International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 4, April-2014, pp: (542-548), Impact Factor: 1.252, Available online at: www.erpublications.com

Offensive Algorithm for Hiding and Extracting Information Using Image Steganography

Vandana Yadav[1], Amandeep[2], Neeraj Rai[3]
[12]M.Tech Computer Science & Engineering, Galgotia University, Gr. Noida, UP, India
[3]M.Tech Automation & Robotics, Ajay Kumar Garg Engineering College, Ghaziabad, UP, India

Abstract: In this paper we will study the various image based steganographic techniques for information hiding, analyze the problem in them and will propose a novel steganographic algorithm namely 'An offensive algorithm for hiding and extracting information using Image Steganography' for hiding information within the spatial domain of 24-bit color image and as well as extracting it. The motivation for this work includes provision of protection of information during transmission without any detection of information. The proposed technique is implemented in MATLAB 7.5 and is compared with tri-way PVD technique based on the PSNR value for different information images. It is found that the proposed technique is better than the existing technique. Though the proposed technique is better, it still has the scope for improvement. In future we can combine the proposed algorithm with some cryptographic technique in-order to make it more powerful. And also we can take it to the transform domain instead of spatial domain.

Keywords: Information hiding, information security, image steganography, image cryptography, cover image, PSNR.

1. INTRODUCTION

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are being used frequently interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures. The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization including: securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc. Three basic principles of information security are there: Confidentiality, Integrity and Availability. Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. In information security, integrity means that data cannot be modified without authorization. The information must be available when it is needed for any information system to serve its purpose.

1.1. Steganography and Information Hiding

Information hiding is a method of hiding secret messages into a cover-media such that an unintended observer cannot know the existence of the hidden messages. Steganography is the practice of hiding secret message within any media. Steganography is basically the art of writing hidden messages in such a way that no one other than the sender and authorized recipient knows the existence of the message. As defined by Cachin [1], steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. This is basically the form of security through obscurity [2]. The word steganography comes from Greek word "steganos" meaning "covered" and the "graphy" means "writing". Thus, steganography literally means "covered writing". Moreover, it has taken some meaning from the dinosaur called the Stegosaurus. Stegasaurus was an ancient creature that had the unique feature of being covered by a series of vertical plates along its spine, hence the "Stego" part in its name.

Steganography is a very old method of passing messages in secret. This method of message cloaking goes back to the time of the ancient Greeks. The historian Herodotus [3] has written about how an agent wrote a message warning of an invasion on the wood part of a wax tablet. Since, messages were normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer.

Steganography is: "Hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message". It can be used to cloak hidden messages in image, audio and even text files. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic

format new techniques for information hiding have become possible. Steganography can be described by the following formulae:

Cover media + embedded message + stegokey = Stegomedia

2. PROBLEM IDENTIFICATION

In the present scenario the communication of the multimedia data has increased to a large extent. With this increase of multimedia communication the security of these data becomes important; as because there is the huge rise of World Wide Web. And as we know that the internet users frequently need to store, send, or receive data and information, this calls up for the creation of methods to protect these digital information against unauthorized access and manipulation there is a need to have a solution, so as to pass information in a manner that the very existence of the message is unknown to third person or attacker in order to repel attention of the potential attacker. Steganography is one of the possible solutions for such types of problems. Among various types of steganographic techniques, image steganography is best solution.

3. RELATED WORK

In this paper we have briefly discussed about some of the most popular and widely used image based steganographic techniques:

A. LSB Technique

LSB is a simple approach to embed -ding information in an image [4]. Applying LSB technique to each byte of a 24-bit image, three bits can be encoded into each pixel, as each pixel is represented by three bytes. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte. For example, if we use 8-bit image to hide the letter A (has the binary value 01000001), we need eight pixels. Suppose the original eight pixels are:

(00100111) (11101001) (11001000) (00100111) (11001000) (11101001) (11001000) (00100111)

Inserting the letter A (as a binary value) into these eight pixels will give the following (starting from left side):

(00100111) (11101001) (11001000) (00100111) (11001000) (11101000) (11001000) (00100111)

Only the emphasized bits are changed. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image. Common images, like the Mona Lisa painting, should be avoided.

B. PVD Technique

This method [5] is mainly based on the principle of that human eyes are most sensitive to smooth area and least sensitive to the edge areas of an image i.e. the degree of distortion tolerance of an edge area is naturally higher than that of a smooth area. On the basis of this principle, more data bits are embedded in the smooth areas of an image. Actually, the determination of edge or smooth areas is dependent on the difference between two consecutive pixel values. In case of smooth areas, the values of the pixels are very close to each other. On the other hand, the pixels in the edge areas differ from their neighboring pixels by a large amount. Therefore, by checking the difference between two consecutive pixel values smooth or edge area of an image are determined in this technique. Actually, secret data bits are embedded in the image by modifying the difference between two consecutive pixel values.
In this technique, the entire cover image is divided into a number of 2 X 1 non-overlapping blocks. The difference between two consecutive pixel values of each 2 X 1 block is calculated and is checked in which range in the following range table the difference actually falls.

Table 1: Range Table

Range	Difference within the Range	Range Length
R1	From 0 to 7	8
R2	From 8 to 15	8
R3	From 16 to 31	16
R4	From 32 to 63	32
R5	From 64 to 127	64
R6	From 128 to 255	128

Then the length of the range is found. If the range length is L, then log2L number of bits is embedded and the decimal value of the embedded bits is calculated. The calculated decimal value is then added to the lower bound of the range to find the new difference. After this, the two pixel values are modified in such a way that the difference between these two pixel values is equal to the new difference. Similarly, during the extraction phase, the difference between two consecutive pixel values is calculated and the range of that difference is found. Depending on the length of the range, hidden data bits are extracted.

C. Tri-Way PVD Technique

This method is actually an improvement of the PVD method in terms of hiding capacity [6] [7]. In PVD method only one direction is referenced whereas, in this method three directional edges i.e. horizontal, vertical and diagonal edges are taken into consideration in order to hide the secret data bits. At first, the entire cover image is divided into a number of non-overlapping 2 X 2 blocks. Three pixel pairs of each block are used for embedding purpose. The pixel pair that is taken into consideration is in the horizontal, vertical and diagonal directions. Data bits are embedded on the basis of the difference between the two pixel values of each pixel pair. The last row of blocks of the cover is reserved for storing the number of pixel-pairs used for embedding purpose. In case of color image, the pixel value is taken as the value of the blue component i.e. in other words; the difference between the blue channel values of two pixels of each pixel pair is used to embed the data bits. Actually, the pixel located in the first column of first row of each 2 X2 block is taken as the first pixel of each pixel-pair. During embedding operation, each of the three pixel pairs of each 2 X2 block is modified based on the difference value of each pixel pair. After this modification, the optimal pixel pair is found depending on some calculation. After determining the optimal pixel pair, the pixel value of the first pixel of the optimal pixel pair is taken as the pixel value of the pixel located in the first column in the first row of the 2 X 2 block under consideration. Based on the optimal pixel pair, the other two pixel pairs are modified so that the pixel values of the first pixel of those pairs become equal to the pixel value of the first pixel of the optimal pair. The extraction process is same as that of PVD method except that the differences between the pixel values of three pixel pairs of each 2 X 2 block are checked instead of only one pixel pair in one direction.

D. Gutub's Pixel Indicator Technique

The pixel indicator technique uses the least two significant bits of one of the channel from Red, Green and Blue as an indicator for existence of data in the other two channels [8] [9]. The indicator channels are chosen in sequence, with Red being the first. The following table 2 shows the relation between the indicator bits and the amount of hidden data stored in the other.

Table 2: Relation between indicator bits and amount of hidden data

Indicator Bits	Channel 1	Channel 2
00	No Hidden Data	No Hidden Data
01	No Hidden Data	2 bits of Hidden Data
10	2 bits of Hidden Data	No Hidden Data
11	2 bits of Hidden Data	2 bits of Hidden Data

The disadvantage of the algorithm is that the capacity depends on the indicator bits and based on the cover image, the capacity can be very low. Also, the algorithm uses fixed number of bits per channel (2 bits) to store data and the image may get distorted if more bits are used per channel.

4. PROPOSED ALGORITHM

The proposed algorithm takes two inputs, one is 24-bit color image as cover and the other is the information to be hidden, which may be text in form of image as well as image too. Our algorithm works under the spatial domain. In this the hidden information can be extracted from the stego-image without the help of the cover image. Though the hidden data is extracted the cover image cannot be recovered.

A. Algorithm for Hiding Information

Step 1) Load the first input i.e. 24-bit color image as cover.
Step 2) Load the information to be hidden.
Step 3) Consider the R, G and B channels of the pixels of cover image starting from the first pixel to the maximum of the end pixel in-order to hide the information in the cover image, i.e. only the requisite number of pixels are needed from the cover image which can hide the information.

Step 4) Calculate number of 1's and number of 0's in the R-channel of each pixel.
Step 5) Calculate the absolute difference value of number of 1's and 0's in R-channel.
Step 6) Divide the difference obtained by the number of channels which is to be embedded in a pixel. For 24-bit color image it is always 2.
Step 7) Now, the resultant number of bits of the embedding size is to be embedded till a specified number of pixels and then data is to be embedded on the LSB (up to 3rd bit position) part of the Green and Blue bytes of each pixel of the cover image where the Red channel will act as an indicator.
Step 8) Finally, the stego image is produced which contains the hidden information.

B. Algorithm for Extracting Information

Step 1) Load the stego-image from which the information is to be extracted.
Step 2) Consider all the three color channels R, G and B of all pixels starting from the first pixel to the end pixel of the stego-image.
Step 3) Calculate the number of 1's and 0's in the R-channel of each pixel.
Step 4) Calculate the absolute difference of the number of 1's and 0's in the R-channel of each pixel.
Step 5) Divide the obtained difference value by 2 (number of channels to be embedded in a pixel, for 24-bit color image it is 2).
Step 6) The obtained value is the number of bits to be extracted from the stego-image by traversing the specified number of pixels depending on the size of the hidden information. The requisite information is to be extracted from the LSB part of the G and B channel of each pixel of the stego-image.
Step 7) Finally, the hidden information is extracted from the stego-image.

5. IMPLEMENTATION AND RESULT ANALYSIS

The proposed algorithm is implemented in MATLAB 7.5. We have taken several example figures for the purpose of analysis. We are presenting one of the examples here in this paper for better understanding of the algorithm.

We have taken the standard *Lena.bmp* image as the **cover image** and one written information in form of image i.e. *information.bmp* as the **information to be hidden**. The cover image is shown in fig.1, histogram of the cover image is shown in fig.2., message to be hidden is shown in fig.3., histogram of the message to be hidden is shown in fig.4., steganographic image is shown in fig.5., histogram of the steganographic image is shown in fig.6., extracted information is shown in fig.7., and the histogram of the extracted image is shown in fig.8.

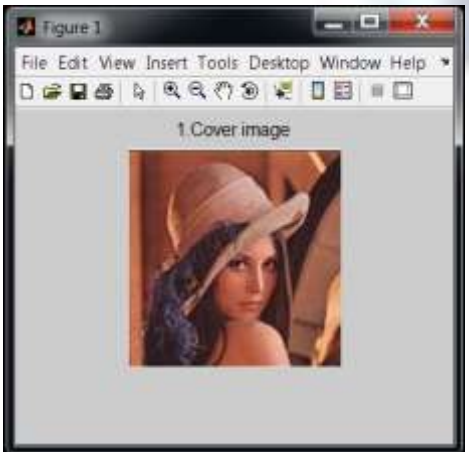

Fig.1. Cover image

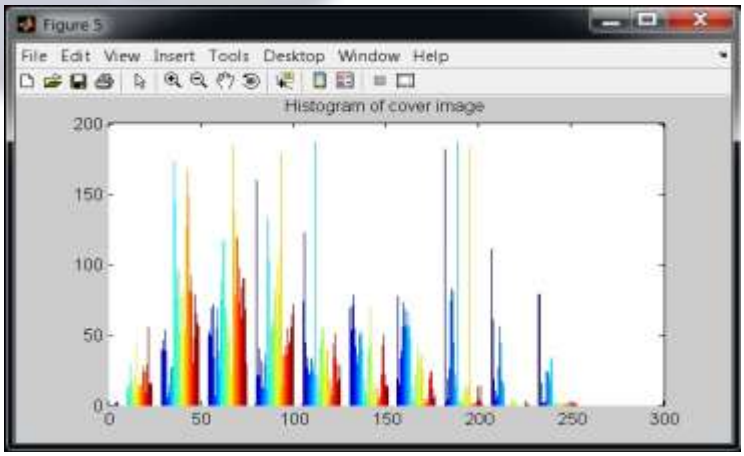

Fig.2. Histogram of the cover image

Fig.3. Message to be hidden

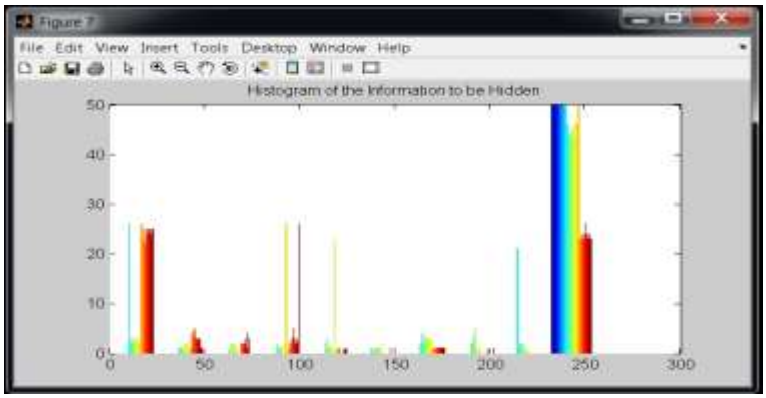

Fig.4. Histogram of the message to be hidden

Fig.5. Steganographic image

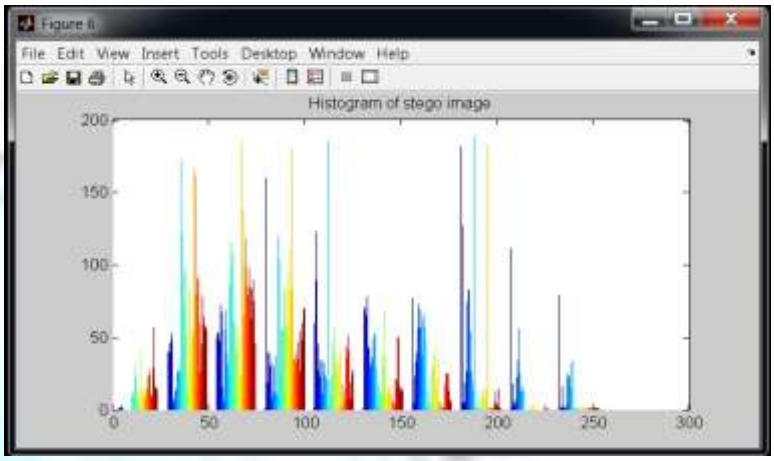

Fig.6. Histogram of the Steganographic image

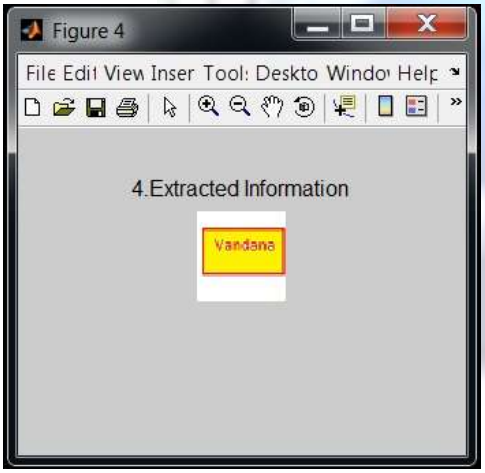

Fig.7. Extracted information

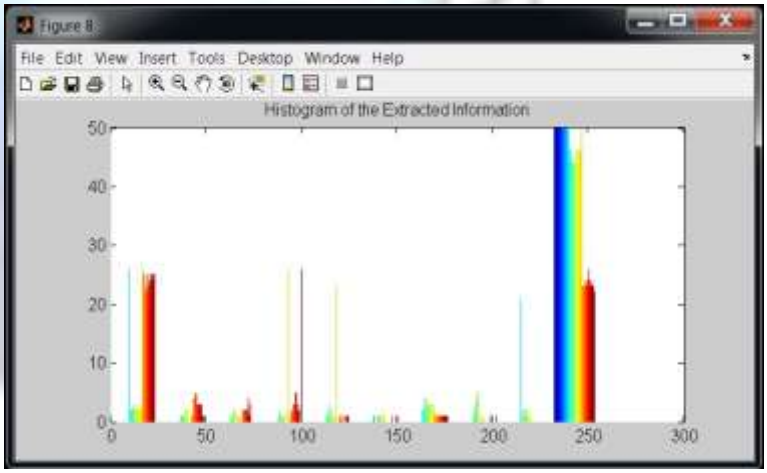

Fig.8. Histogram of the extracted information

In order to analyze the quality of the images we have calculated the PSNR (Peak Signal-to-Noise Ratio) values of the images. PSNR value is basically the ratio between the maximum power signal and the power of the corrupting noise. Mostly, PSNR value is expressed in terms of logarithmic dB scale, as because many of the signals have very wide dynamic range. It is found by rigorous experiment that if the PSNR value for stego-image is greater than 45 then it is considered to be of good quality. PSNR is calculated with the following formulae:

$$PSNR = 10 * \log_{10}\left(\frac{(MAX_i)^2}{MSE}\right)$$

Where, MAX_i is the maximum possible pixel value of the image. MSE is the **mean squared error.** It represents the cumulative squared error between the distorted and the original image. Lower the value of MSE, the lower the error. It is calculated with the following formulae:

$$MSE = \frac{\sum_{m,n}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

where, *M* and *N* are the number of rows and columns in the input images, respectively.

In the above example, we have calculated the PSNR which comes out to be: **53.4358 dB**, which is considered as good quality image. We have compared our proposed algorithm with one of the existing technique i.e. Tri-way PVD technique based on the PSNR value for different information images of same size. The comparison is shown in table 3 and in fig.9.

Table 3: Comparison between Proposed technique and Tri-way PVD technique

Information images (50X50 pixel)	Tri-Way PVD Technique (PSNR in dB)	Proposed Technique (PSNR in dB)
I_1	44.20	55.08
I_2	41.23	52.54
I_3	33.07	55.81
I_4	46.22	56.50
I_5	48.94	56.92
I_6	58.85	56.95
I_7	47.19	53.91
I_8	48.27	49.61
I_9	47.02	57.02
I_{10}	55.60	56.33
I_{11}	43.70	46.14
I_{12}	38.78	53.52

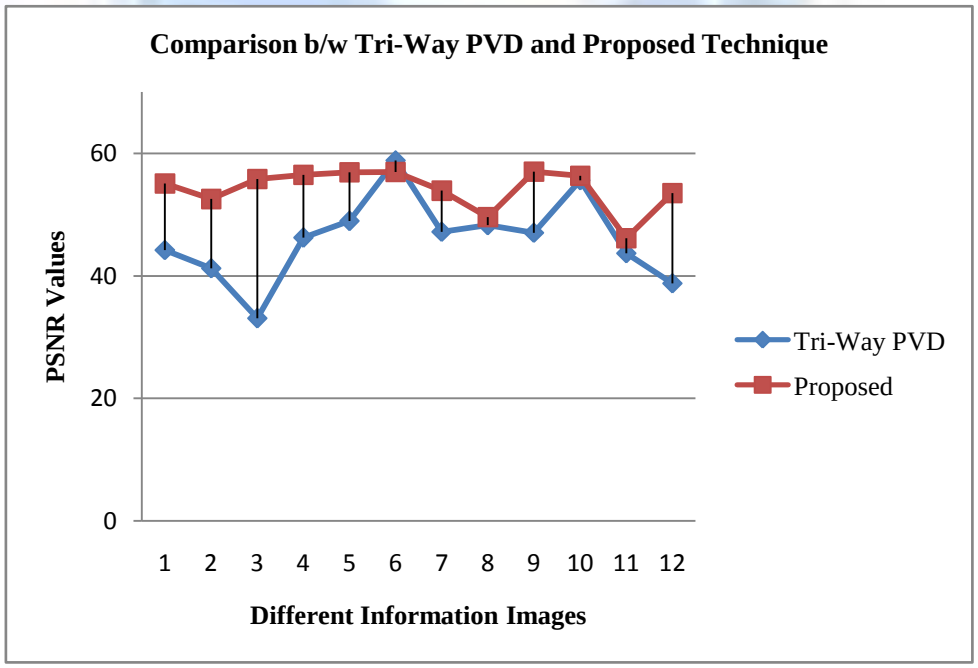

Fig.9:. Comparison between Tri-Way PVD and Proposed Technique

From the above table and the graph we found that the proposed technique is better than the Tri-Way PVD technique.

CONCLUSION & FUTURE SCOPE

In this paper we have studied different image based steganographic techniques for hiding information, and proposed a novel algorithm for the same. The proposed algorithm has two parts, in the first part we hide the information and in the second part the hidden information is extracted. We have implemented the proposed technique in MATLAB 7.5 for several example images. One example is presented in this paper. For the purpose of the quality, we have calculated the PSNR value, for the presented example it is found to be 53.4358 dB. We have also compared the proposed algorithm with one existing algorithm i.e. Tri-Way PVD technique based on the PSNR value for different information images. The comparison is shown in table 3 and fig.9. It is found that our proposed algorithm is better than the existing technique. The proposed approach has various advantages as compared to the other methodology mentioned in the paper. The advantages are:

- Proposed algorithm is a blind approach in spatial domain.
- The quality of the stego-images is highly acceptable by the human eyes which are measured in terms of PSNR values.

Though there are some advantages, some disadvantages are also there. We know the data hiding capacity is higher in spatial domain than transform domain steganography. But, in transform domain, we can do make some transformation without losing the hidden data which is not possible in spatial domain. So, the cover media is much robust in transform domain steganography. Also, we believe that steganography when combined with encryption provides a secure means of secret communications in between two parties. So, it can be improved by combining this approach with a novel encryption algorithm to enhance the security of the hidden data. Moreover, if hiding capacity of the cover image creates the major role then we can use some other steganographic method whose data hiding capacity will be higher than our proposed method.

REFERENCES

[1] Cachin, “An Information-Theoretic Model for Steganography”, In Proceedings nd of 2 Workshops on Information Hiding, MIT Laboratory for Computer Science, May 1998.

[2] Jayaram P, Ranganatha H R, Anupama H S ―INFORMATION HIDING USING AUDIO STEGNOGRAPHY – A SURVEY‖, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[3] Herodotus, “The Histories, chap. 5 - The Fifth Book Entitled Terpsichore, 7 - The Seventh Book Entitled Polymnia”, J. M. Dent & Sons, Ltd, 1992.

[4] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, “An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding”, International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.

[5] C. Wu and W. H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, 24(9-10), pp.1613–1626, 2003.

[6] Chang, Ko-Chin, et al. "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing." Journal of multimedia 3.2 (2008).

[7] Sherly, A. P., and P. P. Amritha. "A Compressed Video Steganography using TPVD." International Journal of Database Management Systems 2.3 (2010).

[8] Gutub, Adnan, et al. "Pixel indicator high capacity technique for RGB image based Steganography." WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications. 2008.

[9] Gutub, Adnan Abdul-Aziz. "Pixel indicator technique for RGB image steganography." Journal of Emerging Technologies in Web Intelligence 2.1 (2010): 56-64.