Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator

Walaa Abu-Marie*, Adnan Gutub, Hussein Abu-Mansour***

** Department of Information technology and Computing Arab Open University Riyadh, KSA*
P. O. Box 84901, Riyadh 11681
Tel: + 966 1 2742277 + 966 1 2742277
Fax: + 966 1 2742696
e-mail: walaa@arabou.edu.sa, hmansour@arabou.edu.sa

*** Center of Excellence in Hajj and Omrah Research, Umm Al-Qura University, Makkah, Saudi Arabia.*
P.O. Box 6287, Makkah 21955, Saudi Arabia
e-mail: aagutub@uqu.edu.sa

Submitted: 31/03/2010
Accepted: 22/05/2010
Appeared: 25/05/2010

Abstract—Using the least significant bits in an image, in this paper we propose two new techniques that use truth table based and determinate array on RGB indicator that utilizes the idea of pixel manipulation and stegokey and deploy them together using the least two significant bits of one of existing channels in the purpose to indicate to data existence in other channels using a (bmp) image format . This technique has come with amazing results especially in data-bit capacity that is hidden and related to the RGB image pixels.

Keywords: Steganography, RGB Bitmap, Pixel Indicator Algorithm, Information hiding, LSB, Cover Image, Stegokey.

1. INTRODUCTION

Steganography is the art of hiding information by embedding messages within each other. It's main purpose is to convey messages secretly by concealing messages behind digital media files. Greek steganography hides data in an electronic word-document file that, by it's turn , might be hidden in an image. This is done by replacing the least word stegano, meaning covered or secret, and graph (writing or drawing).

Basically steganography is a hidden text, such as the text written by invisible ink on a paper or a copyright information hidden in an audio file. But the modified , steganography these days is more often represented with the latest modern digital formats used to hide the high priority information or data with highest redundant bits in the original file from the human's perceivable eye or ear.

Image and audio files match with these requirements, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography which are: Video, Text, Audio and Images.

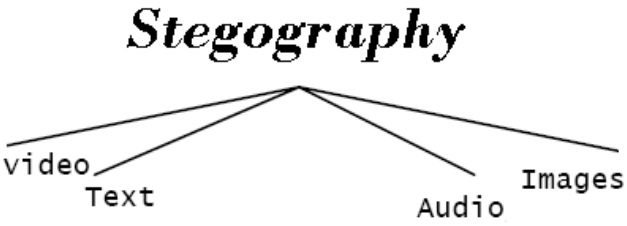


Fig. 1. Main categories of file formats that can be used for steganography.

The steganography techniques require two files: cover media help to hide the data, and the data itself. When we combine the shell image and the hidden message behind we generate a stegofile, which is called a stego-image image. One of the commonly used techniques is the lsb where the least significant bit of each pixel is replaced by bits of the secret till secret message finishes. The risk of information being uncovered with this method is susceptible to all 'sequential scanning' based on techniques, which is threatening its security.

Stego has a number of nefarious applications; however, most notably hiding records of illegal activity, financial fraud, industrial espionage, and communication amongst members of criminal or terrorist organizations. The flow of the paper is as follows. Section 2 lists the history for designing stego-algorithms. Section 3 presents the definition for steganalysis. Section 4 format explain the basics of bmp image. Section 5 discusses our new proposed stego-technique. Modelling the algorithm and testing its results are provided section 6 presents comparisons and conclusion remarks of the work.

2. RELATED WORK

Throughout history, people have hidden information by a multitude of methods and variations. For example, ancient Greeks wrote text on wax-covered tablets. Besides this, it is used to pass a hidden message; a person would scrape wax off a tablet, write a message on the underlying wood and again cover the tablet with wax to make it appear blank and unused. The idea and practice of hiding information has a long history as The Greek historian **Herodotus** writes of a nobleman, **Histaeus** who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message (Morkel et al, 2005*)*

Aeneas the tactician not only proposed many steganographic techniques that could be considered "state of the art" of his time, such as hiding messages in women's earrings or messages carried by pigeons but he also described several methods for hiding in text-by modifying the height of letter strokes or marking letters in a text using small holes. Linguistic steganography, also called acrostic, was one of the most popular ancient steganographic methods. Without forgetting secret messages that were encoded as initial letters of sentences or successive tersest in a poem (Ingmar et al, 1999).

3. THE ALGORITHM

One of the most famous examples is (Amorosa vision) by Giovanni Boccacio. A more advanced version of linguistic steganography originally conceived in China and reinvented by Cardan (1501-1576) is the famous Cardan's Grille. The letters of the secret message do not form a regular structure but a random pattern. Moreover the message is read simply by placing a mask over the text. This mask is an early example of a secret (stego) key that had to be shared between communicating parties. In addition, Acrostic was also used in World War I by both the Germans and Allies (González et al, 2008).

A precursor of modern steganographic methods were described by François Bacon. The latter used italic or normal fonts to encode binary representations of letters in his works. Furthermore, five letters of the cover Work could hold five bits and thus one letter of the alphabet. What made this method relatively inconspicuous was the variability of sixteenth-century typography. During World War II, people also used milk, vinegar, fruit juices and urine to write secret messages. When heated, these fluids become darker and the message could be read.

The following, the Germans hided data as microdots. This involved photographing the message to be hidden and reduce the size so that it could be used as a period within another document. Mr. J. Edgar Hoover, FBI director, described once the use of microdots as "the enemy's masterpiece of espionage". One of the valuable incident to mention here is about In the Pueblo Incident. US crew of the USS Pueblo re-search ship when they were captured by North Korea. In an attempt by North Korea to show that the US crews have in fact defected, the North Korea captured photographs of of American prisoners after compelling them to smile so show a nice photo while feeling comfortable. The US Crew used the nger gesture to discredit the pictures and send home a clear indication that they were in distress.

Recent applications of steganography include using special inks to write the messages to be hidden in note section and also the entertainment industry using digital watermarking and fingerprinting of audio and video for copyright reservation . More to tell that United States government stated that Osama Bin Laden and the al-Qaeda organization use steganography to send messages through websites and newsgroups. During the 16-17th century, people had arisen a large literature on steganography and many of the methods depended on novel means of encoding information.

4. STEGANALYSIS

The art and the science of detecting hidden messages using steganography; is analogous to cryptanalysis applied to cryptography. Steganalysis itself is the practice of attacking steganographic methods by detection, destruction, extraction, or modification of embedded data. Understanding the means by which attackers can defeat steganographic systems is necessary for the design and development of superior, more robust systems. The meaning of a successful attack is dependent on the application; for a secret communication application the mere detection and proof that some kind of data is hidden within the stego-image is a successful attack.

While it is possible to hide messages within a variety of data file types, image data is likely to be the medium of choice for cyber criminals for several reasons. First, because of the high level of redundancy in image data, is possible to embed a great deal of hidden information. Second, (*Bergman and Davidson, 2006*) innocuous-looking images are commonplace on every computer and arouse little suspicion.

For a steganalysis pirate attempting to defeat a copyright mark, a successful attack requires that he not only detects the mark but also destroys or modifies the mark without significant degradation of the perceptual quality of the stego-image.

- The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload.

- Unlike cryptanalysis, where it is obvious that intercepted data contains a message, steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload.
- It is complicated primarily by four things:
- The suspect files may or may not have any encoded data.
- The payloads may have been encrypted before being encoded.
- Noise or irrelevant data encoded will reduce stealth but can make analysis very time-consuming.
- Unless you can completely recover, decrypt, and inspect the payload, you often can't be sure whether you really have a file used for transport or not-- all you have is a probability.

Figuring out a hidden message is the first step in steganalysis and is considered an "attack" on the hidden information. Attacks may come in several different forms depending on what information is available to the steganalyst.

There are two other types of attacks against steganography. The first is the known message attack. In this case the steganalyst (one who does steganalysis) has a known hidden message and the corresponding stego-image. In this case the objective is to determine patterns that result from hiding the message. These patterns can then be used to analyze other stegoobjects in the future. The second attack is the chosen-message attack. In this case the steganalyst will create a message and use a known stego-tool to create a stego-image. This known stego image is then analyzed to (J.Silman etc.al,2001)determine patterns for later use against other stegoimages .

5. BITMAP LOSS COMPRESS

The first image format we are going to cover is one of the simplest Windows BMP is the native image format in the Microsoft Windows operating system. It supports image with 1,4,8,16,24 and 32 bit per pixel, although BMP files using 16 and 32 bit per pixel are rare. BMP also supports simple run – length compression for 4 and 8 bit per pixel.

Multi – byte integer in the windows BMP format are stored the least significant bytes first. Data stored in the BMP format consists entirely of complete bytes so bit string ordering is not an issue.

The **BMP** image standard is used by Windows and elsewhere to represent graphics images in any of several different display and compression options.((Rafael.C.. et.al,2008) The BMP advantages are that each pixel is usually independently available for any alteration or modification. Ad that repeated use does not normally degrade the image because lossy compression is not used.

The main shortening is the size of the files being used , is usually horrendous compared to JPEG, fractal, GIF, or other lossy compression schemes. The BMP file structure is very simple: the header data which include read the file header, read bmp information header, color palette and bmp data.

5.1 File header

This block of bytes is at the start of the file and is used to identify the file. A typical application reads this block first to ensure that the file is actually a BMP file and that it is not damaged. And contains information about the type, size, and layout of a device-independent bitmap file. The header is defined as a BITMAPFILEHEADER structure.

Note that the first two bytes of the BMP file format (thus the BMP header) are stored in big-endian order. This is the magic number 'BM'. (All of the other integer values are stored in little-endian format (i.e. least-significant byte first). (*http://www.whisqu.se/per/docs/graphics52.htm*)

5.2 Information header

The bitmap-information header is block of bytes tells the application detailed information about the image, defined as a BITMAPINFOHEADER structure, specifies the dimensions, compression type, and color format for the bitmap, which will be used to display the image on the screen. Matches the header used internally by Windows and has several different variants. All of them contain a dword (a **dword** (double word) is a unit of data that is twice the size of a word) field, (*http://en.wikipedia.org/wiki/BMP_file_format*) specifying their size, so that an application can easily determine which header is used in the image.

Table 1. File Header

BMP File Header	Stores general information about the BMP file.
Bitmap Information (DIB header)	Stores detailed information about the bitmap image.
Color Palette	Stores the definition of the colors being used for indexed color bitmaps.
Bitmap Data	Stores the actual image, pixel by pixel.

5.3 Color table

The color table, defined as an array of RGBQUAD structures, contains as many elements as there are colors in the bitmap. The color table is not present for bitmaps with 24 color bits because each pixel is presented by 24-bit red-green-blue (RGB) values in the actual bitmap data area. The colors in the table should appear in order of importance(*ronald det.al,2003)*. This helps a display driver render a bitmap on a

device that cannot display as many colors as there are in the bitmap.

The BITMAPINFO structure can be used to represent a combined bitmap-information header and color table. The bitmap bits, immediately following the color table, consist of an array of BYTE values representing consecutive rows, or "scan lines," of the bitmap. Each scan line consists of consecutive bytes presenting the pixels in the scan line, in left-to-right order. The number of bytes representing a scan line depends on the color format and the width, in pixels, of the bitmap. If necessary, a scan line must be zero-padded to end on a 32-bit boundary. However, segment boundaries can appear anywhere in the bitmap. The scan lines in the bitmap are stored from bottom up. This means that the first byte in the array represents the pixels in the lower - left corner of the bitmap and the last byte represents the pixels in the upper-right corner(http://www.digicamsoft.com/bmp/bmp.html) .

5.4 Bitmap data

This block of bytes describes the image, pixel by pixel. Pixels are stored "upside-down" with respect to normal image raster scan order, starting in the lower left corner, going from left to right, and then row by row from the bottom to the top of the image. Uncompressed Windows bitmaps can also be stored from the top row to the bottom, if the image height value is negative. The only four legal numbers of bits per pixel are 1, 4, 8, and 24.The biBitCount member of the BITMAPINFOHEADER structure determines the number of bits that define(http://www.digicamsoft.com/bmp/bmp.html) each pixel and the maximum number of colors in the bitmap.

5.5 Bitmap-file structures

Each bitmap file contains a bitmap-file header, a bitmap-information header, a color table and an array of bytes that defines the bitmap bits. The file has the following (http://www.digicamsoft.com/bmp/bmp.html) form:

BITMAPFILEHEADER bmfh;

BITMAPINFOHEADER bmih;

RGBQUAD aColors[];

BYTE aBitmapBits[];

6. TECHNIQUES

6.1 Introduction

An early work on the image steganography is Least Significant Bit technique (LSB). This technique is simple in regarding the embedding and de-embedding (extracting messages) processes. To hide a secret message in an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.

6.2 Least significant bit

Since BMP is not widely used the suspicion might arise if it is transmitted with an LSB stego . When image are used as carrier in Steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image . The massage can be stored in the LSB of one color of the RGB value or in the parity bit of the entire RGB value . A BMP is capable of hiding guite a large message . LSB in BMP is most sutable for applications where the focus is on the amount of information to be transmitted and not on the secrecy of that information. If more number of bits is altered it may result in a larger possibility that the altered bit can be seen with the human eye . But with the LSB the main objective of Steganography to pass a message to areceiver without an intruder even knowing that a message is being passed is being achieved .

6.3 Stego–1 Bit LSB

The data stored in the computer as bits, and the bit is the smallest unit which hold the information; and that is in theory. But practically the bit is positive or negative electric pulse and represented as o or 1 just.

And each 8 bits together named Byte, and the bit is one field from binary number 0 or 1.

The byte from 8 bits, so the byte include 2^8=256, and each 1024 byte = 1 Kilo Byte (KB), each 1204(KB)=1Mega Byte (MB) and each 1024(MB)= 1Gega Byte (GB)

The values of bits in each byte been like this:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

And that clear that the one bit represent 256 value , from 0 when each bit hold 0 (0 0 0 0 0 0 0 0) to 265 when each bit hold 1

So, if we want to represent number 65 by using binary system it will be:

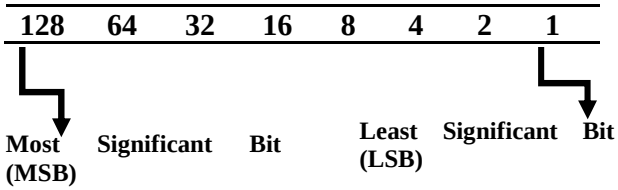
0	**1**	**0**	**0**	**0**	**0**	**0**	**1**

And the last number which is in the right represent the least significant bit.

Now, if you try to change the right number from 1 to 0, the number will be 64 rather than 65.

And try to change the left bit from 0 to 1, the number will be 193.

And that means that the last bit is the least significant bit (I mean the right bit) and which even if we change it to 0 the number becomes 64.



The least Significant Bit and The Most Significant Bit.

Now, if we are going to change this value; that will not make clear changes to that level that can make us discover the additions or changes were done. And the one byte doesn't represent the color value of color image alone; there are two bytes with it. That means that the change will be least than if it done. And that what make us going to clear images rather than the images has gray gradient in hiding process.

This method changes only single LSB in the image . Changing the LSB will only chang the integer value of the byte by one . This small change is not noticeable . The visual appearance of a color and hence the image itself is not changed .

Image based steganography using truth table based on RGB indicator used pixel and from this pixel take the random value for R, G or B, when LSB for two value from RGB equal to 0 will convert to 1 and when equal to 1 will convert to 0، and this value will be the X, Y coordination of the pixel in the image. And the second step by using additional module 2٦. Third, is to hide by pixel indicator technique for RGB image steganographically. An image can define as a matrix, and it is array from pixels, each pixel has x-axis and y-axis and include RGB values, and each color from these contain 8 bits.

In the algorithm we have (the user will enter the number and the program will go to the pixel hold this number) choose pixel and choose two random value of RGB color value of this pixel, the first one will be the X value and the second will be the Y value, and the (x,y) is coordinate of other pixel in the image Ex. in first time; Requests from the user to enter number from 1-240,000 to determine the first pixel and choose R and B value, so R=X-coordinate and B=Y-coordinate for the new pixel, then hide the text in this new pixel. And to second hide the program will choose other random pixel and choose from it the random color value i.e. GB and so on.

The next attempt we have use a mathematical operation called additional modulo in between the text and the third value of color is the key. Use additional module 26 in modular arithmetic by using encryption formula, The formula is given below:

$$C \equiv p + K \bmod 26 \qquad (1)$$

After, convert the message by using ASIIC code, and then convert to binary used indicator technique for RGB images.

Now, we use least two significant bits technique (LSB) of one of the channels Red, Green or Blue as an indicator of data existence in the other two channels. The indicator bits are choosing randomly in the channel. The indicator channel is not fixed. And chosen based on a sequence. In the first pixel Red is the indicator, while Green is channel 1 and Blue is the channel 2. In the second pixel, Green is the indicator, while Red is channel 1 and Blue is channel 2. In third pixel Blue is the indicator, while Red is channel 1 and Green is channel 2. And it will stop based on the length of the secret message, which is stored in the first 8 bytes of the cover image.

During our implementation phase, we have tested the algorithm for different sets of images as well as text messages. For each and every normal bitmap images the proposed technique is working fine. We have also calculated that using a standard 300 X 400 (120,000 pixel) bitmap image, have been used to hide text message of 240,000 characters. So, to illustrate my model, we will show only one satisfactory experimental result due to the limitation of space.

To test the algorithm, let we send the text message:
(HI)

- The first method request from the user to enter a number from 1-240,000 to determine the first pixel and take two random value from RGB, when LSB equal to 0 the program will convert it 1 and when it equal to 1 it will convert it 0, suppose R= 122 and B= 30, so we will have two-dimensional (122, 30), then Chose pixel to coordinate (122, 30).
- Now, in the next attempt we will encrypt the original text message letter by letter by applying a Function which involves certain mathematical operations using addition modulo 26, and the key will be the third color value and it is here the green color, and guess its value is 13, and will apply module 26 function: (equation (1)); *p*= value of litter, and here is the table of coding scheme for alphabetical:

Table 2. Table Of Coding Scheme For Alphabetical

A	**B**	**C**	**D**	**E**	**V**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	1 0	1 1	**1 2**
N	O	P	Q	R	S	T	U	V	W	X	Y	**Z**
1 3	**1 4**	**1 5**	**1 6**	**1 7**	**1 8**	**1 9**	**2 0**	**2 1**	**2 2**	**2 3**	**2 4**	**2 5**

H= 7 and I = 8
And compensation in the formula:-
C= p + K mod 26
C= 7 +13 mod 26
C= 20
And as in the table; U = 20, or applying the formula on I letter so it encoding to V letter. So then I have two letters (UV) and then convert it to ASCII code table then to binary and hide it. Then back to ASCII code table, we will find (UV) value:-
U= 85 and V = 86
And convert to binary code The value will be ( )

- Then the program will hide (HI) pixel in coordinate (122, 30). By using pixel indicator high capacity technique for RGB image based steganography.

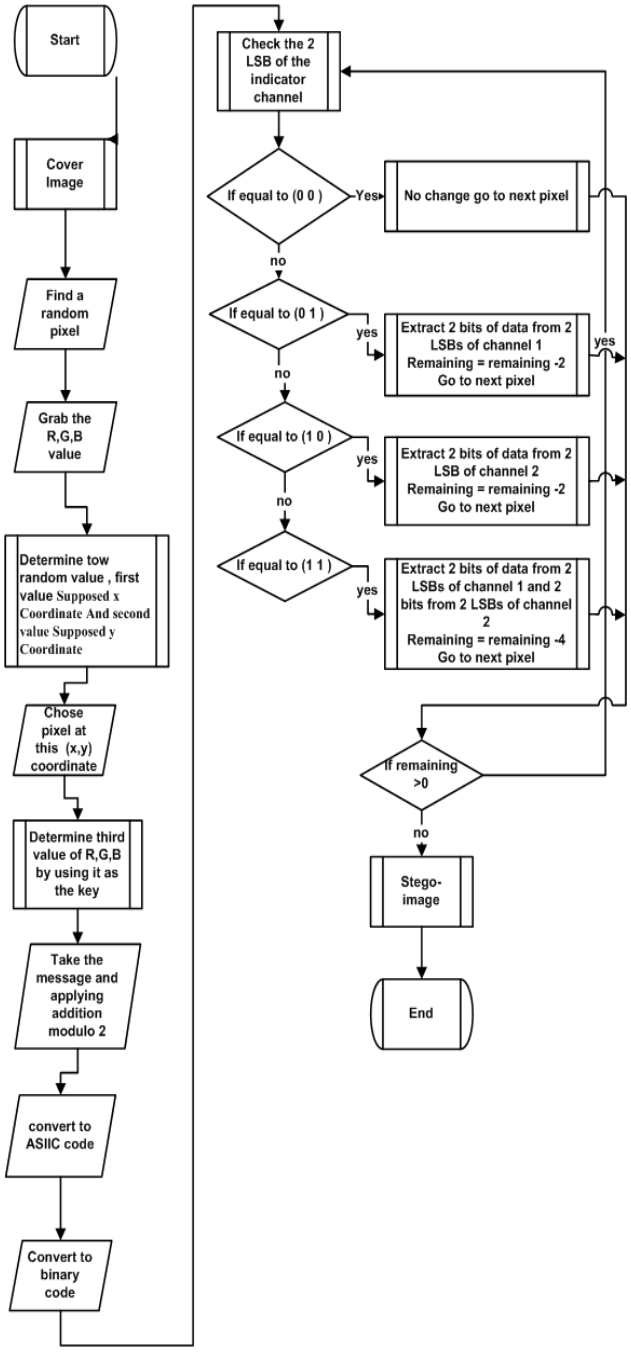


Fig. 2. Hide Text Flowchart

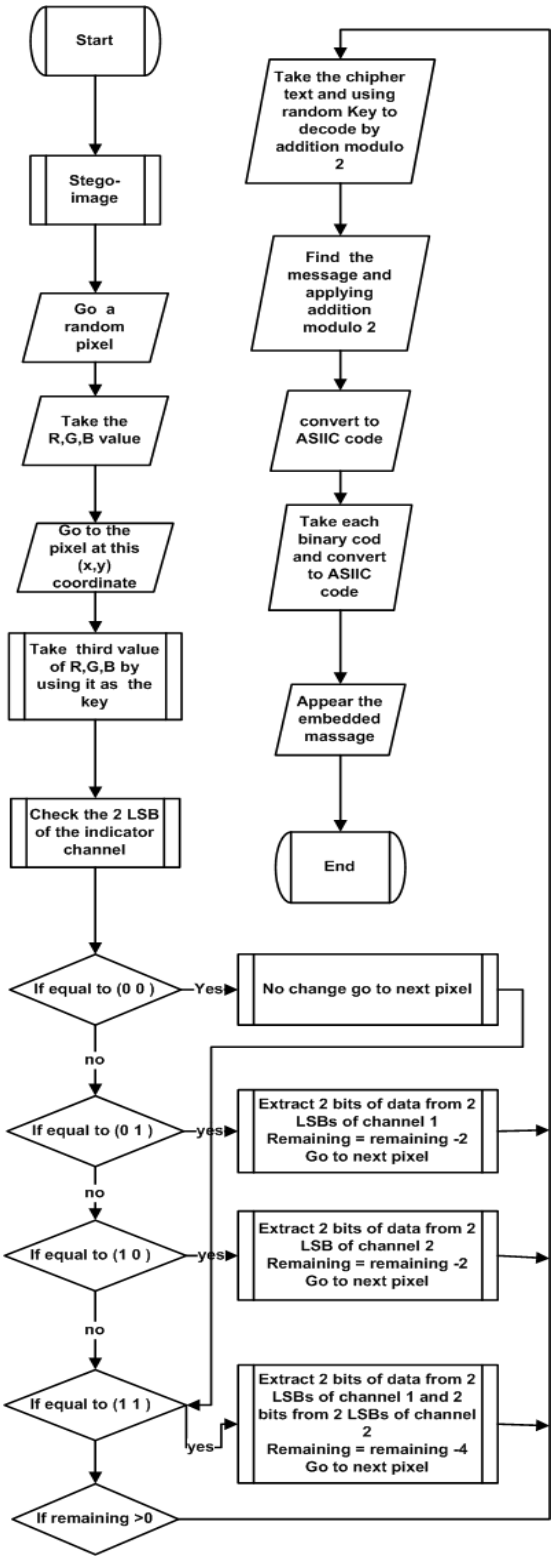


Fig. 3. Find Text Flowchart

We have used new technique based on requests from the user to enter number from 1-240,000 to determine the pixel, then take R,G,B value and convert its value to array 2*2(Row count equal column count), and R, G value will be the first row value, and B, W values will be the second row value (W is the requests value from the user which he should enter it between 0 to 255).

We convert it to 2*2 array to find determine of the array.

The way to find determine: (RxW – GxB)

We will take the absolute value then make it on mod 255 and then go to the channel has the value witch same as most 255 result and consider as indicator. So, the text will hide based on the indicator.

After, we hide it by pixel indicator technique for RGB image steganographically. An image can define as a matrix, and it is array from pixels, a 24-bit color image has three components corresponding to Red, Green and Blue. The three components are normally quantized using 8 bits. An image made of these components is described as a 24-bit color image. Each byte can have a value from 0 to 255 representing the intensity of the color. The darkest color value is 0 and the brightest is 255.

The algorithm chooses pixel to hold the number entered by the user and take R,G,B value of this pixel, and choose the W value from the user, this number will be between 0 and 255 , Then convert R,G,B,W to array 2*2 .

The R,G in the first row and B,W in the second row, then calculate the determine for the array by multiply the first value with the fourth value then subtraction it from the status value from multiply the second value with third value.

We make mod 255 for determine value because the color. Then take the determine vale; and choose value for R, G and B same as determine value and every time take new value.

There are many applications for digital steganography of images, including copyright protection, feature tagging, and secret communications, to test the validity of this technique, we will impose value, and an experiment was done to test the effectiveness of the algorithm.

We have also calculated that using a standard 450 X 500 (255,000 pixel) bitmap image, have been used to hide text message of 450,000 characters. When the user enter a number from 1-255,000 to determine the first pixel the value will be R= 30, G= 10, B=19, W= 22.

$$\begin{bmatrix} 30 & 10 \\ 19 & 22 \end{bmatrix}$$

$\Rightarrow$ Determine = (30*22)-(10*19) = 470

Then, take mod 255 for value = 215, so it will go to the pixel which has R value =215, When find more than once from R=D in the cover Image , this will hide as order vector color and consider as indicator and hide Band G.

7. RESULTS AND DISCUSSION

In steganography, checking the effectiveness of an algorithm can be done by performing steganalysis. Steganalysis is the art of detecting hidden information. Usually, people do not have the original images making it more difficult to tell whether there is hidden information on an image. Here, we satisfy the aim that says Steganography is an effective way to obscure information and hide sensitive information.

The present algorithm allows an individual to hide information inside other information with hopes that the transfer medium will be so obscure that no one would ever think to examine the contents of the file. The algorithm which is described by determine or coordinate array is presented and it is possible to implement a Steganography algorithm to hide a large amount of information into carrier bitmap image.

We used layers of security by obscuring the context in which it was transferred with continued research and an improvement in algorithms design and using the array features, and encrypt the information before hide it and using key also.

The algorithm is more efficient than the most familiar algorithm like (S-Tools) Capacity: The amount of data that can be hidden without significantly changing the cover medium (M.Juneja,P.S. Sandhu, And Ekta Walia.etc,2009). The capacity of information can be hidden in the S-Tools twice that what hidden in my algorithm look for table See table 4 and 5 for an example.

Impression about robustness is that it is achieved, as long as the image is not modified or compressed. If this robustness issue is true, the algorithm request key to improve the security, and in the following table
See table 3 for an example.

Table 3. Rotation Between S-Tools And My Propose

	S-Tools	My Algorithm
Robustness (ROB)	Low	High
Domain type (DOM)	Low	High
Capacity	High	Low
Confidentiality	Low	High

In the above table; the domain type is high because we use the indicator then the array features then using MOD feature, and about the confidentiality we think it is high because we used more technique to hide the text and it can be more secure by hides the data at the top right corner of the image and works its way across the image (then down - in scan lines) pixel by pixel.

Chen and Wornell state that there are three conflicting goals to any information hiding technique: maximizing capacity, minimizing distortion between cover-object and stego-object, and maximizing robustness. Information hiding models should be perceptually transparent.

Table 4. Capacity Of Data

Count of pixel on image	S-Tools	**First propose**
120,000	360,000	240,000

Table 5. Capacity Of Data

Count of pixel on image	S-Tools	**second propose**
255,000	765,000	510,000

8- SECURITY ANALYSES

In the propose image based on steganography using truth table also based on RGB indicator; the user will choose number of the pixel, and that in the analyst stage is difficult to know the number of the pixel which chosen. In addition, if we guess that the crackers knows the number which entered, so the hiding will not be in the pixel which hold that number chosen. The application will follow more than one step to reach to the pixel. In brief, it will take not only two values from RGB values, but will be the (x, y) coordinate of the pixel hidden inside it, using truth table based on RGB indicator using pixel , using the additional module will make it more secure and more difficult to break it from the cracker as well.

To improve the security level that barely met; the program will not hide the text in the chosen pixel which will increase the security level. The procedure will start by taking the three values from RGB and fourth value (W) which were random values taken from the end user. Then make Mod 255 before hiding the text inside a pixel; Encrypting the message before embedding it will aid in safeguarding from being figured out by unauthorized person who success to decode the data .The RGB has three channels, and will be changed by continuing without roles, and by using the indicator on many places on the image that will improve the integrity of the message .

However, none of steganographic methods we examined could resist a concerted attack if someone knew that there was a message in a given document. For the greatest level of secrecy, a combination of both steganography and cryptography is necessary.

The sequential method hides the data at the top left corner of the image and works its way across the image (then down - in scan lines) pixel by pixel. As it goes on , it changes the least significant bits of the pixel colors to match the message. To decode the process the least significant bits starting at the top left are read off. This is not very secured because it's really easy to read off the least significant bits. It also isn't clever because if the message doesn't completely fill up the possible space then just the top part of the image is degraded but the bottom is left unchanged - making it easy to tell what's been changed.

9. CONCLUSION

In this survey we have developed two new techniques to hide text in an image, by using the array features to improve the security for the hidden text, secure the information, choose pixels and hide in another, also using indicator to be difficult to retrieve the data. We have applied these techniques in the purpose of hiding data by using LSB. We believe there will be a huge increase in the legitimate uses of stego in the business world. One key to the increased use of stego will be more automation of the process of transporting a file to the end user.

REFERENCES

A. Gutub, L. Ghouti , A. Amin, T. Alkharobi, M.K. Ibrahim, "Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking", Inter. Conf. On Security And Cryptography - Secrypt, Barcelona, Spain, July 28 - 31, 2007.

Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi "Pixel Indicator High Capacity Technique For Rgb Image Based Steganography "

Xiangyang Lu, Daoshun Wang, Wei Hu2 and Fenlin Liu1"Blind Detection For Image Steganography: A System Framework And Implementation "Received October 2007; Revised March 2008

B. Chen and G. W. Wornell, "Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia," The Journal of VLSI Signal Processing, vol. 27, pp. 7-3, 2001"

Deshpande Neeta, Kamalapur Snehal "Implementation Of Lsb Steganography And Its Evaluation For Various Bits " Computer Science Dept ,K.K.Wagh Institute Of Engineering Education & Research, Nashik India

Daniel L. Currie, III, Cynthia E. Irvine"Surmounting the Effects of Lossy Compression on Steganography" Naval Postgraduate School, Proceedings of the 19th National Information System Security Conference, Baltimore, Md, October 1996,pp. 194-201.

Farhan Khan And Adnan Abdul-Aziz Gutub "Message Concealment Techniques Using Image Based Steganography "Department Of Computer Engineering, King Fahd University Of Petroleum & Minerals, Dhahran, 31261, Kingdom Of Saudi Arabia.

Hassan Mathkour , Batool Al-Sadoon, Ameur Touir , "A New Image Steganography Technique" Computer Science Department ,College Of Computer And Information Sciences ,King Saud University ,Riyadh Saudi Arabia © 2008

Mamta Juneja, Parvinder S. Sandhu, And Ekta Walia "Application Of Lsb Based Steganographic Technique For 8-Bit Color Images "Proceedings Of World Academy Of Science, Engineering And Technology Volume 38 February 2009 Issn: 2070-3740.

Momotaz Begum, Nurun Nahar, Kaneez Fatimah, M. K. Hasan, and M. A. Rahman"an efficient algorithm for codebook design in transform vector quantization" Bangladesh University of Engineering and Technology (BUET), Dhaka-1000, Bangladesh, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, Canada

Joshua Silman "Steganography and Steganalysis: An Overview",from the SANS Institute Reading Room site,august 2001.

T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," inProceedings of the Fifth Annual Information Security South Africa Conference(ISSA2005), Sandton, South Africa, June/July 2005

Clifford Bergman and Jennifer Davidson 'An Artificial Neural Network for Wavelet Steganalysis' Iowa State University, October 1, 2004–September 31, 2006

Ronald D. Krutz, consulting editor " hiding in plain sight:steganography and the art of covert communication " john miano , edition: 2, compressed image file formats: jpeg, png, gif, xbm, bmp, illustrated ,published addison-wesley, 1999

Jonathan cummins, Patrick diskin, Samuel lau and Robert parlett "Steganography and digital watermarking" copyright © 2004, , school of computer science, the University of Birmingham.

Rafael c. Gonzalez, Richard Eugene woods "Digital image processing" copyright 2008.

ingemar j. cox ,matthew l. miller ,jeffrey a. bloom ,jessica ridrich ,ton kalker (digital watermarking and steganography) Copyright © 2008 by Elsevier Inc. All rights reserved.

http://www.fileformat.info/format/bmp/corion.htm accessed on 16/12/2008

http://en.wikipedia.org/wiki/BMP_file_format accessed on 16/12/2008

http://atlc.sourceforge.net/bmp.html accessed on 17/12/2008

http://www.whisqu.se/per/docs/graphics52.htm accessed on 16/12/2008

http://local.wasp.uwa.edu.au/~pbourke/dataformats/bmp/ accessed on 2/1/2009

http://www.designer-info.com/Writing/bmp_tiff_jpeg_gif.htm accessed on 2/1/2009

http://www.daubnet.com/en/file-format-bmp accessed on 3/1/2009

http://www.um.edu.mt/__data/assets/pdf_file/0019/53263/Ing._Paul_Debono_1.pdf accessed on 12/2/2009

http://www.martinreddy.net/gfx/2d-hi.html accessed on 12/2/2009

http://www.digicamsoft.com/bmp/bmp.html accessed on 17/12/2008

http://graphicssoft.about.com/od/glossary/g/bitmap.htm accessed on 3/1/2009

http://personal.denison.edu/~bressoud/cs171-f06/programs/steganography.html accessed on 2/1/2009.

AUTHORS PROFILE

Walaa Ismaiel Abu Marie received the B.E. degree in Information Technology and communication from University of Arab Open University, Saudi Arabia, Riyadh branch, in 2009.

Adnan Abdul-Aziz Gutub is currently working as a researcher at the Center of Research Excellence in Hajj and Omrah at Umm Al Qura University, Makkah Al-Mukarramah, all Muslims religious Holy City located within the Kingdom of Saudi Arabia.

Adnan is an associate professor in Computer Engineering previously affiliated with King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran, Saudi Arabia. He received his Ph.D. degree (2002) in Electrical & Computer Engineering from Oregon State University, USA. He has his BS in Electrical Engineering and MS in Computer Engineering both from KFUPM, Saudi Arabia.

Adnan's research interests are in optimizing, modeling, simulating, and synthesizing VLSI hardware for crypto and security computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields. He has some work in modeling architectures for RSA and elliptic curve crypto operations. His interest in computer security also involved steganography such as simple image based steganography and Arabic text steganography.

Adnan has been awarded the UK visiting internship for 2 months of summer 2005 and summer 2008, both sponsored by the British Council in Saudi Arabia. The 2005 summer research visit was at Brunel University to collaborate with the Bio-Inspired Intelligent System (BIIS) research group in a project to speed-up a scalable modular inversion hardware architecture. The 2008 visit was at University of Southampton with the Pervasive Systems Centre (PSC) for research related to advanced techniques for Arabic text steganography and data security.

Adnan Gutub filled many administrative academic positions in KFUPM; he had the experience of chairing the Computer Engineering department (COE) at KFUPM from 2006 to 2010.

Hussein Abu-Mansour is currently a PhD candidate in Huddersfield University, UK. He received his Bachelor in computer science from Al-Zaytoonah Private University, Jordan(2001) and MSc from Jordan University of Science and Technology, Jordan (2003). His research interests include data mining, steganography and Knowledge discovery from database.