Journal of Engineering and Sustainable Development
www.jeasd.org
Vol. 22, No.03, May 2018
ISSN 2520-0917

Multi-level Steganography System Using Wavelet Transform

Dr. Rajaa aldeen Abad Khalid [*1], Aman Ala'a Hussain[2]

1) Senior Lecturer, communication systems. Department of network engineering , College of information engineering , Al- Naheain Unversity, Baghdad, Iraq.
2) M.Sc., graduate , Department of communication and information engineering , College of information engineering , Al- Naheain Unversity, Baghdad, Iraq.

Abstract: Sending encrypted messages frequently will draw the attention of third parties, i.e. crackers andhackers, perhaps causing attempts to break and reveal the original messages. In a digital world, steganography is introduced to hide the existence of the communication by concealing a secret message inside another unsuspicious message.The aim of this paper isto produce proposed method to provide a high level security system by implementing and designing multi-level steganography system to hide data in a color video-cover. This system is more complex system, it implemented in two levels of embedding and this is an issue of the high level of security because it required two levels of extraction to extract the hidden data. The system is implemented in the frequency domain, using wavelet transform domain. The idea of using transformation in the proposed system is due to the results of previous published works which indicated the hiding in the frequency domain is more effective than hiding in time domain, due to compactness attributes of some transforms and due to its robustness. A singular value decomposition (SVD) is also used in this proposed system. MATLAB programming environment is used to simulate the total system.

Keywords: *Steganography, Watermarking , Wavelet Transform (WT),* DWT, *SVD* .

نظام اخفاء متعدد المستويات باستخدام محول ويفليت

الخلاصة: ان ارسال الرسائل المجفرة بشكل مستمر سيرسم التوجه لطرف ثالث هم كاسروا الجفرة و لصوص البيانات ، و ربما سيتسبب بمحاولات لكسر و كشف الرسائل الأصلية . في العالم الرقمي فقد قدم اخفاء الرسائل لتغطية وجود الأتصالات بواسطة تغطية رسالة سرية داخل رسالة اعتيادية لاتثير الشكوك .يهدف البحث الجاري الى انتاج طريقة مقترحة لتجهيز نظام امني عالي المستوى بواسطة تصميم و تنفيذ نظام اخفاء متعدد المستويات لأخفاء بيانات بغطاء فديو ملون . هذا النظام أكثر تعقيدا فقد تم تنفيذه بمستويين من التغطية أو التضمين السري وهذا ما يعطي المستوى العالي للأمان لأنه يتطلب مستويين من انتزاع المعلومات لاستخراج البيانات المخفية . و قد تم تنفيذ النظام في المجال الترددي باستخدام محول ويفليت ، و الفكرة من استخدام هذا التحويل في النظام المقترح هو بسبب ما أشارت اليه الدراسات السابقة بكون هذا النوع من التحويل أكثر فعالية والتي حددت ان التحويل في المجال الترددي أكثر تأثيرا من التحويل في مجال الزمن ، بسبب ميزات التضامن لبعض المحولات وباعتبار قوته عموما . كما تم استخدام مفكك القيمة المفردة (SVD) أيضا في هذا النظام المقترح واستخدم برنامج ماتلاب كبيئة لمحاكاة النظام كليا .

*Corresponding Author rajaajdeen@coie-nahrain.iq

1. Introduction

Today there is a lot of articles suggest the usage of Internet to pass different kinds of information using various techniques (including e-mail, chat room, bulletin boards and other web sites). There is also much speculation that some groups may use techniques of (data hiding) to help their communications. In order to ensure the privacy of the communication between two parties[1].

One of the hot spots in security research is Information Hiding. It is driven by two of the biggest policy issues of information age copyright protection (Watermarking) and state surveillance (Steganography), Steganography's intent is to hide the existence of a hidden message, 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[9].

An information hiding system is characterized by having three different aspects that contend with each other as shown in Figure 1, capacity, security, and robustness. Capacity refers to the amount of data bits that can be hidden in the cover medium, and robustness is concerned about the amount of modification the stego medium can resist before an adversary can modify or destroy the hidden information[4] and security relates to the ability of an eavesdropper to detect the hidden information easily. Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information. The closer the stego image to the cover image, the higher the security[2,3].

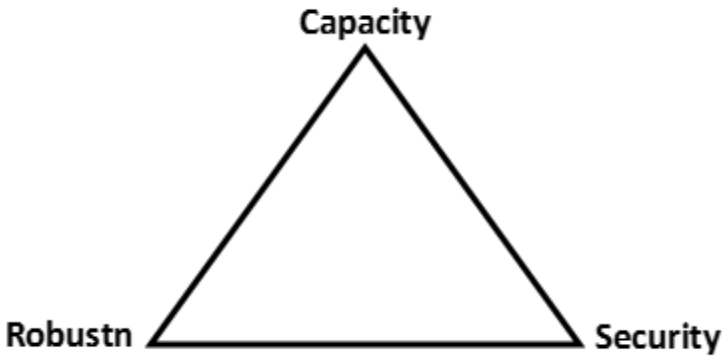


Figure (1): Information-hiding system features [4].

Although all digital file formats can be used for steganography, but the image and video files are more suitable because of their high degree of redundancy [4].

1.2. Related works

In 2008, Dr. AtefJawad AL-najjae presented " The Decoy: Multi-Level Digital Multimedia Steganography Model"[6] in this proposed model adds a level of security through the main theme of steganography: “hiding information in plain sight”. The cover object usually does not invite suspicion, since it looks similar to the original

object for the general observer. A hacker will use additional tools to look further, and will probably be satisfied with the decoy as the hidden object.

In 2010, A.K. Al-Frajat, H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan[5] presented "Hiding data in a video file: an overview". In this paper the video based steganography has been discussed and the advantages of using video file as a cover carrier for steganography have been proposed, steganography embedding types in video has been illustrated in this study. In addition the video architecture has been proposed, and how can make use of the internal structure of the video to hide secure data

In 2012, Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta Banik2 presented "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique"[7] In this paper a new method of audio steganographypresented where two secret messages can be hidden. Twotraditional method of steganography blended in a levelbased approach to reach the goal. The output stego objectis very difficult to decode which makes this methodsuccessful in the world of audio steganography.

In 2012, Marghny H. Mohamed1, Naziha M. Al-Aidroos2, and Mohamed A. Bamatraf presented " Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference " [8] In this paper, a new scheme using combination between LSB and PVD methods is proposed. This method increased the capacity of hidden data by embeddingmore data bits in the edge pixels, and to reduce the stego image degradation we embed a less data bits in the smooth pixels.

2. Multilevel Steganography

Multi-Level Steganography has advantage of difficult decoding and sending two secret message through a single cover object. Layering approach gives opportunity to do so. In this paper two layered approach has been presented. At the first level, cover file(C) can be embedded with the first secret message S1. Assuming the stego file as C1 which is cover file for next level where secret message can be denoted as S2. Now the final stego file created as C12. So C12 holds both S1 and S2.Two levels of steganography can be identified as layer 1 and layer 2.figure.2 shows the general block diagram for the multi-level steganography[7,6].

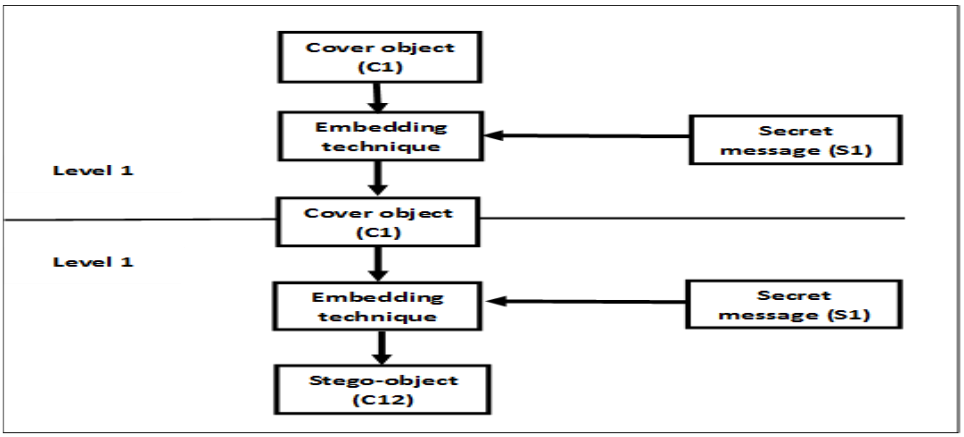


Figure (2): general block diagram for multi-level steganography [7].

3. Discrete Wavelet Transform

DWT is used for digital images. Many DWTs are available. Depending on the application appropriate one should be used. The simplest one is Haar transform. To hide text message integer wavelet transform can be used. When DWT is applied to an image it is decomposed into 4 sub bands: LL, HL, LH and HH. LL part contains the most significant features. So if the information is hidden in LL part the stego image can withstand compression or other manipulations. But sometimes distortion may be produced in the stego image and then other sub bands can be used[2].

4. Singular value decomposition (SVD)

With several applications in signal processing and statistics Singular Value Decomposition is a factorization of a complex matrix,. SVD is generalisation of the spectral theorem to arbitrary, not necessarily square, matrices. The SVD of an image A with size m×m is given by A = USVT, where U and V are orthogonal matrices. The matrix U contains a set of orthonormal output basis vector directions for the matrix A.

The elements of S are only nonzero on the diagonal and are called singular values of A The matrix V thus contains a set of orthonormal input vector directions for the matrix A. The matrix Σ contains the singular values, which can be thought of as scalar "gain controls" by which each corresponding input is multiplied to give a corresponding output. Singular Value Decomposition formula of an image can be written as:

$$A = USV^T = \sum_i^r = \sigma_i u_i s_i v_i^T \qquad (1)$$

The first r columns of U are the left singular vectors, whereas the r columns of V are the right singular vectors of image A. The rank of A is r, S=diag ($\sigma 1$, $\sigma 2 \ldots$, σn) satisfies $\sigma 1 \geq \sigma 2 \geq \cdots \geq \sigma n > 0$.

The singular values (diagonal matrix„s‟) represents the luminance or colour intensity of the image and the matrices „u‟ and „v‟ represents the geometry of the image when SVD is applied to the image. The slight variation in the singular values doesn‟t change the visual perception of the image, that means it have very good stability, now it has been scientifically proved.The SVD is applied to message image (or video) and each frame to each subband of the cover video to obtain the singular values of the message and cover files[12,13].

5. Cover File

The first step of the proposed systems is by reading the cover file. In order to verify the efficiency and feasibility a digital video file is used as a cover for data hidden. In the digital video steganography we have the flexibility of make a selective frame steganography to higher the security of the system or using the wall video for hiding a huge amount of data.

Everyone knows how much that cover affects the success of data hiding process, when the cover that has data hiding capacity and provide high degree of imperceptibility

and a complex nature may be classified as good cover type also, the applications of usage of that cover is included evaluating the goodness of that cover to the steganography.In this study MPEG file format is used as a cover media for hosting the secret data. The major advantage of MPEG compared to other video coding formats is that MPEG files are much smaller for the same quality. This is because MPEG uses very sophisticated compression techniques[7].

6. Message File

In this project unlimited message size can be used to hide in the cover.
The type of message used in this paper is image message, and it must be convert to gray scale image.Secret image is considered file of type JPEG which is stands for joint picture expert group with extension (.jpg)[11].
To hide this data in the cover, preprocessing operation (which is resizing) for the message files must be done to make the size of the message suitable to the size of the cover frames.

7. Proposed Method

In this paper, the proposed system is a multi-level steganography system.This system added additional degree of security and is implemented in the transform domain to hide six grey scale images (image or text) in a video cover file, using discrete wavelet transform (DWT) and SVD.

7.1 Hiding Module

At this module two levels of embedding process is proposed. The block diagram of this module shown in figure.3.
Level 1:
The first level of embedding involves merging of every two images of the six secret images as follows:
Step 1: Read the six secret images.
Step 2: Resize the six message image to 256x256 pixel.
Step 3: merge every two images in one matrix as the following algorithm:

```
function txt= txtxtract(R)
txt=zeros(size(im,1),size(im,2));
for i=1:size(R,1)
   for j=1:size(R,2)
      if (bitand(R(i,j),1)==1)
         txt(i,j)=255;
      else
         txt(i,j)=0;
       end
   end
end
```

After the first level of embedding, three matrices are obtained, the first matrix resulted from merging secret images 1 and 2, the second matrix resulted from merging secret image 3 and 4 and the third matrix resulted from merging secret images 5 and 6.

Level 2:

The second level of embedding involve hiding the resulted three matrices from the first level in a video cover object to obtain the stego-cover, The details of this steps are given below:

Step 1: take SVD for each output matrix, the equation of this process is described by equation (1) mentioned in section (4).

Step 2: Read the cover video.

Step 3: Resize video frames to 256x256 pixel.

Step 4: Extract each Frame from the cover video.

Step 5: For each single frame extract (R,G,B) frames.

Step 6: Take DWT to each (R,G,B) frames.

Step 7: decompose the cover frames into 4 sub bands: LL, HL, LH and HH.

Step 8: Apply SVD to each subband: $A^k = U^k{}_a \sum^k{}_a V^{kT}$,k=1,2,3,4, where k denotes LL,HL,LH,HH subbands, and λ_i^k ,i=1,……..n are the singular values of $\sum_a^k$

Step 9: Modify the singular values of the cover image in each sub band with the singular values of the visual singular value resulted in step 3 of the second level using the following equation:

$\lambda_i{}^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}$,i=*1,…,n, and k = 1,2,3,* α: is the alpha value (which is a variable that can be changed to obtain better constructed secret image)

λ_i: is the singular values of the cover frames.

λ_{wi}: is the singular values of the message image.

$\lambda_i{}^*$: is the modified singular values (the singular values of the stego-cover).

The singular values of the R frame of the video cover are modified with the singular values of the first matrix, the singular values of the G frame of the cover are modified with the singular values of the second matrix and the singular values of the B frame of the cover are modified with the singular values of the third matrix. A new stego (R,G,b) frames is resulted.

Step 10: Obtain the 4 sets of modified DWT coefficients by taking inverse SVD: $A^{*k} = U^k{}_a \sum^{*k}{}_a V^{kT}$, k=1,2,3,4.

Step 11: Apply the inverse DWT using the 4 sets of modified DWT coefficients to produce the new (R,G,B) frames.

Step 12: construct new I frame.

Step 13: construct a stenography video.

7.2 Extraction Module

Extraction module also implemented in two levels. The block diagram of extracted module is shown in the figure below:

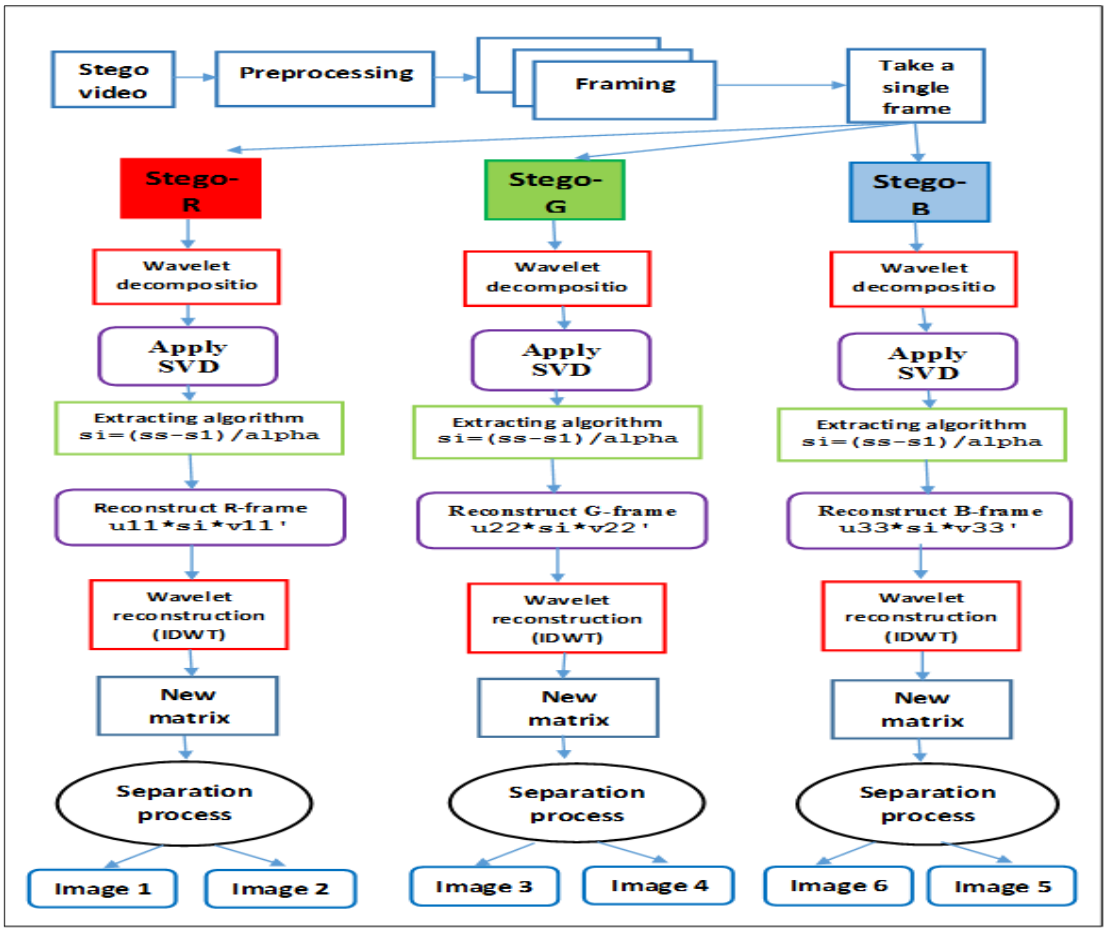


Figure (3) : extraction module of proposed system 2.

Level 1:

The first level involve extract the three matrices from the stego-cover video. Fig () show illustrated algorithm of the first level of extraction:

The details for extraction illustrated in the fallowing steps

Step1: Read the stenography video.

Step 2: Extract each frame from video.

Step 3: for each frame extract (R, G, B) frames.

Step 4: Take DWT to each frame (R,G, B).

Step 5: Apply SVD to LL subband, the equation of this process is described by equation (1) mentioned in section (4).

Step 6: extract the singular values using the following equation:

$\lambda_{wi}^{k} = (\lambda_i^{*k} - \lambda_i^{k}) / \alpha_k$ where i=1,…..,n, and k=1,2,3,4.

α: is the alpha value (which is a variable that can be changed to obtain better constructed secret image)

λ_i^{*}: is the singular values of the steg-cover frames.

λ_i: is the singular values of the original cover frames

λ_{wi}: is the singular values of the message image.

Step 7:obtain the 3 matrices from stego (R,G,B) frames by taking inverse SVD.

Level 2:

The second level of extraction involve the separation process of every two images from the three matrices resulted from the firs level, The details of this steps shown in Figure (3) are given below:

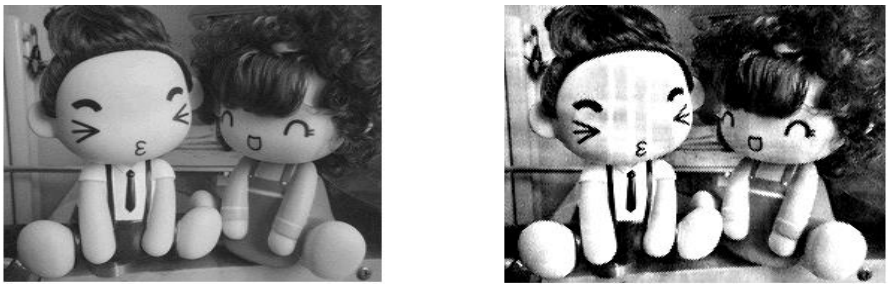
Step 8: now extract image1 (Even location of x+y) and image2 from (Odd location of x+y) from the first matrix, image3 (Even location of x+y) and image4 from (Odd location of x+y) and image5 (Even location of x+y) and image6 from (Odd location of x+y). where (x and y) are the rows and columns of the matrices. As the following:

```
function [tx1 tx2]= imxtract(diim)
tx1=zeros(size(diim,1),size(diim,2));
tx2=zeros(size(diim,1),size(diim,2));
for x=1:size(diim,1)
   for y=1:size(diim,2)
      % Extract the image for text image 1
      if(mod((x+y),2)==0)
         tx1(x,y,:)=diim(x,y,:);
      elseif(x~=size(diim,1) && y~=size(diim,1))
         tx1(x,y,:)=diim(x+1,y,:);
      end
      % Extract the image for text image 2
      if(x~=size(diim,1) && y~=size(diim,2) && (mod((x+y),2)==0))
         tx2(x,y,:)=diim(x+1,y,:);
      else
         tx2(x,y,:)=diim(x,y,:);
      end
    end
end
```

8. Experimental Results

The algorithm is tested in MATLAB. The results with video cover and six secret images are shown. In this paper we obtain the test results for hiding the six secret images file in a video cover.

The video cover size is 256x256 pixel and the secret image size is 256x256 pixel.Figures below shows the six original imagesbefore the embedding process and after the extraction process.

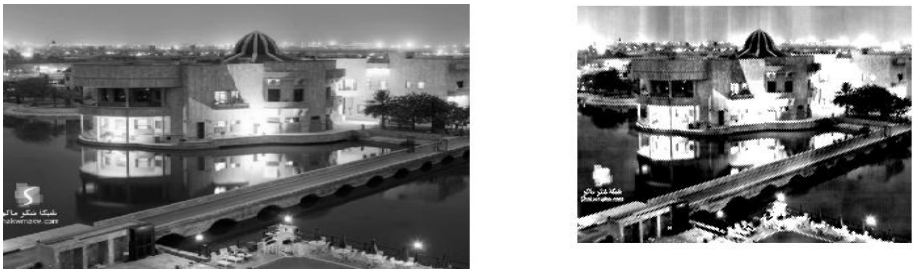


(a) (b)

Figure (5): image 1, a. before embedding b. after extracted

(a) (b)

Figure (6): image 2, a. before embedding, b. after extracted.



(a) (b)

Figure (7): image 3, a. before embedding, b. after extracted.

(a) (b)

Figure (8): image 4, a. before embedding, b. after extracted.

(a) (b)

Figure (9): image 5, a. before embedding, b. after extracted.

(a) (b)

Figure (10): image 6, a. before embedding, b. after extracted.

The table below shows the values of SNR, PSNR, MSE and Time for the six images using discrete wavelet transform.

Table .1 shows the results of the six images before embedding and after the extracting.

Video 1					
Image no.	method	SNR	PSNR	MSE	Time
Image 1	DWT	-0.2373	60.7337	0.0549	49.3275
Image 2	DWT	-1.2808	60.2454	0.0615	55.0996
Image 3	DWT	-0.5195	60.6331	0.0562	55.7236
Image 4	DWT	-1.3062	60.0146	0.0648	50.1947
Image 5	DWT	-0.8820	60.5852	0.0568	53.9528
Image 6	DWT	-0.0764	59.3024	0.0745	51.1059
Video 2					
Image 1	DWT	-0.5245	59.4583	0.0654	48.5752
Image 3	DWT	-0.5421	59.4578	0.0634	56.4785
Image 3	DWT	-0.6541	58.5421	0.0547	57.5488
Image 4	DWT	-0.9521	59.5421	0.0754	49.5468
Image 5	DWT	-0.5421	60.5421	0.0647	55.8457
Image 6	DWT	-0.0745	58.6541	0.0845	49.5487

9. Conclusions

The proposed model adds a level of security by using a new approach of steganography to obtain secure stego-cover. The cover object usually does not invite suspicion, since it looks similar to the original object for the general observer. In this paper, the system of hiding six grey scale images in a color video cover is implemented in tow levels of embedding process, the first level by the merging process of every tow images. At the first level three matrices are resulted. The second level of embedding involve hiding the resulted three matrices from the first level in a cover-video using discrete wavelet transform and singular value decomposition. Here also the embedding capacity is increased, because in this system six images instead of one embedded in only one cover.An exactly reverse procedure is followed at the receiver side to retrieve the embedded message by implementing two levels of extraction process.

9. References

1. A. F. K. AL-Hillaly, , December, (2004) , *" Data Hiding in Speech Data Using Wavelet Transform"* M. Sc Thesis, University of Baghdad, Baghdad, Iraq.
2. Hemalatha S, U. Acharya, Renuka A and P. R. Kamath, , March, 2013, *"A Secure Color Image Steganography in Transform Domain"*, International Journal on Cryptography and Information Security (IJCIS), Volume: 3, No.1, Manipal, Karnataka, India.
3. E. Ghasemi, J. Shanbehzadeh, N. Fassihi, ,(March, 2011), *"High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm"*, proceeding of the International Multiconference of Engineers and Computer Scientists 2011,Vo1ume: I, IMECS 2011, Hong Kong.
4. M. H. Mohamed, N. M. Al-Aidroos, and M. A. Bamatraf, (November, 2012), *"Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference"*, International Journal in Foundations of Computer Science & Technology (IJFCST), Volume: 2, No.6.
5. H. F. A. Al-Wahhab, (April, 2007), *"Text Steganography in Audio Media"*, M. Sc Thesis, Al-Nahrain University, Baghdad, Iraq.
6. A. J. AL-NAJJAR, , (July 23-25, 2008) , *" The Decoy: Multi-Level Digital Multimedia Steganography Model"*, 12th WSEAS International Conference on communications, Heraklion, Greece, Saudi Arabia.
7. Prof. S. K. Bandyopadhyay and B. G. Banik, (July – August, 2012), *" Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique"*, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume: 1, Issue 2, India.
8. M. H. Mohamed, N. M. Al-Aidroos, and M. A. Bamatraf,(November, 2012) *"Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference"*, International Journal in Foundations of Computer Science & Technology (IJFCST), Volume: 2, No.6,.

9. M. K. Kadhim,(2005), *"Implementation of Steganography Methods on MPEG files"*, M. Sc Thesis, University of Technology, Baghdad,Iraq,.
10. X. Xu, S. Dexter and A. M. Eskicioglu,(2003), *"A hybrid scheme for encryption and watermarking"*, The Graduate Center of the City University of New York, New York City,.
11. H. A. A. Darweesh, (2010) , *"Novel Technology for Image Steganography Based on Multi-level DWT and Block Permutation System"*, Baghdad, Iraq.
12. KapreBhagyashri S, Joshi M.Y.,(2010) , *"Robust Image Watermarking based on Singular Value Decomposition and Discrete Wavelet Transform"*, IEEE .
13. S. Marusic, D. B. H. Tay, G. Deng and M. Palaniswami,(2005), *"Even Length Biorthoganal wavelets for Digital Watermarking"*,IEEE.