DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4241

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A REVIEW: ENHANCED STEGANOGRAPHY TECHNIQUE FOR 2D BARCODE IMAGES

Priya Sidhu
Department of Computer Engineering,
UCoE, Punjabi University,
Patiala, India

Gaurav Deep
Department of Computer Engineering,
UCoE, Punjabi University,
Patiala, India

Abstract: Digital Steganography is a procedure of concealing key messages in a cover media while transmission happens between sender and receiver. Security of secret information has by and large been a vital matter from days passed by occasions to the present time [9]. The main merit of image steganography is that the message is encoded inside the image without any recognition to human eye or system of an attacker. Techniques for image steganography focuses on securing the transparency of the information that is hidden inside an image while ciphering. This paper includes a new method for LSB (Least Significant Bit) based image steganography for 2D barcode images. The main aspects of encoding data look over to develop an improved LSB encoding method [1].

Keywords: Steganography, Process, Methodology, Barcode, Steganography Techniques

INTRODUCTION

The advancement in technologies as Internet enabled the transmission of large amount of data in quite less time. One of the important steps in transmission of data is security against unauthorized access. Thus, Steganography is one among security techniques that refines the security of data that is being transmitted [1]. The word Steganography means "included writing" from Greek. In Steganography, it offers secrecy of text or images to avoid them from attackers [7]. A stego-key that is the key that is beneficial and helps the data to be concealed inside the cover image, and the steganography algorithm helps to cart the stego-object is carted by the ciphering algorithm. The resultant output holds the secret message, is stego-image and it is dispatched to the legatee's device gets the dispatched stego-image to recover the data from the image by utilizing of the desteganography [14].

Image is a collection of information that can be sent anywhere for giving any relevant information, and is also used in hiding information that is growing an important for information security. The least significant bit (LSB) embedding algorithm is a basic algorithm, and helps to do the fast encryption of the data in an easy way to conceal the large amount of data, while it is one of the most known algorithm in the area of concealing data [3].

PROCESS

- **Message / Transformed Message:** The message is information which helps to be hidden into some feasible digital media and convert to un-readable form that is Transformed Message.
- **Cover Media:** It is the carrier of message such as image, audio, video or other digital media.
- **Stego Key:** It is utilized to embed message considering upon the encrypting algorithm. Embedding algorithm is the technique for installing the mystery message into the cover image.
- **Ciphering:** The part in which encoder encodes the message into the digital media.
- **Deciphering:** The part in which legatee decodes the modified message from the digital media [5][7].

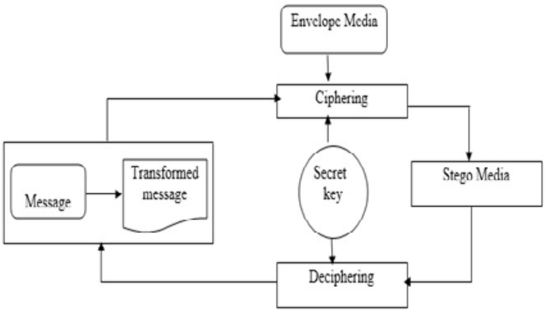

Fig 1: Overview of The Proposed System [5]

Steganography allows to change digital carriers such as text, images, audio, video, or protocol, the modifications are for the hidden message, but there should be invisibility in change to the channel. In steganography, the sender should select feasible message channel before concealing the data, the concealed message, and the secret key also, and steganography algorithms that should be able to cipher the text more efficiently. On the other side, after getting the text the legatee decrypts the concealed data using the deciphering algorithm and a secret key [2].

STEGANOGRAPHY TECHNIQUES

Steganography techniques are the techniques that help to hide the data with full security without any obstacles to the legatee while receiving the data that is vital and to be transparent to the attackers. Classification of stenography techniques on the basis of the cover modifications used in the embedding process is as follows:

- **Spatial Domain Techniques:** Spatial steganography has different types that are expert in changing some bits of image pixel values for hiding data. Least significant bit (LSB) based steganography is the basic technique that to conceal the secret message data of pixel values' LSBs without introducing many perceptible twists. Spatial steganography has many varieties, changing some of the bits in the pixel value of the image to conceal the data. Changes in the value of the LSB are invisible for human eyes [16].

- **Transform Domain Techniques:** This technique implants key information in the recurrence area of the sign. Change space strategies shroud messages in critical zones of the cover image improving them made to issues in contrast with LSB approach.
- **Masking and Filtering:** These techniques marks an image to hide the information same as for paper watermarks. These methods prefer to secure them in more relevant areas rather than encoding the information in the noisy areas. The obscured message is more integral to the cover image.
- **Distortion Techniques:** In this method, the learning of novel spread in the interpreting procedure is key at the beneficiary side. This methodology the distinctions with the principal spread keeping in mind that the end goal is to remake the gathering of alteration utilized by sender. This modification is to recognize the secret message after been received by the legatee. The pseudo-randomly chosen pixels are used to cipher the message [16].

MAGIC PENTAGON OF STEGANOGRAPHY

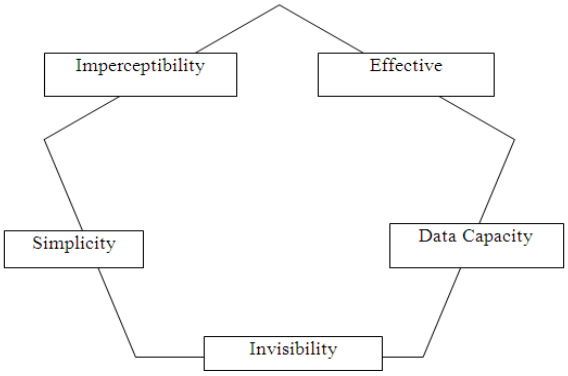

Fig.2 Magic Pentagon of Steganography

Magic Pentagon of Steganography are as following aspects [4]:

1. **Imperceptibility:** The difference between stego image and input image should be out of view from the mysterious attacker, can't recognize secret data. If, the lot of data is concealed in the image then it will bring about weakening of stego-image.
2. **Effective:** Stego-image does not to be changed regardless of the possibility that it experiences change, sharping, separating, running, obscuring, trimming and other adjustment and so on.
3. **Simplicity of recognition and extraction:** For unauthorized users who do not have a key, it should be extremely a big obstacle to reveal its information and might be simply deciphered by receiver.
4. **Data capacity:** The watermarked image must figure out how to take huge amount of data without loading the course or the underlying image. That property recognizes the amount of data must be implanted for right carriage [16].
5. **Invisibility:** The information is undetectable to people in general and no one can get to the mystery information without authorization of sender. The perceptual quality would be decreased in stego-image as compared to cover image [5].

IMAGE STEGANOGRAPHY

The main technique for concealing key information is used in the images. An image is a concoction of the so many pixels that contain different color intensities. In images, you can discover different sort of record configurations are way out. We can conceal the cover subject in the cover media which is main and primary source; text, images, sound, motion picture(video) and so on. The cover image size is always dependably bigger than the size of stego image and output of encoded image is called stego-image. With the assistance of PSNR we can calculate the comparison between the noise present in the cover image and the stego image. PSNR is an effective characterized by means of the mean squared error (MSE).

The PSNR is labelled as:

$$PSNR= 10\ \frac{LOG10(\ R2\ )}{MSE}$$

If, PSNR has maximum value then it demonstrates that image has better quality that is it has lower value of distortion. The possibility of visible attack by human eye will only be lesser if PSNR value is also very high [7].

DATA HIDING IN 2D BARCODE

A barcode can be mounted on the side mirror of vehicle and barcode reader scans that barcode and then it checks that the user and vehicle is registered or not. A barcode is a series of parallel black bars and white spaces, both of varying widths. Different combinations of the bars and spaces represent different characters, such as numbers or letters. Each combination or sequence of bars and spaces is a code that can be translated into information related to the vehicle. A barcode reader is required to read a barcode. Barcode readers may be fixed, portable batch, or portable RF. The barcode simply provides a reference number that tells a computer to access information [9].

Table 1. Comparison between Barcodes

S.No.	Features	1D Barcode	2D Barcode	3D Barcode
1	Introduced in	1974	1988	1994
2	Design	Zebra–stripped	Square	Embossed
3	Type of data	Numeric	Alpha numeric	Alpha numeric
4	Storage Capacity	25-30 characters	up to 1800 letters	Maximum capacity
5	Stored in form	Linear	Horizontally, vertically	Horizontally, vertically
6	Temperature	No Change	No Change	Shape changes
7	Purpose	Prints cost price	Read and write	Stores maximum data

8	Error correction	No error correction	Corrects upto 30%	Self-correcting

2D Barcode

Since last couple of years, two-dimensional (2D) barcode have picked up the consideration of the general population from the mechanical foundations and bit by bit supplanted one dimensional standardized tags in numerous projects on account of their higher data stockpiling limit. QR code is subsequently as a data compartment which can be gotten and decoded by brilliant phones straightforwardly. Network scanner tag containing a ton more amount of data than their 1D form an ordinary QR code is only a highly contrasting pixilated box. Encoded data may incorporate simple content, work of art, or direct clients to a site or greeting page for extra data. Moreover, Barcode innovation is predominant in rate, stead quickness, data volume, and expense. The information in the code could be ensured, which needs extraordinary programming to unravel and interpret, which guarantee more prominent security [8].

Quick Response barcode is a two-dimensional scanner tag with high information thickness, mistake remedy capacity and simple security instrument. Amid, the beginning of the QR codes, the reason was to make utilization of the snappy association with the particular website page with the URL data changed over to the QR code design. However, nowadays they remain as information compartments that give more security when encoded following from the perspective of information covering up examines, QR code should then be viewed as the undeniable watermarks. The aforementioned is the motivation behind why we utilize QR code as an information holder and scramble it in our arranged application [11].

LITERATURE SURVEY

- Sherin Sugathan et al. [2016][1], presented in this paper a simple LSB replacement algorithm that will help in improving the quality of a stego-image. In this paper, result also indicates that the proposed algorithm is good especially while encrypting the secret data at higher LSB bit positions.
- Hilal Almara’beh, et al. [2016][2], presented that Audio and Video Steganography is one of the most useful and secured form of steganography. With the rise of computer technologies and internet, the protection of information has become most challenging. This paper presents a standard view of steganography, effective steganographic methods PNSR, MSE, SNR, MD, etc. and different techniques that are LSB, DCT, DWT, phase coding, and echo hiding used in audio and video steganography. The different techniques help to improve the security in steganography.
- Xinyi Zhou et al. [2016][3], proposed a method for cryptography that is combined with LSB based Color Image steganography to refine the encryption technology for improving the security od the hidden data, improving human eye visual features ad image authentication. This paper results in finding that no change in visual characteristics of cover image, unauthorized cannot find the location of hidden data and security also increase of information hiding.
- Sumeet Kaur et al. [2015][5], presents the classifications of different image steganography techniques, features and comparison of steganography techniques. This paper concludes with the uncompressed file formats that can easily hide data or not. It also focuses on complete study of different techniques and strategies.
- Pritam Kumari et al. [2013][6], describes about the actual meaning, background , methods and comparison of the steganography technique. Also, about the comparison among cryptography and steganography.
- Gagandeep Kaur et al. [2015][7], presents the meaning of steganography, techniques and types of steganography. The proposed method for blending hidden data into an image without disturbance. The modification becomes obstacle for the unauthorized users to find the changes done to stego-image and also helps to secure the data from illegal user.
- Priyanka Gaur et. al. [2014][8], presents in this paper about barcodes; its definition, types, proposed method to read the barcodes and different operations applied to barcodes. The recognition and segmentation of barcodes with different methods and mathematical calculations.
- Praveen T. et. al. [2013][9], proposed a technique for securing the high capacity of data in Barcodes using Chaos Based Feedback Stream as data is been encrypted in barcodes, that helps to increase the efficiency.
- Sharu Goel et. al. [2014][11], presents about the barcode, its types:1D barcode, 2D barcode, 3D barcode; also, about the encryption technique that is used to encrypt huge amount of data in Barcodes.

  This paper includes the advantages of barcodes in today’s era and distinguishes how barcode is created and data is embedded into it.
- D. Antony Praveen Kumar et. al. [2016][12], proposed the LSB technique to improve both image security and image quality that is least significant bit(LSB). In this paper, we conclude that the proposed system was generated to message transmission effectively in Least Significance Bit method and QR code pattern image to inprove the security. Finally, the result tells that it is used to improve the performance level of the system as compared to existing methodology.
- Anil Khurana et. al. [2012][15], presented this paper about Least significant bit (LSB)and Most significant bit steganography comparison in the images that is either Greyscale or RGB. LSB based steganography is used to encodes the text message in LSB of the pixels of cover image whereas MSB based steganography encodes the text message in MSB of pixels of cover image. This paper compares the results of LSB based steganography and MSB based steganography by calculating Mean square error.
- Mehdi Hussain et. al. [2013][16], presents the exponential growth, the communication of system users over the internet and the different steganographic techniques. In this paper, it was analyzed that image degrades when hidden data capacity in increased more than limit in LSB technique.

METHODOLOGY

The 2D barcode image is taken as cover image to hide the information. The first code is fragmented, to conceal the information, into smaller parts, where smaller part is chosen by applying edge detection clustering and then the bit will be encrypted in Region of Interest and that can be made by applying Least Significant Bit Algorithm. The information in each part is the bit of encoded into 2D barcode image relating to that bit of information [6].

At sender side:

The main steps that are required to hide data by using this technique are as follows [3]:

Step 1: Select the 2D Barcode image.

Step 2: Create the color table from the image.

Step 3: Generate the clusters of all the colors.

Step 4: Expand the clusters by measuring the mid-points and which of the cluster is nearest to other cluster's mid-point make them as single cluster [12].

Step 5: The secret data is converted to binary form using ASCII format and then encoded inside the pixel.

Step 6: Apply LSB to the expanded cluster in which data is to be concealed.

Step 7: Stego 2D Barcode image is obtained [15].

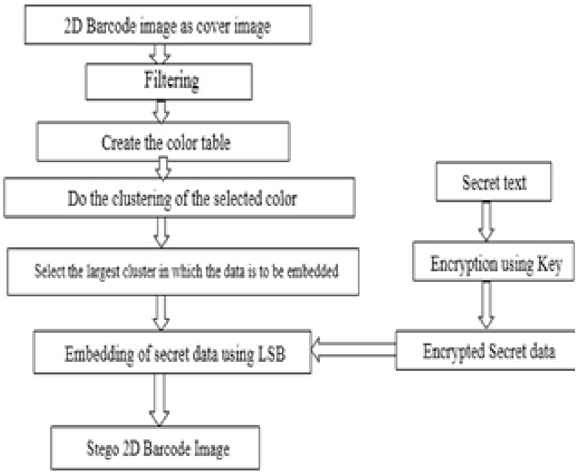
2D Barcode image as cover image
Filtering
Create the color table
Do the clustering of the selected color
Select the largest cluster in which the data is to be embedded
Embedding of secret data using LSB
Stego 2D Barcode Image
Secret text
Encryption using Key
Encrypted Secret data

Fig 3. Proposed Ciphering Technique

At Receiver side:

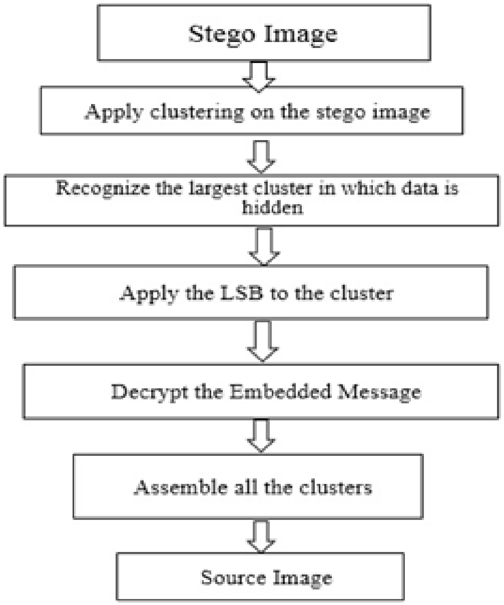
Stego Image
Apply clustering on the stego image
Recognize the largest cluster in which data is hidden
Apply the LSB to the cluster
Decrypt the Embedded Message
Assemble all the clusters
Source Image

Fig 4. Proposed Deciphering Technique

At receiver side the procedure is applied in inverse form which is as follows:

Step 1: In the first step of extraction phase, take the stego-image as input image.

Step 2: Create the clusters of the stego image.

Step 3: Select the cluster in which data is hidden.

Step4: Apply LSB to the selected cluster.

Step 5: Decrypt the encoded message.

Step 6: Extract the Secret message and assemble the clusters.

Step 7: The original 2D barcode cover image is obtained [13].

CONCLUSION

The proposed method is made to make it a better way to add-on the concealed information to image without distortion and with the use of conversion using Least Significant Bit algorithm, that disables to recognize the changes made in stego image for the unauthorized users to identify the location of the sensitive information and crack the code encrypted in the image and the information is secured from illegal user.

The Proposed LSB method is to enhance the existing techniques using 2D barcode images and existing LSB technique. The code design style, edge detection clustering, methodology have now been proposed for ciphering and deciphering the information data. Therefore, the proposed method has been moving the information in the protected segment by using Least Significance Bit method on 2D barcode image. Therefore, the system is designed to improve the efficiency stage to examine existing system.

REFERENCES

[1] Sherin Sugathan, "An Improved LSB Embedding Technique for Image Steganography", 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT),2016 IEEE.

[2] Almara'beh, Hilal, "Steganography Techniques-Data Security Using Audio and Video." Almara'beh International Journal of Advanced Research in Computer Science and Software Engineering 6.2 (2016): 45-50.

[3] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, " Improved Method for LSB Based Color Imagesteganography Combined with Cryptography", ICIS 2016, June 26-29, 2016 IEEE,Japan.

[4] Pallavi Das, Satish Chandra Kushwaha, Madhuparna Chakraborty, "Multiple Embedding Secret Key Image Steganography Using Lsb Substitution And Arnold Transform", 978-1- 4788-7225 -8/15, 2nd International Conference On Electronics And Communication System(Icecs 2015)

[5] Sumeet Kaur, Savina Bansal, R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", 978-93-80544-12-0/14 2014 IEEE.

[6] Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan, "Data Security Using Image Steganography And Weighing Its Techniques", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 11, NOVEMBER 2013,ISSN 2277-8616.

[7] Gagandeep Kaur, Er.Gaurav Deep, “HSI Color Space Conversion Steganography using Elliptic Curve”, International Journal of Innovations & Advancement in Computer Science, IJIACS, ISSN 2347 – 8616, June 2015, Volume 4, Issue 6,

[8] Priyanka Gaur, Shamik Tiwari, “Recognition of 2D Barcode Images Using Edge Detection and Morphological Operation International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 1277-1282.

[9] Praveen.T, Muthaiah.RM, Krishnamoorthy.N, “Transmitting Bulk Amount Of Data In The Form Of Qr Code With CBFSC And Chunking Techniques- Fighting Against Cryptanalytic Attacks”, International Journal Of Computer Engineering And Technology (IJCET), ISSN 0976 – 6375, July-A,2013, Volume 4, Issue 4.

[10] Ravi K Sheth, Rashmi M. Tank, “Image Steganography Techniques”, International Journal of Computer Engineering and Sciences(IJCES), 2015, Volume-1 Issue-2.

[11] Sharu Goel , Ajay Kumar Singh, “A Secure and Optimal QR Code”, International Journal Of Engineering Research & Management Technology, September- 2014,Volume 1, Issue-5.

[12] D. Antony Praveen Kumar ,M. Baskaran, J. Jocin.and Mr. G. Diju Daniel, April 2016,“Data Hiding Using LSB with QR Code Data Pattern Image”, International Journal of Science Technology & Engineering, Volume 2 ,Issue 10.

[13] C. K. Chan, L. M. Cheng, “Hiding data in image by simple LSB substitution”, pattern recognition, Vol. 37, No. 3, 2004, pp. 469-474

[14] Arvind Kumar, Km. Pooja, July 2002, “Steganography- A Data Hiding Technique” International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010 enclosure,” IEICE Trans. Commun., vol. E85-B, no. 7, pp.1360-1367.

[15] Anil Khurana, B.Mohit Mehta, “Comparison of LSB and MSB based Image Steganography”, IJCST Vol. 3, ISSue 3, July - SepT 2012, InternatIonal Journal of Computer SCIenCe and technology.

[16] Mehdi Hussain, Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54,May,2013