International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.6 (Nov-2020)

http://dx.doi.org/10.12785/ijcds/0906023

Un-Imperceptible Image Steganography Approach (U-IISA) in Excel sheet

Maad Kamal Al-anni[1], Rafah M. Almuttairi[2] and Husam Ibrahiem Husain Alsaadi *[3]*[4]

[1]Faculty of Engineering, Al-Iraqia University, Baghdad, Iraq
[2]Faculty of Fine Arts, University of Babylon, Babylon, Iraq
[3] Faculty of Education, the University of Mustansiriy, Baghdad, Iraq.
[4] Faculty of Engineering, Altinbas University, Istanbul, 34676, Turkey.

Received 16 Apr. 2020, Revised 22 Oct. 2020, Accepted 24 Oct. 2020, Published 1 Nov. 2020

Abstract: : obliquely, the obfuscation becomes the vital mannerism for preserving the surreptitious data, so far it is necessary to pay more attention to the art of hiding important images for the purpose of sending crucial decisions through the public media. It is usually happened to hide important data in the image file to keep them away from being hacked illegally. The current work, a unique and efficient method for hiding images in the MS Excel file is proposed, where data can be transferred with speed and security with slight changes in the file size or any doubts from whom previously read its specifications or even the naked eye could not recognize the variation, could be un-imperceptible for interceptors. The proposed method is to hide the colour or gray image with varied sizes impeded in the Excel file in order to be transferred from the sender to the recipient without any change in its resolution. It also involves transferring the colored image with its resolution details if the recipient is interested in such details, or it could be transferred as a gray image if the color is not a required datum. In both cases, the color does not affect the safety instead of the involving speed through the process of sending and the speed of image recovery by the recipient where the size of the data decreased, the main strength of Propose System is the method does not affect the file used for hiding along with the mannerism of handling the information header with its technique is unique so far being involved in literature survey. Wheras there is no difference in the technology of embedding, but a difference in the method of embedding, we do not use traditional approach or sequential approach to embed the data, we use zigzag approach, and likewise, the coding method is unconventional, it is new approach as we mentioned in the manuscript.

Keywords: Steganography, Encryption, Gray and Colour Image, MS –Excel Sheet, Least Significant Bit(LSB

1. Introduction

Nowadays, the surreptitious data becomes more and more vulnerable than computer assets, so it has become necessary to pay attention to the art of hiding important secret images in order to send them to the places where critical decisions are made. Usually, the important data is hidden in different files such as video, images, sound, or other files in order to protect it from those who are trying to access them illegally. In the proposed method, images with different sizes (original size, 256*256 and 512*512) and different colors (colored or gray) were hidden by embedding them inside an Excel file for transfer from the sender to the recipient, depending on the desire to win quality or speed, or both, where if the color details are important to the recipient, we send them as they are, without changing the color and if they are not important, they are sent in gray to reduce the speed of embed and retrieval. As for the size, it depends on the importance of the accuracy of the images to the recipient. The larger it is, the more accurate it will be, but the faster the embedding and retrieval rate. In all cases, the color and size do not affect the confidentiality of the information, but rather the speed of embedding at the sender and the speed of image recovery at the recipient when the size of the data embedded is less.

In this proposal, sophisticated methods of encryption and concealment were used, so that the unauthorized person could not retrieve that data when doubting its existence. Matlab programming and GUI interfaces were used to facilitate the application process for the user.

The most important features of the application include:

- The consistency or fixation of file size: A very slight change in the file size of the vector. As the file size of the Excel does not change by embedding an image except by a slight amount (several kilobytes) compared to the size of the hidden file (several few megabytes

Email: muad.rashed@aliraqia.edu.iq, maadk_anni@live.com, rafah@uobabylon.edu.iq, husam.alsaadi@ogr.altinbas.edu.tr

- Unrecognizable: The involvement would be hidden enough to the extent that it could be even felt with the naked eye or by any person. It would absolutely be unrecognizable that there is such an image file within the Excel file.
- No cost required: It doesn't need to buy expensive computers, no need for high necessary expenses for executing the application. It is possible to be applied on normal personal computer with its available normal properties. The higher the processor speed, the faster the hide and retrieve speed
- Facilitate to use: It can be applied by those who do not have programming experience. The application has interfaces that even persons with low PC skills could use it easily. It has been programmed with GUI interfaces to make it friendly to the user.

A. *Beneficiaries of the Application:*

It is used in many fields, such as medical and military, it can be useful and usable for transferring images of secret maps between the distance military headquarters. So through setting a plan of a roadmap to any military process and the leader would transfer it to the specified situation of execution, he could send it easily by the meant Excel file and transfer it safely, so if it is hacked by the enemy, the data would be saved unrecognizable. The enemy would concern with textual data rather the image data. Then if the map is colored and necessary to transfer it with full details, means the color is necessary to be saved as it is for its necessity. Otherwise, if the colures are not important to be sent so it could be transferred plainly without the details or data of colors that will ensure small size data and recovery speed through receipt where the time of recovering and transferring is so important to be concerned with especially in the military or medical issues and so on.

The difficulty of retrieving the image in the proposed method comes from the following reasons:

- Encryption: the embedded data is encrypted in a complexed way.
- Masking method: the method of masking, which is embedded randomly in the Excel file, is very complicated.

Embedding method: the method of embedding data is not serial, but zigzag.

2. RELATED WORKS

In [6], they proposed impervious stages to the research work by adding multi-security levels that create multiple-defense frontals against brute force. Thus, it is a little bit complicated for an unauthorized person in order to visualize the original data or intact it, , they proposed the grey-level adjustment and different encryption calculations (bitxor and shuffling operation of bit-wise, and stegano-based cryptography), and information hiding which accomplishing at the average of normal PSNR of 58dB, RMSE with 0.6673, and NCC with 0.9917 of their proposed framework with contrast and existing research done in the state of arts with PSNR=40, RMSE=0.8115, and NCC=0.981, so they improved the security just as the nature of stego images and gave promising outcomes as far as imperceptibility and security. In addition, the excellent stego images and its less changeability in histogram, likewise approve the validation of the proposed approach.

In [7], they used the art of steganography in cover medium with imperceptible visualization by three image channels. Additionally explained that the steganography better hiding data than cryptography due to it conceals the substance of the message yet not the presence of the message without the attention to steganalysis as brought right now, productive Steganography systems are being presented dependent on LSB based Steganography(two significant bits), diagonal pixels of the image. Symmetric and Asymmetric key- based cryptography additionally being utilized right now.

In [8], a new mechanism for steganography has been presented in order to secure a huge sensetive data via cover media as three channel image. different Size Image Segmentations (DSIS) and Modified Least Significant Bits (MLSB) where used in this work, DSIS algorithm has been utilized randomly instead of sequentially for embedding a secret image before embedding itself; The random replacement also applied to the bit-wise at byte, an effective hypothesis is shown simulation results that is employed efficiently and satisfied high imperceptible steganography images for both low band and high band of payload.

In [9], author introduced the approach of encoding the audio message, then hiding a short audio message into three channel media (Red-Green-Blue palette) using Least-Significant Bit (LSB) technique, the introduced a technique that demonstrated a higher resemblance between the cover image and attained steganography image, he had also concluded of future work by embedding the audio message within video file.

Reference [10] at 2018 presented the Stenography through the font color palette of MS-Excel Sheet Cells with the mechanism of the embedding the sensitive information, it the primary methodology used to conceal the information, considering the technique for movement between non-empty cells of the content and the sequential mannerism for selecting the actual hiding cells increasing camouflage whenever the outside looker or intruder tries to guess or visually preview, meanwhile it adds the significant role for perturbation of extracting those data by the intruder or unauthorized user and makes the approach much more sophisticated against the brute force.

Reference [11] was proposed a modern approach for stowing away data by utilizing the spacing occurred inter-word and the inter-paragraph as a crossover technique in the research work for steganography.

In [12], researchers introduced a Zigzag Hybrid Embedded calculation that is utilized in the proposed framework. DES and LSB methods used to encode information and afterward concealed it in the Excel sheet, assumption to have a three channel pallet (Red-Green-Blue) which permits dissipating the encoded information upon Cover Excel File (CEF) with a slight changes in Background Color Schema. The modification after embedding is slightly for visual observatory sense, brute force or intruders have explicitly no chance in attempting to discover, it would be so doubtful to observe the modification, no opportunity to figure any progressions by visual look.

In [13], another methodology for steganography in Microsoft words MS-word, the primary thought is that setting any background color for undetectable characters, for example, the space or the carriage return isn't reflected or seen in the file properties.

3. Terminology and basic knowledge

A. Image

An Image is a portrayal of a Real picture as series of coefficients that can be stored and dealt by a computerized PC. So as to make an interpretation of the image into its coefficients, it is separated into small pieces called pixels (picture components). For every pixel, the image-driven collector records a pixels, or a series of coefficients that depict some properties, for example, its attribute (the intensity of the light) or its shading that translate into numerical values [1] [2]. The values are in assortments of rows and columns that relate to the vertical and horizontal location of the pixels in the picture as shown in Fig.1.

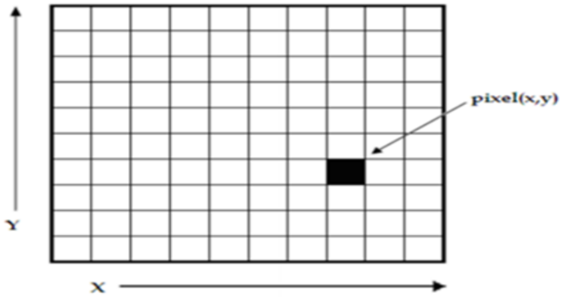


Figure 1. Digital Image Pixel

Computerized pictures have few fundamental qualities. For instance:-

1) Digital Image: Digital images (Monochrome Image)are the least complexed kind of pictures and can take on two values, normally highly contrasting, or [0] & [1]. A paired picture are alluded to as a 1 bit/pixel image while it takes just a binary digit to represent each pixel. Show Fig.2.

Two-level Images are regularly made from Grey-scale Pictures through a threshold is turned white "One", and those below it turned black "Zero" as shown in Fig.2. We distinguished parameter of object in the picture to be as (2)

$$b(x,y) = \begin{cases} 1 \; if \; the \; point \; in \; the \; object \\ 0 \; if \; the \; point \; in \; the \; background \end{cases} \quad (1)$$

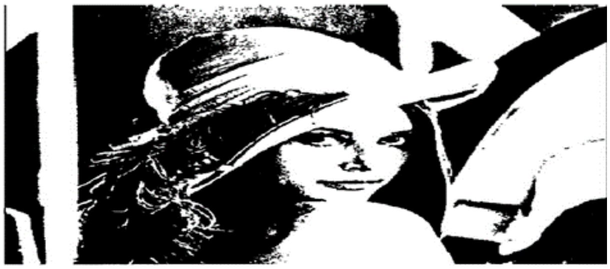
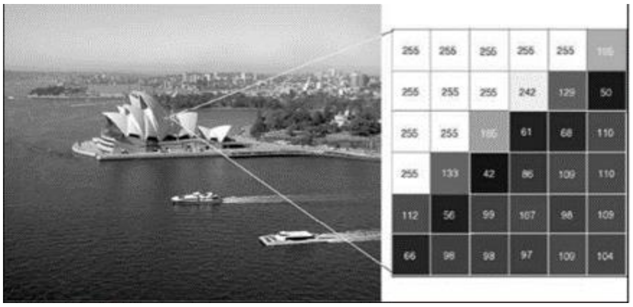


Figure 2. "One" or "Zero" is allotted in each pixel as a single bit (0 or 1) • A 640 x 640 two-level image requires 43.5 KB of storage.

2) Grey-scale image: Grey-scale pictures are always referred to as monochrome, or one-color Image. They contain brightness data, no color data. The different various brightness levels are accessible. The typical image contains 8 bit/pixel (information, which permits us to have the range (0-255), the far high value indicates distinctive brightness (black) levels as shown in Fig.3. The 8 bits image is commonly because of the way that the byte is represented, which relates to 8-bits of information is the standard unit in the realm of computerized PC with 6 x 6 sub-region as shown in Fig.3.



255	255	255	255	255	185
255	255	255	242	129	50
255	255	185	61	68	110
255	133	42	86	109	110
112	56	99	107	98	109
66	98	98	97	100	104

Figure 3 . A 680 x 520 grayscale image requires over 360 KB of storage, with 6 x 6 sub-region details.

3) Color Image: Color image utilized two-dimenional matric for each color channel with the same size likewise, two-dimentional matric for red (R), two-dimentional matric for green (G), and two-dimentional matric for blue (B) as shown in Fig.4. every pixel is normally represented to be a 24-bit number containing the measure of its red (R), green (G), and blue (B) parts, For some applications, RGB color info is changed into scientific space that decouples the brightness info from the color info. The *hue/saturation /lightness (HSL) color change permits us to depict RGB Imags in such a way that it can be more promptly comprehend as it is illustrated in Fig.4.*

Figure 4. Three bytes (e.g., RGB) channel image are depicted each pixel, 640 x 480 24-bit color image, 921.6 KB of storage

1) Indexed Image: An Indexed representation—where a 2D matrix contains a pointer to a color palette (or Look Up Table - (LUT)), a 2D matrix of a similar size as the image contains files (pointers) to a color palette (or color map) of fixed greatest size (typically 256 colors). The color map is just a list of colors utilized in that image. (Fig. 5) shows an indexed color image and a 4 × 4 selected region, where every pixel shows the list and the estimations of R, G, and B at the color palette that the file focuses to Show Fig. 5.

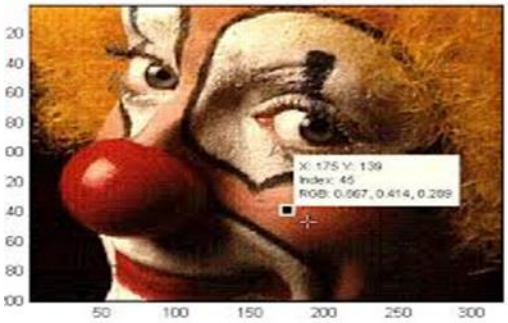


Figure 5. Indexed Image Requires Color along with Look-Up Tables (LUTs), A 640 x 480 8-bit color, storage of 307.2 KB.

B. Least Significant Bit (LSB)

While having a look from outside of MS-Excel sheet, the two types of the possible interchange and exchanging of normal Excel file, while in fact, this Excel file is loaded with invisible bit-wise concealment, it could be embedded the intended image into an Excel file by using Least Significant Bit (LSB). The least significant bit is the lowest bit and is the least significant value in a series of numbers in bit-wise binary representation; For example, in the binary bit-wise 00111001, the Least Significant Bit LSB is the far right [3] of bit-wise . The Most Significant Bit (MSB) happens as we move to the far left [4] of bit-wise. (MSB) 10111001 (LSB) number 00111001.

So, the cryptographer maintains the concealing of the secret image within a color pallet of three channels (Red-Green-Blue), trivial bits should be exploited and filled by image fragments upon its strategic method. It should be noted that Steganography is quite different from the watermark: in steganography, there is a concealment of illegal data for an illegal purpose, while watermark, is mostly used to save copyrights for creative commons.

C. MS-Excel Sheet Color Schema Format

The main advantage of Microsoft Office is to provide the color schema in their default setting parameters, the Microsoft office brings us the benefaction to use these advantages for hiding the image within these Excel Cells into sheet itself, each sheet is built up with own color pallet of the cell/cells in MS Excel sheet, likewise it falls into, 1st is Font Color Formatting (FCF) schema, 2nd is Border Color Formatting schema, and last one is Formatting (BCF) schema of Background Color Formatting BCF [5]. Each one from these schema formats in MS-Excel Sheet color consists of a set of 24 binary digital numbers as Red Green Blue (RGB) color schema as illustrated in Fig.6. This schema permits the use of this method to use the image steganography using utilizing the Least Significant Bit (LSB), below are the main advantage of using the MS-Excel Format:

1) Excel file does not attract attention, because its size is small and the image size is large. The traditional thing is to not embed a large file in a small file
2) The number of cells is very large, reaching billions, and this provides us with sufficient capacity for embedding.

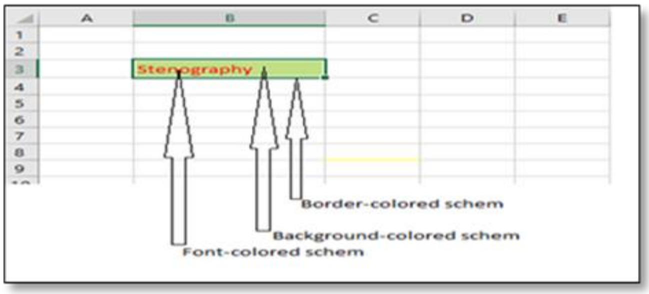


Figure 6. MS-Excel cell's color schema

C. System Specifications

The proposed systems were performed using an "Intel Core I 7, 2,26 GHz processor with 6 GB of RAM". The communication tests made with the 30 Gb/s Ethernet network in terms of high speed circumstances. It is obvious that a Matlab could run on a much more competitive machine than the expectation in terms of imperceptibility and secrecy. The program used to develop the imperceptible Image Steganography Approach (U-IISA) is Matlab R2016a as shown in Fig.12, Notification of System limitations that hamper the overall performance are, First the speed of both computers(sender and receiver), second the both sides have to use the same version of MS-Excel.

4. UN-IMPERCIBTIBLE IMAGE STEGANORAPHY APPROACH

The current work mainly proposed a method for hiding images in the Excel file. The main contribution of this paper is the use of an Excel file for transferring images by embedding the image data into the background color of Excel file cells. The idea is novel and creative. This section is to explain in depth the research technical with experiment.

Despite the proposed method reliance on the traditional (LSB) algorithm for hiding, but it is considered as one of the new methods of concealment, which started from encoding image data and then the method of zigzag way of embed it.

In order to apply the proposed model (U-IISA) for hidden image, gather all bits available in image pixel color into one vector, fragmentation and flipping parts, then defragmentation was used to encode the image data, while LSB algorithm is used to hide data via fragment the vector, finally, distribute parts on a specific Excel cell background color in zigzag way to embed it.

To apply proposed model (U-IISA) for extract image, extract data that was embedded in a specific background cell in Excel file, then gather it in one vector, after that do fragmentation and flipping these parts, then defragmentation as same as we do in embed method to obtain a new vector, depending on the type of original image, we will convert the vector to new array. As shown in Fig. 13 (Overall Proposed System (U-IISA)).

Finally, convert this array to the original image. The detailed description for this proposed model is below.

A. Preprocessing

It is the most important stage of the proposed model, as determine the below issues effects on the efficiency of the model. Decision should be taken carefully depending on the type of information need to be hided.

In some cases image could be transmit in gray even though the original one was colored, for example if authorized sender have analyzed the secret information and ensured that there is no missing data will be if the secret image has been change form RGB color to gray color, so the decision for same cases will be sending the image in gray color to gain speed and there is no wasted time to transmit unimportant data.

Another case can be effect on the efficiency of the model, the size of the secret image. Authorized sender must check the minimum size of the secret image that can contain full information of data, for example, in case the secret image is very big and if the resize of the image to small size will keep all information in save. In this case the image must be resized to the minimum to speed up transmission time. Therefore, our approach can be used to hide colored or grayed images with varied sizes. Authorized sender must be careful of the following:

- Original image size
- Size of the sent image (256*256, 512*512, …)
- Dimensions of the sent image (length and width)
- Sent image format (Gray or RGB)

The secret image file size will differ from the original size depending on the nature of the image data. The resulting file might be smaller to ensure speed up the time of embed, extract, and transmit of image in an excel file, or it might be larger to ensure the accuracy of the image data details, after that, length of encoded data and number of cells in Excel sheet are determined. Gaining speed and accuracy one of the most important aim of preprocessing stage, as our method does not depend on a fixed size of the image, but is analyzed and decision taken to change its size and details of its data, as explained below.

The following equations are needed in preprocessing stage:

- To calculate number of bits in image:

$$No.of\ bits = length * width * No.of\ color * 8 \qquad (2)$$

- To calculate number of cells in RGB color image:

$$No.of\ cells = No.of\ bits\ /\ 6 \qquad (3)$$

- To calculate number of cells in Gray color image:

$$No.\ of\ cells = No.\ of\ bits\ /\ 4 \qquad (4)$$

In our application, the first window is image selection window, to determine the best image size and format to transmit all details of data, as shown in Fig.7.

Decision should be taken first weather the image must be embedded in the same color of the original image or there is no need for the color, in this case the colored image will be changed to a gray image to make the size of the image less, and that will affect the time of embedding data to excel cells and the time of extracting the image from excel cells, in this case we are going to gain speed.

In case the original image is small, and need to be larger to ensure that all details are cleared to the receiver, in this case the size of image will be increased and the time of embedding and extracting data of image will be increased, in this case we gain accuracy instead of speed.

In case the original image is big and there is no change in details if the size becomes lesser, we should change the size to gain the speed of embedding and extracting image.

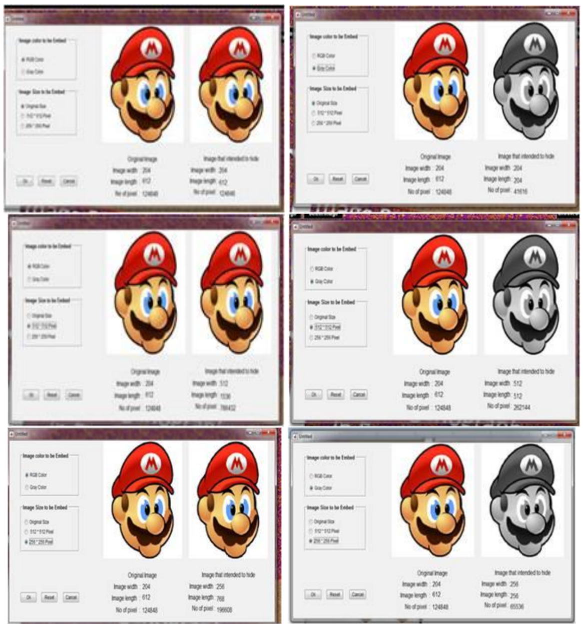


Figure 7. Original size less than 256*256 pixel

During the transition between the cases of color and size, the required choice in terms of the number of cells required for concealment becomes clear, through which we determine the win in the speed of concealment, or the accuracy of the image.

In case of the size of original image color (42*113) pixel size is smaller than (256*256), we show that to gain the speed to hide, we must select original image size with gray color, as it's the lowest in the number of cells between gray image colors that needs to hid, while if we want to gain the accuracy in the image, we must select original in both of RGB image color and size, as it's the lowest in the number of cells between RGB image colors. As we show in table 1 and Fig.8.

TABLE 1. SIZE OF ORIGINAL IMAGE IS A SMALLER THAN 256*256 PIXEL SIZE

Image size and format	Width	Length	No.of colors	bit per color	No. of bytes	No of bits	No. of cells
Original RGB	42	113	3	8	14238	113904	18984
Original Gray	42	113	1	8	4746	37968	9492
512*512 RGB	512	512	3	8	786432	6291456	1048576
512*513 Gray	512	512	1	8	262144	2097152	524288
256*256 RGB	256	256	3	8	196608	1572864	262144
256*257 Gray	256	256	1	8	65536	524288	131072

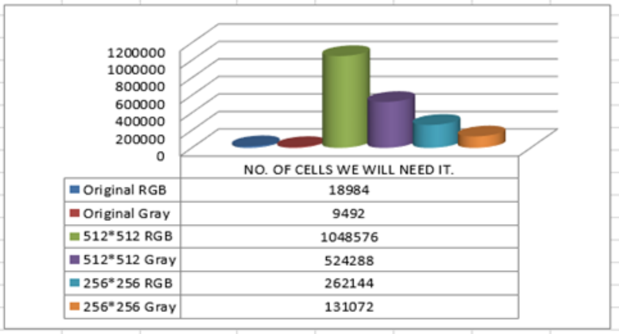


Figure 8. No. of cells needs when choice color and size image.

In the second case of the size we took original image color in (305*305) and it is between (256*256) and (512*512), we show that to gain the speed to hide, we must select (256*256) size with gray color, while if we want to gain the accuracy in the image, we must select original RGB image color with (512*512) size, it's the lowest in the number of cells between RGB image colors. If we want to gain the speed and accuracy at the same time, we select the original image without change as in table 2 and Fig.9.

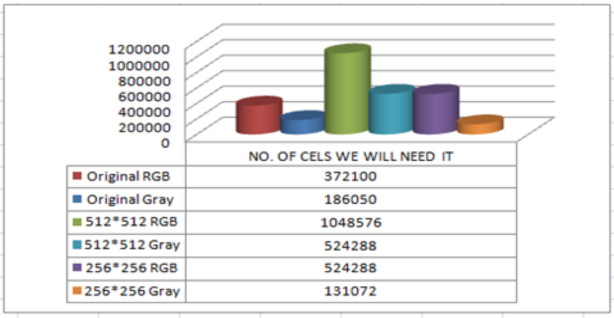


Figure 9. No. of cells needs when choice color and size image.

TABLE 2. SIZE OF ORIGINA IMAGE IS BETWEEN (256*256) and (512*512) PIXEL SIZE

Image size and format	width	Length	No. of color	Bit per color	No. of bytes	No of bits	No. of cells
Original RGB	305	305	3	8	279075	2232600	372100
Original Gray	305	305	1	8	93025	744200	186050
512*512 RGB	512	512	3	8	786432	6291456	1048576
512*512 Gray	512	512	1	8	262144	2097152	524288
256*256 RGB	256	256	3	8	196608	1572864	262144
256*256 Gray	256	256	1	8	65536	524288	131072

In third case of the size of original image color we choice a (774*1032) pixel size and it is bigger than (512*512), we show that to gain the speed to hide, we must select (256*256) size with gray color, while if we want to gain the accuracy in the image, we must select original RGB image color with original size, as we show in table 3 and Fig.10.

TABLE 3. SIZE OF ORIGINA IMAGE IS A HIGHER THAN 512*512 PIXEL SIZE.

image format and size	width	Length	No. of color	Bit per colors	No. of bytes	No of bits	No. of cells
Original RGB	774	1032	3	8	2396304	19170432	3195072
Original Gray	774	1032	1	8	798768	6390144	1597536
512*512 RGB	512	512	3	8	786432	6291456	1048576
512*512 Gray	512	512	1	8	262144	2097152	524288
256*256 RGB	256	256	3	8	196608	1572864	262144
256*256 Gray	256	256	1	8	65536	524288	131072

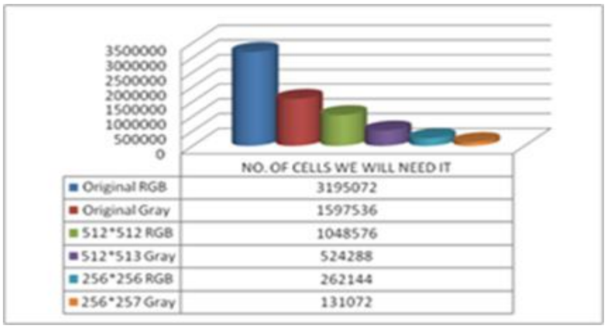


Figure 10. No. of cells needs when choice color and size image.

For the 3rd example, if we want to gain the speed and accuracy at the same time, we select the original image without change, finally, for gain speed and accuracy are briefly shown in the table 4.

TABLE 4. THE SPEED AND ACCURACY GAIN IN BRIEFLY

Image Size	Lower than (256*256)		Higher(256*256) Lower (512*512)		Higher than (512*512)	
	RGB	Gray	RGB	Gray	RGB	Gray
Original		Speed			accuracy	
512*512	Accuracy		accuracy			
256*256				speed		Speed

B. Embede Data

In this process we will embed the image data in the background color of the Excel file cells. This process will pass in several steps to prepare the image data to be an encoded data in order to embed it in the cells of Excel file.

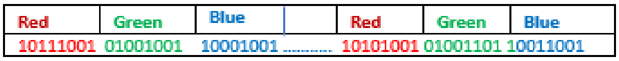
1) Select Image: When the image is selected to be hidden, upload its data to the proposed program to implement its data via some function in order to systematically change its data via encryption processes. The purpose of this encryption is to increase the protection of data from intrusion or unauthorized people to retrieve that data. Also, it is considered the first line of data protection.

If we talk about the RGB image, we know that the image data is a matrix (M, N) of pixels and every pixel of the image is a 24-bit representation of the RGB color mixture. In the following example, if this data is a part of an image and we want to embed it in a specific Excel file:

Red	Green	Blue	
10011101	10010010	10010001	1st pixel
10010101	10110010	10011001	2nd pixel
10011101	10011010	11010000	3rd pixel
10110100	11010011	10110001	nth pixel

For each color, each pixel in colored image will separately flip the data from right to left. This step is to strengthen the data encryption in order to obstruct the retrieval process by intruders, as follows:

Red	Green	Blue	
10111001	01001001	10001001	1st pixel
10101001	01001101	10011001	2nd pixel
10111001	01011001	00001011	3rd pixel
00101101	11001011	10001101	Nth pixel

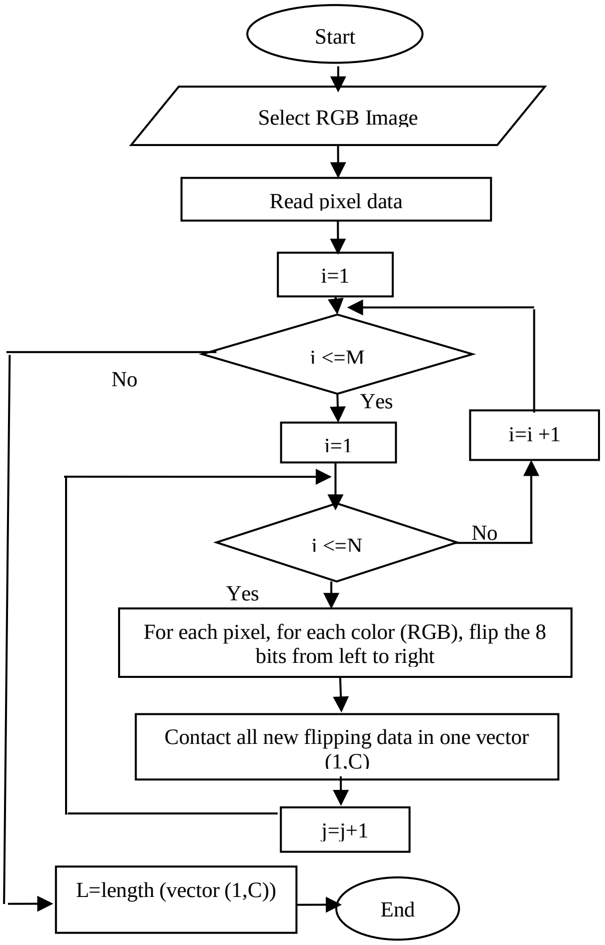


Red	Green	Blue		Red	Green	Blue
10111001	01001001	10001001	....	10101001	01001101	10011001

Then, it will gather this data into a vector (1 * n) as follows:

After this step, the image data is encrypted and is ready to embed now. In the next step we will prepare Excel data to embed the encoded data. This step is explained briefly in the pseudo code : Select Image box bellow and in the Flowchart 1.

```
Pseudo code: Select Image:
Choose the RGB image that we want to hid, read image data array (M,N).
For i= 1 to M
 For j =1 to N
     • For each pixel, for each color (RGB), flip the 8 bits from left to right.
     • Contact all new flipping data in one vector (1,C)
 End
End
L= length (vector (1,C))
```


Start
Select RGB Image
Read pixel data
i=1
i <=M
No
Yes
i=1
i=i +1
i <=N
No
Yes
For each pixel, for each color (RGB), flip the 8 bits from left to right
Contact all new flipping data in one vector (1,C)
j=j+1
L=length (vector (1,C))
End

Flowchart 1. Selecting image

2) Select Excel File: In this step, we will select the Excel file that we want to embed the encrypted data in. When the intended file is specified, it will be prepared to embed data. This step has two stages(psedo code : Select Excel File box):

a) Assign Header: Assign address cell (HMR500) as a header to imbedded information about the encrypted data that will be embedded later, involves its first cell name and number of the cell that will embedded in cover, which is randomly selected. Also, the number of bits of the encrypted data the header information is shown in Fig.11. Certainly, the selection of the first cell will be after the cell (HMR500) in order to ensure that no inclusion is made over the header information and this is done through (5), (6).

$$row = 10000 * riund\ (rond, 2) \qquad (5)$$

$$column = 10 * round(\ round, 1) \qquad (6)$$

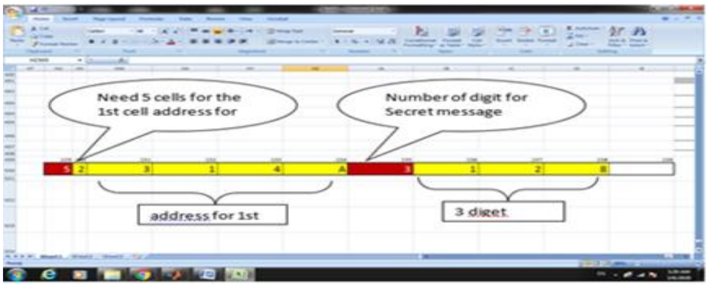
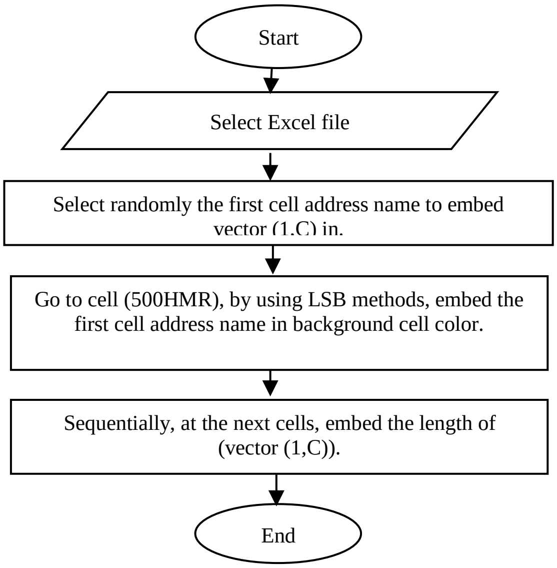

Need 5 cells for the 1st cell address for
Number of digit for Secret message
5
2
3
1
4
A
3
1
2
8
address for 1st
3 diget

Figure 11. Hidden process for the header information.

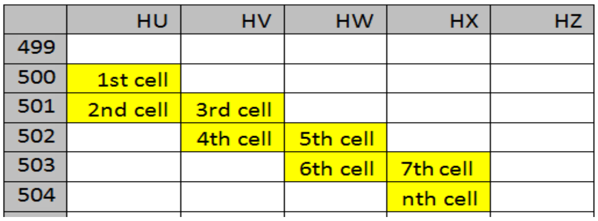
b) *Embed Header:* The second step of embed encoded data in the background color of Excel cells are explained in the next pseudo code and also in flowchart 2.


Start
Select Excel file
Select randomly the first cell address name to embed vector (1,C) in.
Go to cell (500HMR), by using LSB methods, embed the first cell address name in background cell color.
Sequentially, at the next cells, embed the length of (vector (1,C)).
End

Flowchart 2. Selecting MS-Excel File

```
Pseudo code: Select Excel file
• Choose the appropriate Excel file.
• Select randomly the first cell address name to embed vector (1,C) in.
• Go to cell (HMR 500), by using LSB algorithm; embed the first cell address name in background cell color.
• Sequentially, at the next cells, embed the length of (vector (1,C)).
```

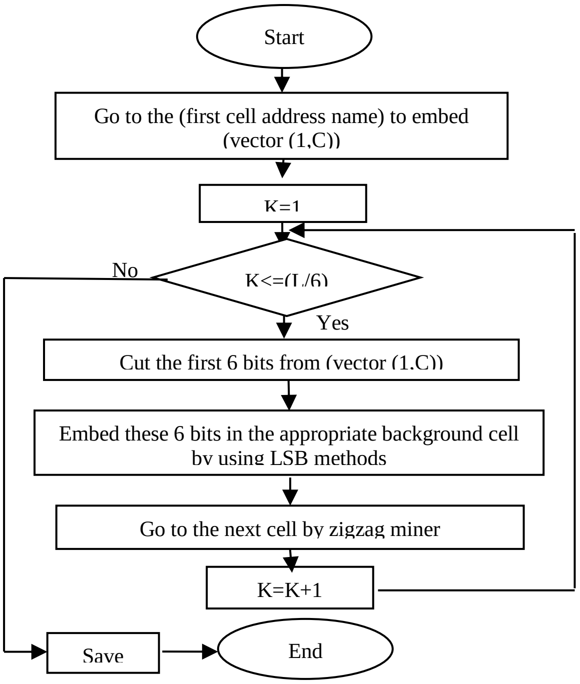
3) The Embedding and Saving Process: This process is done after preparing both encoded data and ground for embed. Every 6 bits of encoded data will be strip and embed in the background color of the cell via 2 bits per color in RGB color. The method that is applied for embed data is the least significant bit (LSB). The distribution of the bits on the cells will be in the manner of zigzag way, as shown in Fig 12.



	HU	HV	HW	HX	HZ
499					
500	1st cell				
501	2nd cell	3rd cell			
502		4th cell	5th cell		
503			6th cell	7th cell	
504				nth cell	

Figure 12. Manner of zigzag way.

The embed process steps are explained in the next pseudo code : Embedded Data Box and also in flowchart 3.


Start
Go to the (first cell address name) to embed (vector (1,C))
K=1
K<=(L/6)
No
Yes
Cut the first 6 bits from (vector (1,C))
Embed these 6 bits in the appropriate background cell by using LSB methods
Go to the next cell by zigzag miner
K=K+1
Save
End

Flowchart 3.Embedding Data

C. Extract data

It is the part where the image is retrieved through extracting the data that was embedded in the Excel file, as follows

```
Pseudo code: Embed data (Embedding and Saving Process)
To embed parts, go to the (first cell address name) to embed (vector (1,C))
For k= 1 to L/6
    • Cut the first 6 bits from front of (vector (1,C))
    • Embed these 6 bits in the appropriate background cell color by using LSB methods. Distribute 2 bits for each color (RGB)
    • Go to the next cell by zigzag way
End
```

Choosing the Excel file that contains the encrypted data, and through the information which is embedded in this file, we can extract the first cell name which is the starting point that contains the encrypted data. In addition, the number of bits through which we identify the last cell that contains the encrypted data.

After reaching the first cell that contains the encrypted data, we take the first 2 bits from each color R, G and B in background cell color to create the first 6 bits in a vector.

The process continues (N/6) times until reaching the last bit embedded in the cells provided that the transition from one cell to another is in the manner of zigzag in the same as a way of embedded previously. With each time, the new extracted data will join with the previous data that was extracted to create a vector (1 * N) as shown in the following figure.

10111001010010011000100110101001010011011001100110111001010110010000

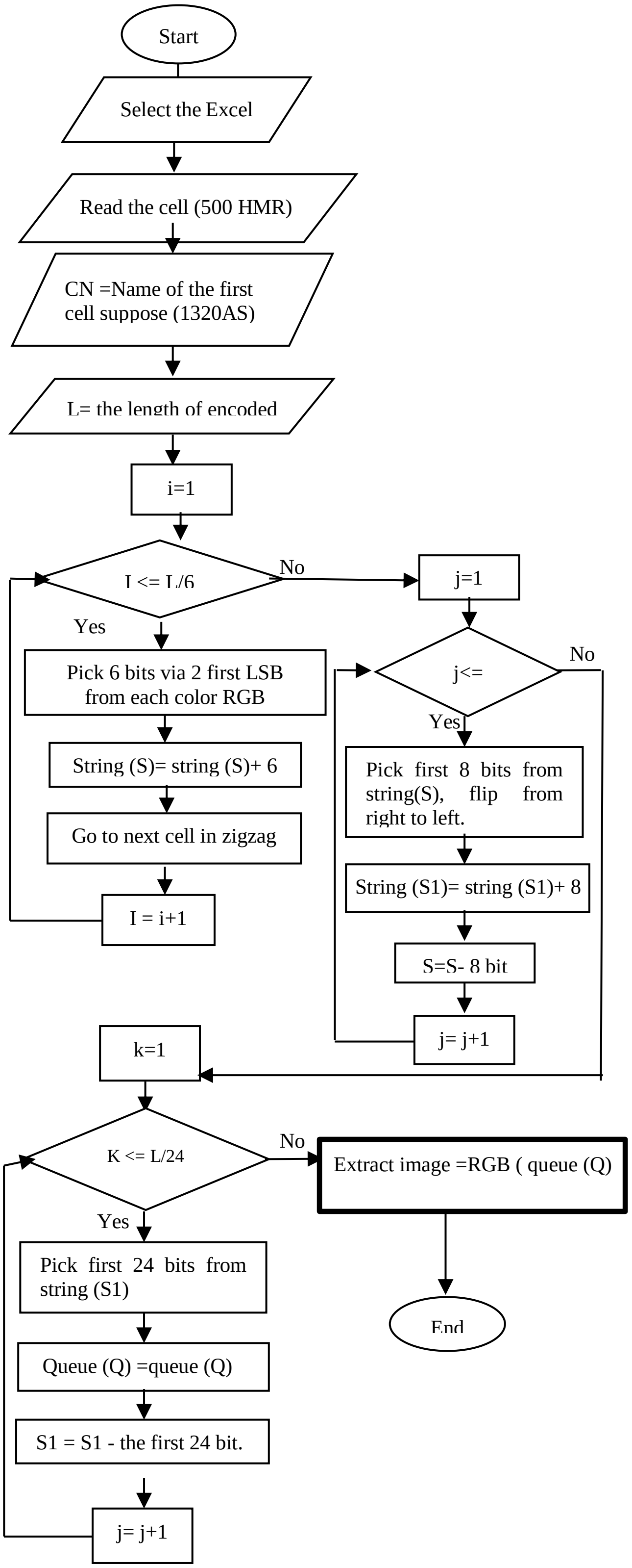
Then each 8-bit is cut separately to create a matrix (N/24, 3), for each row being a RGB pixel with 24-bit data.

Red	Green	Blue	
10111001	01001001	10001001	1 st pixel
10101001	01001101	10011001	2 nd pixel
10111001	01011001	00001011	3 rd pixel
00101011	11101001	01001001	N th pixel

Then it flips each 8 bits from right to left as shown below.

Red	**Green**	**Blue**	
10011101	10010010	10010001	1st pixel
10010101	10110010	10011001	2nd pixel
10011101	10011010	11010000	3rd pixel
11010100	10010111	10010010	Nth pixel

After this step, this data will convert to get the original image. The next pseudo code: Extract data Box and flowchart 4 are to explain the extracting data process.



Flowchart 4. Extracting Data

Pseudo code: Extract data

```
1) Select the Excel file that contains the encrypted data. Go to the
   cell (HMR 500)
    • Retrieve the name of the first cell in which the data was
      embedded, suppose (1320AS)
    • Sequentially, Retrieve from the next cells the length of encoded
      data (L) that was embedded.
2) Go to the first cell (1320AS) in order to start to retrieve the
encoded data.
    • For i =1 to L /6
        ✓ Pick 6 bits via 2 first LSB from each color RGB in one cell
        and gather it on the end of string (S).
        ✓ Go to next cell in zigzag way.
    • For j = 1 to L/8
        ✓ Pick first 8 bits from string(S), flip from right to left.
        ✓ Insert the 8 bit in end of new string S1.
        ✓ S = the rest of S except the first 8 bit. .
    • For k= 1 to L/24
        ✓ Pick first 24 bits from string (S1) and insert it in a queue
          (Q)
        ✓ S1 = the rest of S1 except the first 8 bit.
    • Convert the queue (Q) to RGB image.
```

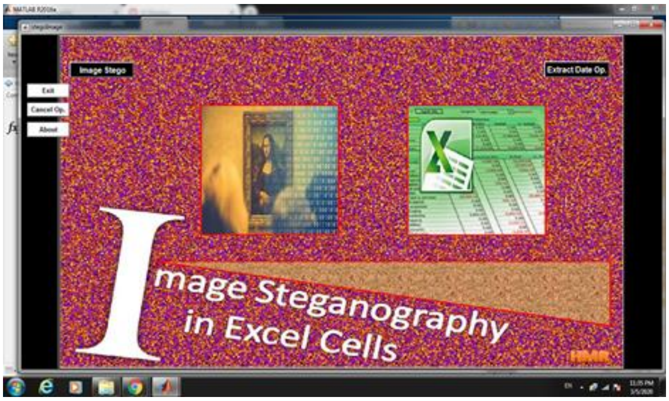


Figure 13. Overall Proposed System (U-IISA)

5. CONCLUSION AND FUTURE WORK

- As we know, the embedding process must have less than a third of the volume of data included to ensure that the host is not affected by the addition.
- Although the size of the Excel file (the host) is small compared to the size of the (added) image, the size of the Excel was not changed much.
- In the practical application of the program, a three-megabyte-sized image was hidden in an Excel file of 312 KB. We note that the Excel file, as the result of the process containing the image has become 320 KB. That is, the amount of change is very small.
- Image embedding speed depends on processor speed and image size to be hidden.
- There are two reasons explaining the novelty in this paper, the first of which is to hide an image of a very large size compared to the medium in which it is hidden, and the second is to hide an image in an Excel file.

Additionally as we mentioned in introduction section, the difficulty of retrieving the image of U=IISA is Encryption: the embedded data is encrypted in a complexed way. Masking method: the method of masking, which is embedded randomly in the Excel file, is very complicated. Embedding method: the method of embedding data is not serial, but in zigzag minor.

REFERENCES

[1] C . Rafael. Gonzalez & E .Richard. Woods, Addison-Wesley, “Digital Image Processing”, 2002.

[2] D. Vernon, “Machine Vision: Automated Visual Inspection and Robot Vision”, Prentice Hall, 1991.

[3] S. M. Klim, “SELECTED LEAST SIGNIFICANT BIT APPROACH FOR HIDING INFORMATION INSIDE COLOR IMAGE STEGANOGRAPHY BY USING MAGIC SQUARE”, Journal of Engineering and sustainable Development, Vol. 21, No.01, ISSN 2520-0917, Misan University-Engineering college, Misan, Iraq, January 2017.

[4] A. Khurana, 2B. Mohit Mehta, “Comparison of LSB and MSB based Image Steganography”, InternatIonal Journal of Computer SCIenCe and teChnology, IJCST Vol. 3, ISSue 3, July - SepT 2012, India.

[5]] P. Mcfedries, “Excel@ Formulas & Functions,” ISBN-13: 978-0-7897-5564-3 ISBN-10: 0-7897-5564-5, USA, 2016.

[6] K. Muhammad, J/ Ahmad, M. Sajjad, M. Zubair, “SECURE IMAGE STEGANOGRAPHY USING CRYPTOGRAPHY AND IMAGE TRANSPOSITION”, NED University Journal of Research 12.4 (2015): 81-91.

[7] Ch. Maiti*, D. Baksi, I. Zamider, P. Gorai, and D. R. Kisku,” Data Hiding in Images Using Some Efficient Steganography Techn.iques”. Signal Processing, Image Processing and Pattern Recognition. SIP 2011. Communications in Computer and Information Science, vol 260. Springer, Berlin, Heidelberg, (2011).

[8] O. M. Al-Shatanawi, and N. N. El. Emam,” A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION”, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015

[9] M.I.Khalil, “Image Steganography: Hiding Short Audio Messages Within Digital Images”, JCS&T - Journal of Computer Science and Technology, Vol. 11, No. 2, October 2011.

[10] H. I. Alsaadi, M.K. Alani, R.M. Almuttairi, O. Bayat, and O.N. UCAN, “Text Steganography in Font Color of MS Excel Sheet,” Association for Computing Machinery. ACM ISBN 978-1-4503-6536-9/18/1, Madrid, Spain © 2018.

[11] L.Y. Por, and B. Delina, “Information Hiding: A New Approach in Text Steganography,” 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008

[12] M.K. Alani, H. I. Alsaadi, R.M. Almuttairi, O. Bayat, and O. UCAN, “Conceal Existence of Encoded Data System (CEEDS)”, 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), DOI: 10.1109/3ICT. 8910278, Sakhier, Bahrain, Bahrain, 2019

[13] Md. Khairullah, “ A Novel Text Steganography System Using Font Color of the Invisible Characters in Microsoft Word Documents.” IEEE Computer Society Washington, DC, USA ©2009. ICCEE '09 Proceedings of the Second International Conference on Computer and Electrical Engineering-Volume 01, 2009.

Dr.Maad Kamal Al-anni is currently a staff member in the College of Engineering, Department of Computer Engineering, engaging also with World University Ranking as a mentor at Al-Iraqia University AIU and an establisher of Research Center called Dynamic Casual Model and brain study center at AIU, Ministry of Higher Education and Scientific Research, Iraq. Had a Ph.D Degree granted an Indian Council for Culture Relationship (ICCR) scholarship to complete Ph.D. research in University of Pune, India in Feb-2005 April, 2010, received Master’s Degree in Computer Science from University of Baghdad, Iraq in October, 2003, received Bachelor’s Degree in Computer Science, Iraq in October, 2001. In 2015 got post-doc’s Degree from Kazan Federal University KFU as Russian Scholarship and a Diploma in Russian Language from South Ural State University SUSU, 2014 Russia, holds an ILETS’ & TOFEL’ Certificates, had jointed visiting lecturers at Europe Universities, Lyon, France, 2014, Bournemouth University, UK, 2013, Strasbourg University, France, 2017, has been authoring several international conference papers in the area of grid computing, Artificial Neural Network, Intrusion Detection System, Data and Network Security, Fuzzy Sets, BigData, Cryptography, ConvNet, OCR, Datamining, DDK, Evolutional Algorithm (visit my Research Gate and Google Scholar with my profile name Maad Kamal Al-anni). During his working in MOH in Iraq has taught several subjects such as Cloud Computing, Distributed Systems, Networks, Operating System, Web based Applications and Data & Networking Security since Feb. 2004 for Undergraduate and Postgraduate students in Different Universities such as Baghdad University, Dyala University, Al-Rafidan University, Al-iraqia University, and Al-Mansour University. Her current research interest is in the area of data grid architecture and fuzzy decision making for grid resources and replica election & enhancing Intrusion Detection systems to search for hidden attack patterns using Hadoop frameworks, and analyzing bigdata with Distributed system to deal with signal and image processing datasets, has several International Published Articles in ISI, SCI, SCOPUS, IEEE, SPRINGER, Digital Open Science Index, Semantic Scholar, Zenedo, OpenAIRE, BASE, WorldCAT, Sherpa/RoMEO, has several International Conferences’ Papers in Preceding’s releases, Association Computer Machinery, and Open Digital Library, is a supervisor of post-graduate students in Msc and Ph.D.

Rafah M. Almuttairi is currently works as a Director of Studies and Planning Department at Ministry of Higher Education and Scientific Research, University of Babylon, Babylon, Iraq. She has completed her Ph.D. research in University of Hyderabad, India in April, 2012. She received her Master's Degree in Computer Science from University of Baghdad, Iraq in October, 2003. She received her Bachelor's Degree in Computer Science and Bachelor Degree in Physics from University of Babylon, Iraq in October, 2001 and October 1994 respectively. In 2007 she has got a Diploma in Arabic-English translation from Osmaina University, Hayderabad, India. She has authored several international conference papers in the area of grid computing. During her working in MOH in Iraq.

Husam Ibrahiem Husain Alsaadi received the B.Sc. degree in information system computer science from Al-Rafdain University College, Baghdad, Iraq in 2000. He received the M.Sc. degrees in computer science from Baghdad University, Iraq, 2004. He is currently pursuing the Ph.D. degree in the Department of Electronic and Computer Engineering, Altinbas University. His research interests in the data mining, machine learning and data hidden.

Husam Ibrahiem Husain Alsaadi received the B.Sc. degree in information system computer science from Al-Rafdain University College, Baghdad, Iraq in 2000. He received the M.Sc. degrees in computer science from Baghdad University, Iraq, 2004. He is currently pursuing the Ph.D. degree in the Department of Electronic and Computer Engineering, Altinbas University. His research interests in the data mining, machine learning and data hidden.