brute force attacks. The time it takes an attacker to execute a brute force attack—in which the attacker tries every conceivable key combination to breach the system—increases exponentially with increasing key length [9]. This algorithm may make use of the MACM parameters a1, b1, and c1 as well as the subband division method (selecting the number of DFB) and the subband dimensions m, n.as keys, hence any exhaustive search through all potential keys is unfeasible to get the secret data since the sum of these keys is huge. Because steganography methods lessen the likelihood of the secret message being discovered, chaotic permutation makes the suggested system more secure.

3.3 RESULTS

Then the results of implementing the algorithm including different type of data (image and text) to be embedded in the cover image. Contourlet transform based steganography was used. This transform provides multiscale and multidirectional representation of an image .The directionality is a power of tow (2^L) where L=[0-7] depending on the size of the image ,so more directionality means less LL coefficients and more HH coefficients which is more suitable for embedding on it ,in the table(1) the energy for different cover image are listed:

- peppers.png for L=[2,2,2]

Table (1) Energy for the subbands for L=[2,2,2]

Peppers.png (512×512)	**{1,3}{1,1}**	**{1,3}{1,2}**	**{1,3}{1,3}**	**{1,3}{1,4}**
	2772.2	894.6076	36.4840	4107.1475
	{1,4}{1,1}	**{1,4}{1,2}**	**{1,4}{1,3}**	**{1,4}{1,4}**
	8577.704	13.3210	1.6398	1055.52134

So after noticing the subbands energy for the level which be choosed and comparing between them to choose in which subband the secret message would be embedded.

3.3.1 RESULTS OF HIDING IMAGE IN IMAGE

This is done by using (512×512)pixels of different cover images ,the size of secret images is varied with variable capacity and variable control parameter α.

3.3.1.1 NON-BLIND SYSTEM

Table(2)shows the results of the quality of the stego image with the size of the secret image that would be embedded in the cover image.The cover image is lena (512×512) and the secret image is the monaliza for different sizes.

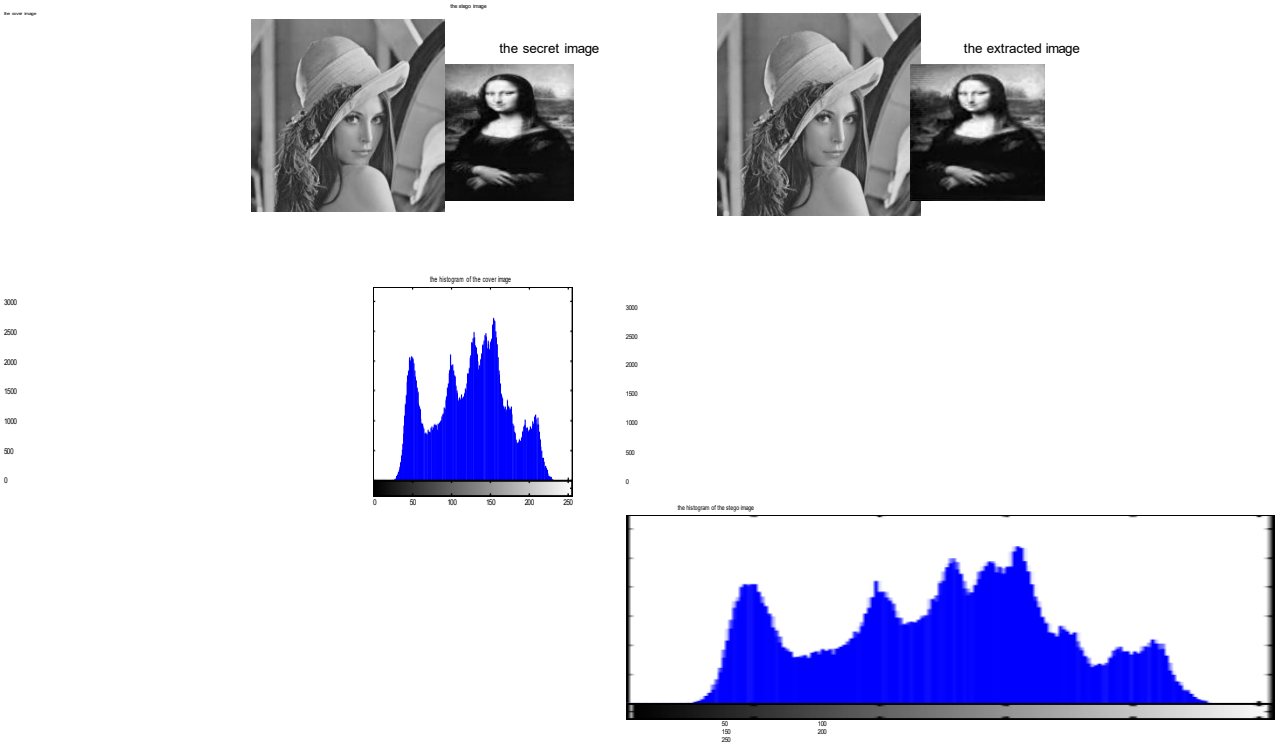
Table(2) Stego image results for different size of the secret image with α=0.05 for non blind system

Dimension of the secret image	**Capacity(%)**	**PSNR** dB	**N.corr.**	**SNR** dB
32*32	**0.39**	59.3170	1	48.1478
32*64	**0.78**	56.2821	1	45.9236
64*64	**1.56**	53.1136	0.9999	45.6374
64*128	**3.125**	49.3010	0.9998	41.2788
128*128	**6.25**	47.5672	0.9998	36.9841
128*256	**12.5**	46.9269	0.9996	36.5478
256*256	**25**	46.7716	0.9992	38.3868
256*512	**50**	42.1048	0.9991	33.8184

Table(3) Results of the stego image for lena as a cover(512*512) and monaliza as a secret image(128*128) for non blind system

	Stego image			Extracted image		
α	**PSNR dB**	**SNR dB**	**N.Corr**	**PSNR dB**	**SNR dB**	**N.Corr.**
0.01	61.3785	50.8087	1	23.1512	14.8374	0.9783
0.03	51.9508	41.4356	0.9999	28.2989	20.2329	0.9922
0.05	47.5672	36.9841	0.9998	30.1912	21.9307	0.9951
0.08	43.4971	32.8844	0.9994	31.1724	22.5636	0.9966
0.1	41.5703	30.9552	0.9990	31.4585	22.7344	0.9972
0.13	39.2936	28.6760	0.9983	31.8254	22.9192	0.9975
0.15	38.0545	27.4295	0.9978	32.0404	23.0317	0.9976
0.18	36.4841	25.4841	0.9968	32.2524	23.2396	0.9977
0.2	35.5842	24.9989	0.9961	32.1790	23.3350	0.9976

The results in table (3) shows the effects of changing the value of the control parameter (α) on the qualities of the stego image and the extracted image.



Figure(10) Histogram results of embedding the cover lena(512*512),the secret monaliza (128*128) for non blind system

Figure (10) shows the histograms of the original cover and stego image for a cover image with (512*512). One can notice that there is no major change in shape of the histogram.

3.3.1.2 BLIND SYSTEM

We use a variety of scenarios, such as altering the capacity, altering the values of alpha(α), and comparing the quality of the extracted picture and the stego image, as shown in table (4), to assess the system's quality. The hidden picture is peppers.png (256x256), whereas the cover image is lena.bmp (512x512).

Table(4) The results of embedding the cover(512×512),the secret (256×256) for blind system

	Stego image			**Extracted image**		
α	**PSNR dB**	**SNR dB**	**N.Corr**	**PSNR dB**	**SNR dB**	N.Corr.
0.03	43.6193	35.1047	0.9994	17.8763	10.1711	0.9172
0.05	41.8646	33.6388	0.9991	21.6297	13.9355	0.9617
0.08	39.3426	31.0055	0.9983	24.0716	16.4329	0.9828
0.1	37.8269	29.3821	0.9977	24.9989	17.3260	0.9872
0.13	35.9229	27.3669	0.9964	25.6198	17.8824	0.9905
0.15	34.8084	26.1979	0.9953	26.0000	18.2226	0.9918
0.18	33.3595	24.6926	0.9935	26.2630	18.4496	0.9930
0.2	32.5037	23.8084	0.9921	26.3730	18.5350	0.9934

Table(5) The results of embedding variable size on the cover lena (512×512) with α=0.06 and secret image is monaliza with variable size for blind system

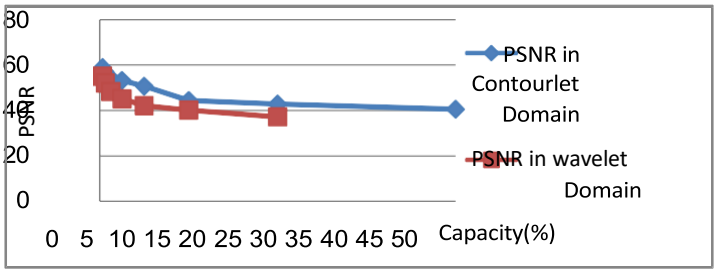
Dimension of the secret image	**Capacity(%)**	**PSNR dB**	**N.corr.**	**SNR dB**
32*32	**0.39**	58.7759	49.4867	1
32*64	**0.78**	57.0029	47.0876	1
64*64	**1.56**	54.3417	45.3417	0.99994
64*128	**3.125**	53.1702	45.3047	0.99993
128*128	**6.25**	50.6927	41.9723	0.99991
128*256	**12.5**	44.3951	35.1540	0.9995
256*256	**25**	42.7789	34.4404	0.9992
256*512	**50**	40.5488	33.6906	0.9987

Table(5) shows the results of embedding variable size on the cover lena (512×512) with the secret image is monaliza with variable size. To compare with a wavelet –based steganography system by setting L=[0]

the size of the secret image is varied to see the difference between the two systems , see table (6) and figure (11).The cover image is lena (512×512) and the cover image is monaliza with α =0.06.

Table(6) Embedding in wavelet domain with α =0.06

Dimension of the secret image	Capacity(%)	PSNR dB	SNR dB	N.corr.
32*32	**0.39**	55.0306	45.4232	1
32*64	**0.78**	52.1209	43.5882	0.99991
64*64	**1.56**	48.2854	36.8436	0.9998
64*128	**3.125**	45.1342	35.4257	0.9996
128*128	**6.25**	42.1410	32.7139	0.9991
128*256	**12.5**	40.1644	33.8576	0.9986
256*256	**25**	37.1554	31.1395	0.9973



Figure(11) Comparison between contourlet and wavelet based steganography blind- system (the cover image is lena(512×512)and the secret image is monaliza with variable size and α =0.06)

Several simulations have been run to assess the performance of the suggested system and compare it to other current methods. Table (7) compares our suggested method with ref. [18–19] for image hiding. For testing purposes, a cover image is chosen to be the lena image (512 x 512) with a hiding capacity of 25%. In [18], steganography based on wavelet and integer wavelet domain is used, whereas in [36], Intermediate Significant Bit Planes are used.

Table (7) Comparison between proposed method and ref.[18-19]

Hiding capacity 25%	Based on wavelet	Based on integer wavelet	Based on intermediate significant bit	Proposed method
PSNR dB	41.10	41.32	37.5516	**42.7789**

3.3.2 RESULTS OF HIDING TEXT IN AN IMAGE

To evaluate the quality of the secret message and the stego picture, a copy of a text message will be taken in different sizes. Figure (12) lists the text message samples that this method uses.



a- T1 **b-** T2

Figure (12) Different secret text messages used

3.3.2.1 NON-BLIND SYSTEM

Figure (15) depicts the embedding of text message (T2) on the cover picture (lena), while Table (8) displays the quality of the stego image based on the size of the secret message that would be embedded in the cover image

Table(8) Results of embedding, the cover (512*512) with different size of secret message for non blind system

dimension	**No.of bits**	**Stego image**			**Extracted image**		
		PSNR dB	SNR dB	N.Corr	PSNR dB	SNR dB	**N.Corr.**
32*32	1,024	69.3646	63.2467	1	51.3682	42.4736	**1**
64*64	4,096	63.0397	46.9229	1	50.9742	40.7584	**1**
128*128	16,384	56.8879	50.6224	1	48.6745	35.5143	**1**
128*256	32,768	55.0724	49.0867	1	45.9783	30.1496	**1**
256*256	65,536	47.0590	37.5902	0.9998	40.3833	22.3721	**0.9997**
350*375	131,250	44.6547	37.7035	0.9996	29.3912	17.3222	**0.9955**
365*403	147,095	44.5187	37.8660	0.9996	29.1718	21.0575	**0.9952**

Table(9) The effect of beta on the non blind system

	Stego image		
β	**PSNR dB**	**SNR dB**	**N.corr.**
5	37.1676	30.8111	0.9973
4	39.1058	32.7493	0.9983
3	41.6046	35.2481	0.9990
2	45.1264	38.7699	0.9996
1	51.1470	44.7905	0.99997








Figure (13): Results of embedding the cover (512*512),the secret (350*375) (131,072)bit for non blind system

Table (9) shows the effect of changing the value of β on the quality of the system where the cover image is lena (512*512), the secret message is T2(350*375)bit. Figure(13) shows the embedding of text message (T2) on the cover image (lena). Table(10)shows the results of the embedding process for all of the secret message (T1-T2)with size(128*256)bit , the cover is women with(256*256) and β= 0.5.

Table(10) Results of embedding different text massage(128*256) in (256*256)cover image

	Stego image			Extracted message		
Secret message	**PSNR db**	**SNR dB**	**N.corr.**	**PSNR dB**	**SNR dB**	**N.corr.**
T1	56.8470	50.6402	1	25.8603	16.2964	0.9932
T5	56.5772	50.3260	1	42.1442	18.0618	0.9998

3.3.2.2 BLIND SYSTEM

Results of the stego (lena is a cover (512*512)) with different text message with size (256*256) are shown in table(11). If the value of beta is changed, the quality of both the stego and extract message will be affected as shown in table(12),where the cover image is women(256×256)and the secret is T1(128×128).

Table(11) Results of embedding different text message(256*256)bit in (512*512)cover image for blind system

	Stego image			Extracted message		
Secret message	**PSNR**	**SNR**	**N.corr.**	**PSNR**	**SNR**	**N.corr.**
T1	44.1165	35.3251	0.9995	23.7719	12.5742	0.9993
T2	44.1470	35.3267	0.9993	23.2798	13.4562	0.9995

Table(12) The effect of beta (β)on the stego image for blind system

	Stego image		
β	**PSNR**	**SNR**	**N.corr.**
5	39.7947	0.9984	34.5852
4	41.5323	0.9989	36.2457
3	43.6274	0.9993	38.1491
2	46.1686	40.1294	0.9996
1	48.9874	4.4063	0.9998

For a comparison between our proposed method and ref.[7] which is worked on steganography based

on Double Density Dual Tree Discrete Wavelet Transform (DD DT DWT). For testing purposes a cover image is selected to be the lena image (512×512) and a secret data is a binary sequence (0, 1) .Table (13) shows the comparison between our proposed system and system in ref. [7].

Table (13) Comparison between our proposed system and system in ref. [7]

	Ref.[7]	Proposed method
Hiding capacity	5000 bit	56,536 bit
PSNR	38.8541bit	**44.1475**

4. CONCLUSIONS

A good result for the extracted message was obtained, demonstrating the robustness of the suggested algorithm to be achieved for data hiding on image. The results obtained for various cover image types and secret message types showed that the stego image had very close properties to the original cover image, making it very difficult to distinguish between them. The high PSNR requirement and the high capacity demand are at odds. In general, an increase in capacity is accompanied by a rise in inaccuracy, which has an inverse effect on the PSNR, SNR, and NC. Capacity and these needs should be traded off. Because the Contourlet Transform has multiscale and multidirectional capabilities, it may expand the hidden message's capacity by up to half the size of the cover picture. By employing the characteristics of this chaotic map as a secret key between the transmitter and receiver, MACM (Modified Arnold Cat Map) improves system security. where compared to the identical system based on Wavelet, the results obtained from the proposed system (where the secret message was an image) clearly show that the embedding on the Contourlet Domain delivers greater quality of the stego picture up to 3.5dB higher than the system based on Wavelet.

REFERENCES

[1] [1] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "Secure Data Transmission Using Steganography and Encryption Technique," International Journal on Cryptography and Information Security (IJCIS), Vol. 2, No. 3, September 2012.

[2] [2]Firas A. Sabir, "Evaluation Of Information Hiding For Still Image," M.Sc. thesis, University of Technology, Baghdad, 2004.

[3] [3] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, 540-7993/03, 2003.

[4] [4] Michael D. Richard, "Estimation and Detection with Chaotic Systems," Cambridge, Massachusetts Institute of Technology, 1994.

[5] [5] Hedieh Sajedi and Mansour Jamzad, "Secure steganography based on embedding capacity," International Journal of Information Security, Volume 8, Issue 6, Springer-Verlag, pp. 433-445, 2009.

[6] [6] Rosanne English, "Comparison of High Capacity Steganography Techniques," IEEE, International Conference on Soft Computing and Pattern Recognition, 978-1-4244-7896-2, 2010.

[7] [7] Sushil Kumar and S.K. Muttoo, "A Multilayered Secure, Robust, and High Capacity Image Steganographic Algorithm," IEEE, 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE, 2008.

[8] [8] Niansheng Liu and Donghui Guo, "Multiple Image Information Hiding Technique Based on Chaotic Sequences," IEEE, International Conference on Convergence Information Technology, 0-7695-3038-9/07, 2007.

[9] [9]Ying Li, Qiang Zhang, and Na Ma "A Stratified Image-Hiding Method Based on Chaos" IEEE Fifth International Conference, Bio-Inspired Computing: Theories and Applications (BIC-TA), 978-1-4244-6437-1, 2010.

[10] [10] Mazhar Tayel, Hamed Shawky, and Alaa El-Din Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data," Advanced Communication Technology (ICACT), 14th International Conference on ICACT, February 2012, IEEE.

[11] [11] Robust Blind Digital Watermarking in Contourlet Domain, Sreejith V, Srijith K, Rajesh Cherian Roy, International Journal of Computer Applications, November 2012.

[12]

[13] [12] Hedieh Sajedi and Mansour Jamzad, "Contourlet transform and cover selection for secure steganography," Springer, 2010.

[14] [13] Malini Mohan & Anurenjan P.R., "A New Algorithm for Data Hiding in Images using Contourlet Transform," IEEE, Recent Advances in Intelligent Computational Systems (RAICS), 978-1-4244-9477-4/11,2011.

[15] [14]H. Farschi and Seyed Mohammad Reza Farschi, "A novel chaotic approach for information hiding in image," Nonlinear Dyn, Springer, 2012.

[16] [15] "The Contourlet Transform: An Efficient Directional Multiresolution Image Representation" by Minh N. Do and Martin Vetterli (Fellow IEEE), IEEE Transactions On Image Rocessing, Vol.14, No.12, December 2005.

[17] [16]Duncan D.-Y. Po and Minh N. Do (IEEE Member) "Directional Multiscale Modeling of Images using the Contourlet Transform" IEEE Transactions On Image Processing, Vol. 15, Issue 6, 2006.

[18] [17] Nagham Salim Mohammed Al-lella, "Contourlet Transformation for Data Hiding," M.Sc. Thesis, Computer Sciences and Mathematics University of Mosul, 2013
[18] Shabir A. Parah, Javaid A. Sheikh, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique," IEEE, International Conference on Emerging Trends in Science, Engineering, and Technology, 978-1-4673-5144-7/12, 2012.

[19] [19] Robust Image Adaptive Steganography using Integer Wavelets, K. B. Raja, S. Sindhu, and T. D. Mahalakshm, IEEE IMAGE PROCESSING, 2011.

[20] [20] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "Steganography Based on Random Pixel Selection for Efficient Data Hiding," International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 2, 2013, pp. 31–44, ISSN Print: 0976–6367, ISSN Online: 0976–6375.

[21] [21] Jaspreet Kaur and Chirag Sharma, "Multimodality Medical Image Fusion using Improved Contourlet Transformation with Log Gabor Filters," International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 2, 2013, pp. 383-389, ISSN Print: 0976-6464, ISSN Online: 0976-6472.

[22] [22]Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi, "An Improved Robust and Secured Image Steganographic Scheme," International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 3, 2012, pp. 22–33, ISSN Print: 0976–6464, ISSN Onlin**e: 0976–6472.**