www.s2is.org
International Journal on Smart Sensing and Intelligent Systems
ISSN 1178-5608

# DESIGN AND IMPLEMENTATION STEGANOGRAPHY SYSTEM BY USING VISIBLE IMAGE

[1,2]Hamdan Lateef Jaheel, [1]Zou Beiji and [3]Ahmed Lteef Jaheel

[1]School of Information Science and Engineering, Central South University, Hunan, P.R. China

[2]Computer Science Department, College of Computer Science and Mathematics, Thi-Qar University, Iraq

[3]College of Information Science and Engineering, Hunan University, Hunan, P.R. China

***Submitted: Feb. 2, 2015*** ***Accepted: Mar. 30, 2015*** ***Published: June 1, 2015***

***Abstract- Steganography refers to the technique of concealing secret information into another cover-media, such as audio, video, image and text in such a manner that the very existence of the information is camouflaged while secret is kept from the knowing of attacker. Watermarking is closely related to Stenography except that it hides information in cover object. Watermarking usually serves the purpose of copyright protection and ownership authentication, for example, watermarking can hide a stego-image inside a visible image and user can retrieve the stego-image and secret image in some way. In this paper, we will integrate two algorithms of information hiding, (steganography) F4 algorithm and (visible image) LSB algorithm to improve the level of protection. The secret image is concealed inside a common image through F4 algorithm and the resultant F4 steg-image is then hidden again as a visible image or watermark inside another image by LSB algorithm. To provide more than one level of protection for the hidden message, we will require additional security level to protect the secret image, which leads to increased complexity of retrieving the secrete image. The results prove the success of system after the secret image is retrieved successfully. The value of MSE, SNR and PSNR is calculated, which refers to an acceptable steganography system.***

**Index terms*:* Visible watermark, Least Significant Bit, Transform Domain Techniques, F4 Algorithm,**

## I. INTRODUCTION

The growing capabilities of modern communication technology call for special means of computer network security. With increasing data exchange rate through internet, network security is becoming more and more important. Therefore, the confidentiality and integrity of data is required to prevent unauthorized access and use. This trend brings the significant growth in the field of information hiding. In addition, the development of publishing and broadcasting technology also calls for other solutions of information hiding, such as audio, video, other sources and all rights reserved.

Availability of digital format may result in widely unauthorized copying because digital format provides the possibility to make many more high-quality copies. Steganography refers to a science of invisible communication. While reverse cryptography aims to secure communications from an eavesdropper, the steganography strives to conceal very presence of the message itself from an observer. General idea of concealing information in digital content has a wider class of applications that go beyond steganography. For example, printed image on a document could be described by metadata that could lead user to its high resolution version. Generally, the metadata provides extra information about an image. Although the metadata can also be stored in the file header of digital image, this model has many limitations. Commonly, when file is transformed to another format (e.g, from TIF file to JPEG file or to BMP file), metadata is lost. Similarly, cropping or any another from of the image manipulation could damage the metadata. The metadata can be attached to an image as long as it is in the digital form and is lost once the image is printed [1].

Information hiding enables metadata to travel with the image no matter in which format or image state (digital or analog). Digital watermarking is a special application of information hiding. Digital watermarking is the process of concealing information into a content digital multimedia in such a way that information (the watermarking) can be extracted later in order to prevent copying and control. Besides, digital watermarking may serve as the method to conceal information or characteristic data during digital transmission. It is widely applied to digital image, video, audio and documents. The digital watermarking is becoming increasingly popular, especially for adding undetectable identification marks, for example, the data of author or copyright [2]. Digital watermarking has become an active area and important research, and the development and investment in watermarking technique is deemed as the priority to help with the treatment of some challenges faced by rapid proliferation of digital contents. The key difference between information hiding and watermarking is the presence of an active enemy. In watermarking applications, such as copyright protection and authentication, there is an active enemy trying to remove, invalidate or forge the watermark. For information hiding, there is no such active enemy because the deletion of information hidden in the content will create no value. Nevertheless, information hiding methods are required to be robust against accidental distortion. Different from information hiding and digital watermarking, steganography aims to communicate securely without being detected. Although the steganography is an ancient art, used for the first time against the Persian by the romans, it has gone through much evolvement through the years [1]. The steganography ways finds its basic application in field of secret communication. It can be used by intelligence agencies throughout world to swap highly confidential data in secret media, e.g. a secret agent conceals the map of a terrorist camp in a photograph using image steganography and publishes it on a forum, and then an officer from head office can download the photograph from this forum and easily retrieve the concealed map [3].

In steganography, reverse other ways of communications, and one’s awareness of underlying communication between the sender and receiver defeats whole purposes. Therefore, first requirement of steganography way is its undetectability. In other words, the steganography way is considered to be insecure, if the warden Wendy is able to distinguish between cover-objects and stego-objects.

Cover-object: refer to the object used as carrier to conceal messages in many various objects. It can be used to conceal messages into many kinds of media, such as image, audio, video, file structure, HTML page and so on.

Stego-object: refer to the object which carries the hidden message. So, given cover-object and a message, the goal of the steganography is to produce a stego-object which can carry the message [4].

The embedding ways for which a number of algorithms have been proposed is transform domain embedding category. Most of the works in this category have been focused on the benefit from redundancies in DCT (discrete cosine transform) domain, which is used in JPEG compression. But there have been other algorithms which benefit from the other transform domains such as the frequency domain.

The embedding in DCT domain is simply done by changing the DCT Coefficients, for instance, by changing the least significant bit of each coefficient. One of the constraints in concealing in DCT domain is that many of the 64 coefficients are equal to zero, and altering them to non-zero value will have an impact on the compression rate. That is why the number of bits one could conceal in the DCT domain is less than the number of bits concealed by LSB method. As the concealing capacity is dependent to the image type used in DCT hiding, the number of non-zero DCT coefficients will be different, depending on texture of image [5].

Therefore, the special part of invisible information fixed on every image is not easily retrieved without the help of specialized technologies while maintaining the image quality [6]. All this is for music, movies, books, and interest in the software publishing industry. Information concealment gives rise to the area of research, including the application in digital media, watermarking and fingerprinting. Steganography is applied to copyright protection, for example, digital media, watermarking and fingerprints hide protected copyright information. Information concealment varies with application [7].

1. Digital watermarking technology is usually applied to copyright protection, for example, owner of the recognition and digital time stamps.
2. Fingerprints, owner of a set of data concealed in unique way, identify a series of user data. It can be added to the copyright information and other purposes. It can track data set and return to unauthorized use.
3. Steganography conceals the secret message within the host data set and makes it presence imperceptible [8].

Many people think informing hiding, steganography, and watermarking refer to the same technology of data hiding. It is right partially because these terminologies are closely associated with each other, and sometimes they can be replaced each other. Information hiding is a general term referring to the message embedding in some host media (Cox, Miller, Bloom, 2002). The purpose of information concealing is to keep information imperceptible or hide the presence of secret information. Steganography means "covered writing" a term derived from the Greek literature. It aims to conceal the very existence of a message. Digital watermarking however embeds information into the host object but the embedded information may be visible (e.g., a company logo), or invisible (in which case, it is similar to steganography). In steganographic communication, sender and receiver depends on agreement on steganographic system and the shared key which specifies how the secret message is encoded in the average cover. To send a secret message, for example, Alice creates a new image with a digital camera and then creates a steganographic model with her shared secret and message. Steganographic system uses the shared secret to specify how the concealed message should be encoded in the redundant bits. The output is a stego image that Alice sends to Bop. When Bop receives the image, he uses the shared key and agreed steganographic model to retrieve the secret message [9].

In this paper, we merge two algorithms for information hiding, namely F4 algorithm and LSB algorithm, to enhance the level of protection for the hidden images. A secret message (image) is concealed inside an image by F4 algorithm and the resultant F4 steg-image is hidden again as a visible image or watermark inside another image by LSB algorithm. This way provides more than one level of protection for the hidden message. In other words, basic on the principle of camouflage and deception, the secret image can be saved first within an image by F4 algorithm (resulting in stego-image), and then hidden again (stego image) in another image by LSB algorithm (that result visible image). The tricky nature of hiding an already hidden image using two different algorithms introduces some complexity and makes it more deceptive to a third party, hence reducing the risk of being detected and significantly enhancing the level of protection.

## II. VISIBLE WATERMARK

Visible watermark is used to determine the ownership of works, and to prevent viewers from unauthorized access beyond their limited coping rights [10]. The visible watermarking is simplest method to determine the origin of digital contents, since no special tool is required to extract the ownership information from content watermarked. Generally, visible watermarking can be divided into two types: irremovable and removable. The former mainly considers two factors: first, watermark must be adaptive to host image or video. In this case, watermark should be visible in watermarked digital content, but must not affect the visual quality of the original art. Second, embedded watermark must be strongly resistant against unintended editing and malicious attacks [11]. By contrast, the removable visible watermarking provides another efficient solution to copyright protection. Original digital content is marked by a removable pattern, like a copyright notification before distribution or release through internet for free exhibition.

Visible watermark is a secondary transparent cover on the primary image. The watermark seems visible to casual viewer when inspected strictly. Visible watermarks can be applied to the following cases:

Copyright protection enhancement: in this case, content owner worries about unauthorized use for commercial purposes (e.g. imprinting coffee mugs) without being paid. Therefore, the content owner wishes to add an ownership mark which is visible, but does not prevent the image being used for other purposes (e.g. academic research).

Notification of ownership origin: in this case, when images are made available via the internet, content owner wishes notify the ownership of the primary materials (library manuscript), so that an observer might be encouraged to patronize the institutions that own the materials [12].

Digital watermarking includes information embedding techniques that provide some information about the carrier. Since watermarks are introduced in more important areas of digital media, watermarking methods may be applied without worrying about the damage to image due to reduced compression. In some cases, digital watermarks may be advertised or are visible.

Visible watermarks are not the same as steganography in definition. The primary difference between steganography and watermarking is its intention. Traditional steganography conceals information while watermark extends information and can be considered special features of the cover image. Digital watermarking may include the type of information, like copyright, ownership, or license. In steganography, the object to be communicated is the hidden message while for digital watermarks, the object to be communicated is the cover and watermarks provide additional information about the cover [13].

## III. LEAST SIGNIFICANT BIT

The most common and simplest data hiding method is the last significant bit (LSB) substitution method. This method conceals the secret data by manipulating the LSB planes of the cover-image in the spatial domain. In the concealing process the value of K represents the number of rightmost bits of every unit pixel in the cover image which will be used to hide secret data and must be firstly determined.

Hidden data is then decomposed to a number of K-bit units. And finally according to a predetermined sequence, each K-bit data unit is concealed into the K-rightmost LSBs of the pixel in the cover-image. In the extraction process, every concealed K-bit data unit is retrieved from the K-rightmost LSBs of the pixels in the cover-image according to the same series used in the concealing process. The secret data is then rebuilt by lining up and merging each of the extracted K-bit data units. Least significant bit (LSB) insertion is a simple and common approach to conceal information in an image file. In this way the LSB of a byte is substitution with an M"s bit. To the human eye the secret image will appear identical to the carrier image. For hiding information inside the image the LSB (least significant bit) way is usually used. For a computer, an image file is as amply a file that shows different colors and intensities of light in different areas of an image [14].

The basic idea here is to insert the secret image in the Least Significant Bits of the images. LSB substitution algorithm is to take the first N cover pixels where N is a total length of the secret message to be hidden in bits. After that, the last bit of all pixels will be replaced by one of the message (image) bits [15,16]. For example, assuming that we have two adjacent pixels (six bytes) with the following RBG encoding:

10010101 01001100 11001101
00010010 00010100 01001011

Now, assuming that we want to conceal the following 6 bits of data 001001:

If the LSB of 6 bytes above is covered by these 6 bits, we will get the following, where bits in bold have been changed.

10110100 01001100 11001101
00010010 00010100 01001011

Now, the 6 bits have been hidden but only at the cost of changing the 4 of their LSB.

## IV. TRANSFORM DOMAIN TECHNIQUES

When JPEG images are compressed to a size smaller than the file to be firstly transferred into the discrete cosine transform (DCT) domain which provides data as high and low frequencies. High frequencies relate to areas of high detail and low frequencies to low detailed areas. Basically, the JPEG compression process is that we can remove some of the high details because our eyes are less sensitive in this area, which means that we will not notice if they are removed. This idea is based on the fact that our eyes are the most sensitive in the plainer areas of an image. To illustrate this, we will take an image of dense forest as an example. When a few random pixels are changed to the black, there are possibilities you will not be able to notice the changes because your eyes will be so distracted by all the other details. However, if the picture is a plain wall you are able to see those black pixels more clearly because the distraction is less (of course unless the wall is painted black). The DCT values (referred to as coefficients) are tweaked in compression and we can similarly tweak some of the values in such a way that they hold message data. This manner makes the concealing much harder to be detected from the steganalytical viewpoint than concealing in the spatial domain because steganalyst would have to do a bit more effects to find any artifacts of embedding.

Before embedding, all 8 x 8 blocks of JPEG image are converted to frequency domain by DCT which is then used to transform each block into DCT coefficients. In a request for the values of whole numbers, each 8x8 block is quantized according to a Quantization Table. Two types of coefficients could be seen in every 8*8 block: DC and AC. It is known that value at the top left of each 8*8 block refers to DC coefficient. The block contains the mean value of all the other coefficients referred as the AC coefficients. DC coefficients provide a good estimation on the level of details in the block because it is very important to each block. Therefore, we cannot manipulate or change the value of DC coefficients because it will lead to the change of many AC coefficients and visual discrepancy when the image is converted back to the spatial domain and viewed normally. For this reason, the JSteg algorithm cannot embed message data over any of the DC coefficients for every block. And also, the algorithm doesn't permit embedding on any AC coefficient equal to 0 or 1 [17].

There are several transforms that could potentially be used to embed the hidden data including the discrete wavelet transform (DWT), fast Fourier transform (FFT), JSteg algorithm outguess0.1, F3 algorithm, F4 algorithm, F5 algorithm and many other ways. However to keep things at a comprehendible level we will only discuss F4 algorithm [18].

## V. F4 ALGORITHM

Tow the weaknesses of algorithm F3 are canceled in one fell swoop by F4 algorithm by mapping negative coefficients to the steganographic value where even-negative coefficients = steganographic 1 odd-negative coefficients = 0 even-positive coefficients =0 (as with JSteg and F3) and odd-positive coefficients =1 [17]. More simply put this means if embed a 0 in a DCT coefficient equal to -3, the result will remain -3 , whereas it would have been modified to -2 using F3. This means that the bit-flips now occur with the roughly same probability.

The following action when you conceal the secret message data according to the algorithm F4 during the quantized DCT coefficients. F4 does not embed on the DC coefficients or any AC coefficient equal to zero. Again the DC coefficient is the same for both image (a) and image (b). This means that the algorithm correctly stay away concealing on these values. In addition, the second AC coefficient in the image (a) equal to 7 is correctly decreasing to 6 when embedding a 0. Similarly the third AC coefficient equal -5 coefficients to -4 when an equal 1 is embedded. This is at the bit-flips denoted in figure 1 [18, 19].

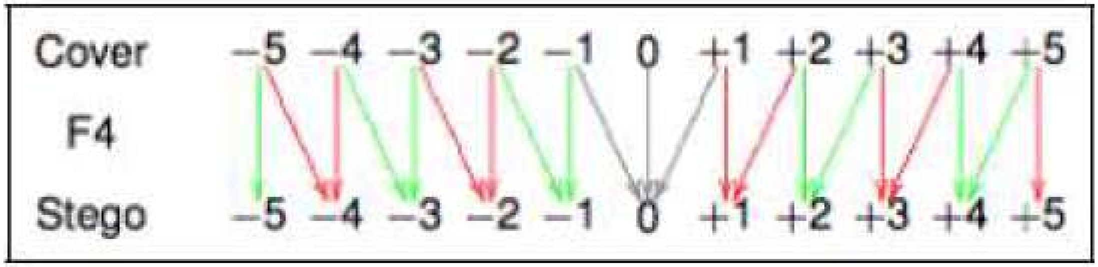

Figure 1: The expected bit flips from the F4 algorithm [19]

## VI. PROPOSED METHOD

In this paper we merge two algorithms for information hiding namely F4 algorithm and LSB algorithm to enhance the level of protection for the hidden images. The secret message (image) is concealed inside an image by using F4 algorithm and the resulta F4 steg-image is further hidden as (visible image or watermark) inside another image by LSB algorithm. This is to provide more than level of protection for the hidden message. In other words, based on the principle of camouflage and deception where the secret image will be saved first within an image by F4 algorithm (result stego-image) and then saved (stego-image) within another image by LSB algorithm (that result visible image). The tricky nature of hiding an already hidden image using two different algorithms introduces some complexity and makes it more deceptive to a third party and hence reduces the risk of being detected. This way can significantly enhance the level of protection.

### *A. Embedding algorithm*

Input: cover image1, cover image2, secret image1 (message1), secret image2(message2)

Step1: read cover image1. JPEG

A. JPEG partitions a cover image1 into non overlapping blocks of 8*8 pixels

B. Calculate DCT coefficient for each block

C. Quantize the coefficients

Step2: hiding process by using F4 algorithm

```
for i = 1, ..., l(m) do
    p← di
   while p = DC or p = 0 do
       p = next DCT coefficient from d
   end while
P←  absolute(pi)
    if P = mi and P > 0 then
      P← P + 1
        absolute(di)   P
     else if P 6= mi and P < 0 then
      P← P + 1
      absolute(di)   P

  end if
  if di = 0 then
      next mi = mi
  end if
 Ci ←  pi
end for
```

Step3: calculate message capacity

Step4: Writ JPEG image by de-quantize and take inverse DCT to obtain stego image1.

Secret image2 (message) = stego image

Step5: Read cover image2.JPEG

Step6: Read secret message ( stego image)

Step7: Cover image2 is converted into the matrix form. Then each byte of the image is taken and replaced with the last bit of LSB to the secret information that is (secret image) of the each bit.

Step8: The secret image also access each pixel to convert into the matrix form, then they convert into arrays of bits in binary's of 0s and 1s, and replaces with the least significant of the bit.

Step9: Add each pixel of the (secret image) into LSB of the pixel of (original image).

Step10: Result visible image.

After the implementation of this algorithm in Matlab 7.6 program gets the results shown in Figure (2) that illustrates new method.

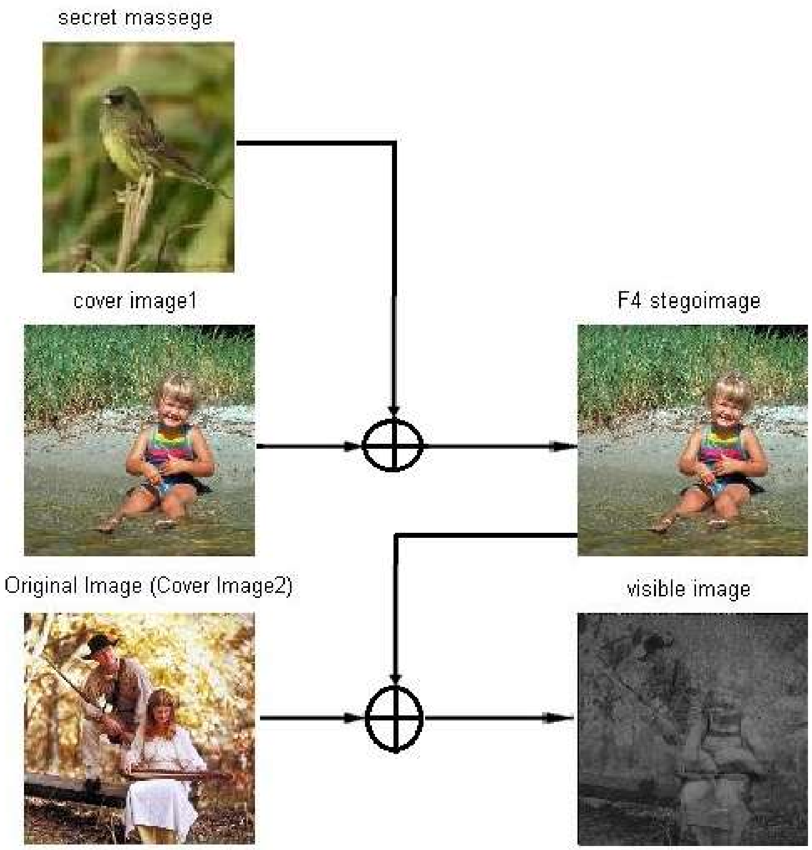

Figure (2): Embedding algorithm

### *B.Retrieval algorithm:*

Step1: read visible image.

Step2: process of finding and extracting the similar bits for both the images, like original image and the secret image. In this process, after the least significant bit is extracted from both images, the output is in the form of bytes, and then they are grouped to obtain images information.

Step3: produce two image (recovered cover image, recovered secret image).

Step4: read recovered secret image.

A. JPEG partitions Stego image2 into non overlapping blocks of 8*8 pixels

B. Calculate DCT coefficient for each block

C. Quantize the coefficients

D. Calculate message capacity

Step5: Extract process by F4 algorithm

```
for i = 1, ..., l(m) do
  p ← di
while p = DC or p = 0 do
   p = next DCT coefficient from d
end while
 P ← absolute(pi)
if P = mi and P > 0 then
mi ← absolute(pi) - 1
else if P 6= mi and P < 0 then
mi ← absolute(pi) + 1
end if
```

Step 6: Writ JPEG image by de-quantize and take inverse DCT to obtain secret image2

final image = Secret image2

After the implementation of this algorithm in Matlab7.6 program got the results shown in figure(3).

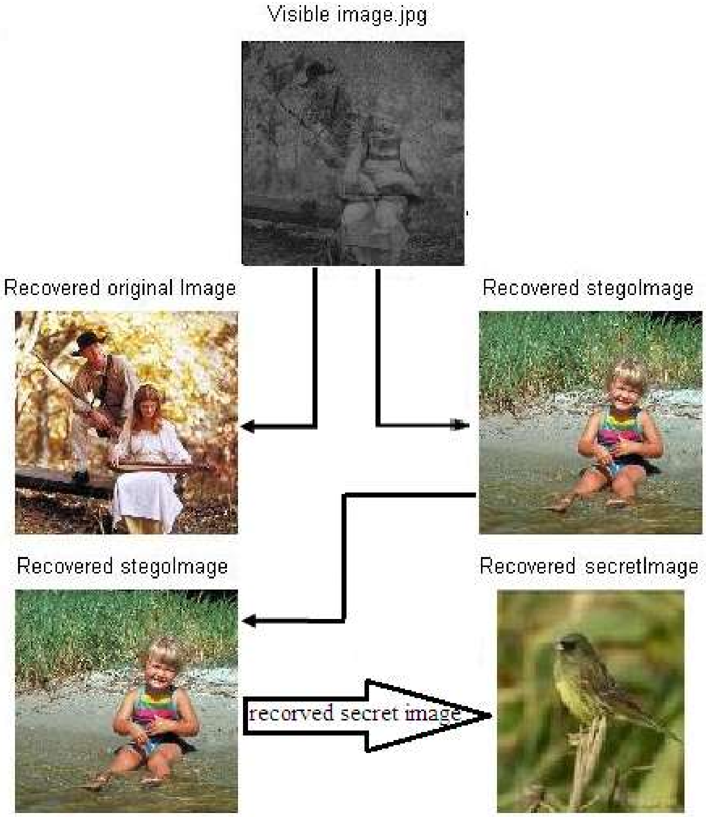

Figure (3): Retrieval algorithm

## VII. IMAGE DATABASE

Some image databases already exist for image processing research. The USC-IPI image database is an example 50 where one can find the classics "Lena, Baboon, Peppers and etc". Put these databases to research on information hiding systems. Some of these images in the database were scanned from copyrighted materials more than 50 images and the origin of many is unknown. Also, some images are from image database of Washington University [20] and Oklahoma state university [21] and also some from special camera. It is impossible to get an exhaustive list of classes of pictures and stock photo companies have a lot of difficulties to set up a satisfactory index. However one can at least retain the main themes that are common among these libraries and that are used very often in the press in order to keep a wide range of kind of pictures color, textures, patterns, shapes and lightning.

## VIII. EXPERIMENTAL AND RESULTS

The performance evaluation of the proposed algorithm is done by MSE (mean squared error), SNR (signal to noise ratio) and PSNR (peak signal noise ratio). The parameters are calculated by equations (1,2 and 3) [22,23]. Experiments implemented will show the results that the secret message (image) is concealed inside an image by F4 algorithm and the resultant F4 steg-image is further hidden as (visible image or watermark) inside another image by LSB algorithm which was implemented. Therefore, we will have additional security level to protect the secret image, which leads to an increase in the complexity of retrieving the secret image.

It is clear from the experience that the technique proposed is not retrieving secret image (secret message) when using Jsteg algorithm or Outquess0.1 algorithm [16], instead of F4 algorithm that have proven successful results and retrieval secret image completely without distortion. The MSE, SNR and PSNR values were calculated after retrieving F4 stego-image. All these results of the PSNR were calculated after sending the final result from visible-image via e-mail to another computer which retrieves the hidden message (image) and then calculates the MSE, SNR and PSNR. These values refer to an acceptable steganography system. Figure (4) illustrates histogram to original image and (retrieved F4 stego-image) after retrieving F4 steg-image from visible image. Table (1) explains MSE values, SNR values and PSNR values for these experimental. Figure (5) explains MSE values, SNR values and PSNR values for these experimental.

$$\mathrm{MSE}\ \ (x-x\square)/\mathrm{MSN} \qquad (1)$$

$$\mathrm{SNR}\ =20*\log10\ ((\max(x))\text{^}2/(\mathrm{sum}(\mathrm{MSE}))) \qquad (2)$$

$$\mathrm{PSNR}=20*\log10((\max(x))\text{^}2/\mathrm{MSE} \qquad (3)$$

**Embedding Capacity:**

It is the maximum capacity of the secret data that can be embedded in the cover image without deteriorating the integrity of the cover image. It can be represented in bytes or bit per pixel (bpp). The calculation is explained in equation (4).

**Capacity = (X*Y)/64 *b*(n-15) (4)**

In this equation, X and Y is the dimension of the cover image. By dividing the product of X,Y by 64, the number of 8*8 blocks is achieved . During data embedding process, no data is embedded in the last 15 coefficients, so that term (n-15) is used here and in each coefficient b bit of data will be embedded [24].

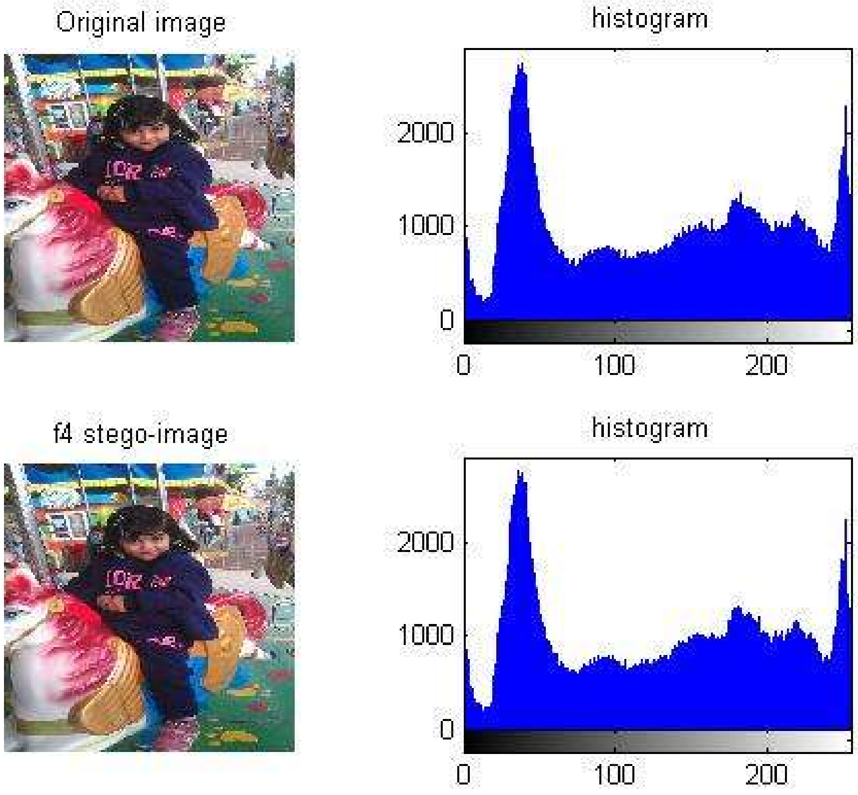

Figure (4): Illustrate histogram to (A) original image and (B) retrieved F4 stego-image.

TABLE I. explains MSE values, SNR values and PSNR values

| | MSE | SNR | PSNR |
|---|---|---|---|
| Couple | 2.1021 | 40.8738 | 44.9042 |
| Ayah | 2.3603 | 38.9081 | 44.4012 |
| Foxy | 3.9109 | 36.5819 | 42.2081 |
| Lena | 1.2831 | 41.3924 | 47.0484 |
| Mushroom | 1.4844 | 38.2989 | 46.4153 |
| Elk | 1.7754 | 38.5925 | 45.6379 |
| Garden | 5.8162 | 35.7783 | 40.4844 |
| Palace | 1.3777 | 41.0603 | 46.7391 |

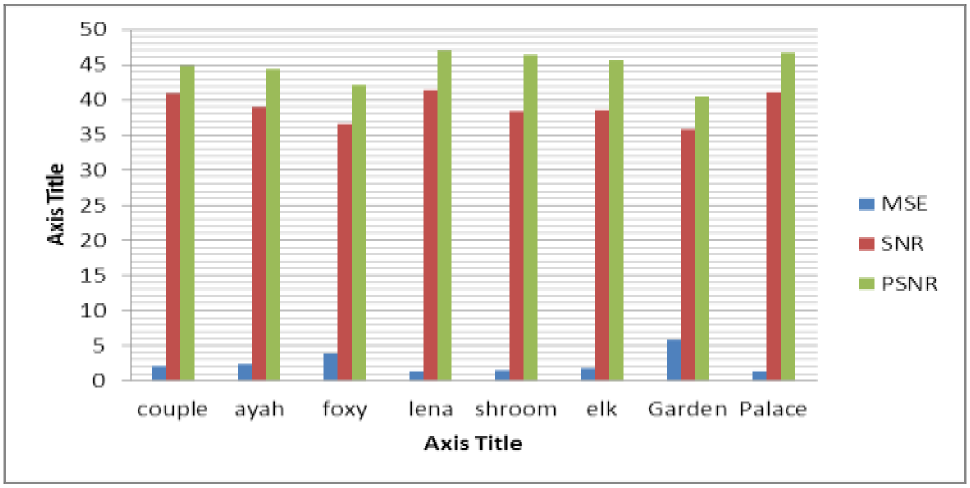

Figure (5): explains MSE values, SNR values and PSNR values

The following table (2) and table (3) explains the DC coefficient is the same for both image(a) in table (2) and image(b) in table (3) meaning that the algorithm can correctly avoid embedding on these values. In addition, we can see that second AC coefficient in image (a) equal to (8) is correctly decremented to 7 when embedding a 0. We can see that the third AC coefficient (-5) increases to -4 when a 1 is embedded. This is what we expect from the bit-flips denoted in figure(1).

Table(2): Explain pixel values before embedding using F4 algorithm

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 143 | 5 | 3 | 0 | 0 | 0 | -1 | 1 |
| 2 | 8 | -1 | 1 | -3 | 1 | 1 | -1 | 1 |
| 3 | -5 | 0 | -1 | 1 | 0 | 0 | 0 | 0 |
| 4 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 5 | -1 | -1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Table(2): Explain pixel values after embedding using F4 algorithm

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 143 | 5 | 3 | 0 | 0 | 0 | -1 | 1 |
| 2 | 7 | -1 | 1 | -3 | 1 | 1 | -1 | 1 |
| 3 | -4 | 0 | -1 | 1 | 0 | 0 | 0 | 0 |
| 4 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 5 | -1 | -1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## IX. CONCLUSIONS

From the above analysis and discussion, we can conclude that the main goal of steganography techniques is to hide the secret image (message) and then retrieve it in a safe manner in such a way that image retrieval will not destroy the hidden message. Alternately, watermark algorithm aims to maintain the author and copyright. For example, a stego-image can be hidden inside a visible image watermarking, and then we can retrieve the stego-image and then the secret image. These technologies provide adaptive measures of embedding the cover message into the original image which can be easily achieved.

When dealing with the image, it is more useful to approach the matter from the visible position. In this paper, we combine two algorithms for information hiding namely F4 steganography algorithm and visible image by LSB algorithm to enhance the level of protection for the hidden image. The secret message (image) is concealed inside an image by F4 algorithm and the resultant F4 steg-image is further hidden as (visible image or visible watermark) inside another image by LSB algorithm. This manner can provide more than one level of protection for the hidden message. In other words, basic on the principle of camouflage and deception, the secret image is saved within an image for the first time with F4 algorithm (producing stego-image), and then stego image is saved for the second time in another image by LSB algorithm (producing visible image).

Overall, I believe that the output from this system has succeeded in achieving the original target. It seems to be the easiest steo-system to be implemented. However, it is a more complicated steego-system much harder to attack. This of course makes perfect sense as the more complex systems are likely to work like that they embed the message data in more intricate fashions with the simpler systems.

## X. REFERENCES

[1] Rajarathnam Chandramouli, Mehdi Kharrazi, Nasir Memon” Image Steganography and Steganalysis: Concepts and Practice” Second International Workshop, Seoul, Korea, Revised Papers, Volume 2939, pp 35-49, 2004.

[2] Jitendra Jain, Punit Johari” Digital Image Watermarking Based on LSB for Gray Scale Image” IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6,pp. 108-112, June 2014.

[3] Firas A. Jassim” Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method” International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, pp. 39-44, June 2013.

[4] Mehdi Hussain and Mureed Hussain” A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, pp 113-124, May 2013.

[5] F. Alturki and R. Mersereau,”Secure blind image steganographic technique using discrete fourier transformation ," IEEE International Conference on Image Processing, Thessaloniki, Greece., vol.2, 542 – 545, 2001.

[6] N. Provos, “Probabilistic Methods for Improving Information Hiding”, CITI Technical Report 01-1, pp. 1-8, January, 2001.

[7] R A Isbell, “Steganography: Hidden Menace or Hidden Saviour”, Steganography White Paper, 10 May 2002.

[8] Alisha Arora, Mrs. Nirvair Neeru, Mrs. Taqdir"IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW" International Journal For Technological Research In Engineering Volume 1, Issue 9,pp.924-929, May-2014.

[9] Kuanchin Chen “Digital Watermarking and Steganography” Western Michigan University, USA 2009, IGI Global.

[10] Provos, N. & Honeyman, P. “Hide and Seek: An introduction to steganography”, IEEE Security and Privacy Journal, vol 1, Issue 3 , pp 32 – 44, 2003.

[11] Fridrich. J., Lukas J. and Goljan M., “Digital Camera Identification from Sensor Noise”,IEEE Transactions on Information Security and Forensics, vol 1(2), pp 205-214, 2006.

[12] N. Provos, “Defending Against Statistical Steganalysis,” In Proceedings of USENIX Security Symposium, pp. 323–335, 2001.

[13] Ajinkya Kawale, Shubham Gaidhani"Digital Image Watermarking"International Journal of Scientific & Engineering Research, Volume 4, Issue 5, pp. 1899-1901, 2013.

[14] Yusuf Perwej, Firoj Parwej , Asif Perwej"An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, pp. 21-38, 2012.

[15] Wang R.Z. , Lin C.F. , Lin J.C. “Image hiding by optimal LSB substitution and genetic algorithm”, Pattern Recognition, vol 34 , no 3 , pp 671 – 683, 2001.

[16] Puneet Kr Sharma and Rajni” ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM” International Journal of Information Sciences and Techniques (IJIST) Vol. 2, No.4, pp. 95-101, July 2012.

[17] Philip Bateman and Dr. Hans “Image Steganography and Steganalysis”, M.S., Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey Guildford Surrey, United Kingdom, Submitted for the Degree of Master of Science in Security Technologies & Applications 2008.

[18] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recognition, vol. 34, no. 3, pp.671-683, Mar. 2001.

[19] A. Westfeld. "F5 - A Steganographic Algorithm: High Capacity Despite Better Steganalysis", Lecture Notes in Computer Science, vol. 2137, pp. 289-302, 2001.

[20] S.C.Mukhopadhyay, F.P.Dawson, M.Iwahara and S.Yamada, “A Novel Compact Magnetic Current Limiter for Three Phase Applications”, IEEE Transactions on Magnetics, Vol. 36, No. 5, pp. 3568-3570, September 2000.

[21] S. Yamada, K. Chomsuwan, S.C.Mukhopadhyay, M.Iwahara, M. Kakikawa and I. Nagano, “Detection of Magnetic Fluid Volume Density with a GMR Sensor”, Journal of Magnetics Society of Japan, Vol. 31, No. 2, pp. 44-47, 2007.

[22] Anju Thomas, D. Sugumar, P.T Vanathi” Blind Image Source Separation based on MMCA using Dictionary Technique” International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 2, Issue 2,pp.182-186, 2013.

[23] Amrita Khamrui, J K Mandal” A Genetic Algorithm based Steganography using Discrete

[24] Cosine Transformation (GASDCT)" International Conference on Computational Intelligence:Modeling Techniques and Applications(CIMTA),Volume 10, Pages 105–111 2013.

[25] Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani, "Steganography: Dct Coefficient Replacement Method and Compare With Jsteg Algorithm" International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, pp.458-462, 2012.

[26] Hamdan L. Jaheel and Zou Beiji,A novel approach of combining steganography algorithms,International Journal on Smart Sensing and Intelligent Systems, vol.8, no.1, pp.90-106, 2015.

[27] Wang Tao, Design of digital image encryption algorithm based on mixed chaotic sequences, International Journal on Smart Sensing and Intelligent Systems, vol.7, no.4, pp. 1453 – 1469, 2014.