Innovative Region Based Steganographic Technique to Provide Security and Authentication to Digital Image

B. Vijaya Kumar, V. Pooja Shukla

Abstract: ***In this advanced world with the growing technology, the demand for security of information is needed in any communication streams of data which is being conveyance from host to intended host over the internet. Obviously, a huge & numerous amount of the data or the information are transferred in our everyday. So, the demand for securing information has become the main concern. Image Steganography is one of the important areas in the field of Steganography. The main purpose of steganography is to protect the surreptitious information from others except from intended receiver & by increasing the security of the covert data in the significant way that information can't be revealed although the intruder knows the methodology of the embedding process. In this paper, The aim is to propose a different yet, an innovative steganographical technique which provides the security on our digital image, and by using a quality measuring technique like Mean Square Error(MSE), Peak Signal Noise Ratio (PSNR) which assure the quality of image has been not degraded even after infusing the covert data inside the image. So to overcome these issues, this paper, suggests a new method to maintain the quality of the image. After embedding the authenticated information in the cover image using Region-Based Least Significant Bit (LSB) technique that provides security of digital image.***

Keywords— Steganography, Least significant bit (LSB), MSE, PSNR, Security

I. INTRODUCTION

In recent few years, the Internet has become an essential part. And sharing of information over the internet is becoming so easy and very convenient that in one blink of eyes the information will be sent to its intended location. But in the meanwhile, we generally get threatened due to the insecurity of losing our exact information which is circulating over the internet. This Question might obviously arise in our mind that "Is our Information is really secure?" In order to deal with such sort of threats and issues, that's why using steganography for securing our digital information or any type of digital data transferring from source to intended destination location is protected from the third parties or attackers, from being misuse of the information. It is taken care by the steganography that our hidden information cannot be identified or traceable to human naked eyes. It mainly focuses on maintaining "the existence of secret information" and protects the secret information from being interrupted by intruders and securely transmits to the intended known-person. The secret message needed to be hidden in suitable digital media can be done in a surreptitious way. The embedding algorithm is the way or method to inject the secret data using least bit value, but randomly inside the image, in such a manner that no one can acquire the embedded furtive information except the intended user only will know it, this method is discussed in Implementation section briefly.

STEGANOGRAHY:

The "Steganography" is a Greek originated word which has been classified into two parts like the first part is "STEGANOS" which means to secret or covered or sealed" and another part is "GRAPHEIN" which means writing" and literally means "HIDDEN WRITING". Digital Steganography is the technical term which is meant "the art and science of writing the hidden secret message inside any type of multimedia data" which helps in protecting and securing the information from any interruption by attackers. The Steganography used for securing the message using different levels of techniques [1].

The main aims of Digital Steganography to hide the actuality of a secret embedded message within the image (cover image) via communication which confirms and provide a promising way for transmitting the information over the internet without being interrupted and safely conveyances the information from source to destination of any type of digital files. The idea of the motivations for developing the image steganography methods is done, according to its use in much different type of organizations to communicate with each other. There are various other government agencies or Intelligence agencies to hide their top secret messages from others. Its fundamental goal is to use Steganography to work accordingly in the planned way of providing security, integrity, authenticity, and quality of digital data [2][3]. Steganography has two important aspects they are: 1) Capacity 2) Imperceptibility (Quality of steganography information). However, these two characteristics are important while processing on digital media. It helps in analyzing the quality of the image is there any major distortions occurred or not because, if there's any major changes are taken place then it leads to the issue of degradability of the image which can become a problem in further. When designing for the Steganographic algorithm few properties need to be implemented which should be taken under consideration carefully are Embedding capacity (Payload), Image Distortions and Undetectable.

The Basic terminology used in Steganography systems are: The cover image, secret message, secret key and embedding algorithm. The cover image carrier's the secret message which is hidden inside it. The secret key used for embedding the secret

Revised Version Manuscript Received on 16 September, 2019.

Dr. B.Vijaya Kumar, Professor & Head of Department, Vidya Jyothi Institute of Technology (VJIT), Hyderabad, India. vijiyasree.b@gmail.com
V.Pooja Shukla, PG Scholar CSE, Vidya Jyothi Institute of Technology (VJIT), Hyderabad, India. poojashukla547@gmail.com

message depending upon the presented algorithms to it. The embedding algorithms are the method of hiding the message in the form of bits inside the cover image. The Steganography system, before hiding the secret message inside cover image we need to develop an effective and appropriate steganography algorithm for encoding the intended secret information in it due to which the sender can send the stego image conveniently to the intended receiver through email, chatting or by any other techniques for sending the message then after receiving the message then intended user will decode with the same key used by the sender .The working of the Steganography System mechanism is shown in the figure: 1

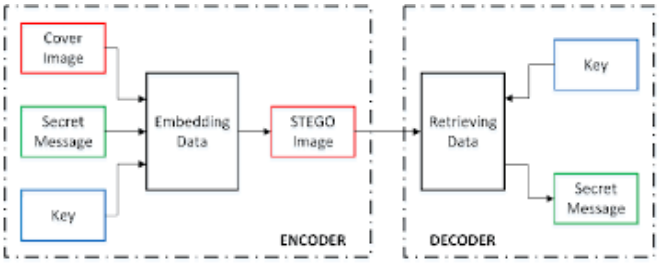

Fig 1: Steganography system mechanism

Nowadays, the image file is most popularly used in this purpose because it easily conveys the communication between the intended sender and receiver only.

IMAGE

An Image is basically in the 2-Dimensional array which is "flat". It's defined in mathematical function as f(x, y) where x & y are vertical dimension (height) and a horizontal dimension (width). The image has the finite number of pixels (picture elements) in rows and columns. The image ranges in between 0 to 255.

Fig 2: 2-D Image

The Digital image is an image that is in the discrete form which is generally referred as the "digital" and the group of combinational binary values with 0's and 1's are called as "pixels". Intensity values are defined as bits and the 8 bits intensity range has 256 possible values. The images are differentiated into three types: Binary (BLACK-WHITE) image, Gray-scale image and RGB color image. The binary image has one-bit value per pixel which is represented by 0 for black &1 for white pixels. The Gray-scale image has an 8bit value per pixel where "00000000" is fully black and "11111111" is fully white pixels. The RGB image contains lots of information and it has 24 bits value per pixel. These types of image are very useful for hiding the information with a bit change in the image resolution which does not affect the image's quality and makes sure that our intended secret message is fully secured without any loss. In this research paper, the RGB image is converted into Gray-scale image which is used as the message carrier to hide the secret messages by using least significant bit hiding technique but in a different way, this is discussed in the proposed method.

THE MATRIX OF IMAGE:

We know that images are represented in rows and columns i.e., M*N and each and every element in this matrix are known as image elements or image's pixels.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & f(0,2) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & f(1,2) & \dots & f(1,N-1) \\ \vdots & \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & f(M-1,2) & \dots & f(M-1,N-1) \end{bmatrix}$$

Fig :3 Matrix of an image

There are few different types of categories in steganography they are text steganography, Image steganography, Audio/Video steganography, TCP/IP protocol steganography and etc.

Image Steganography is the process of hiding furtive message inside the digital image (cover image) and protects it from intruders for any causing any issues. The message is embedded in the digital image by help of the embedding algorithm using the secret key. The resulting stego-image is sent to the receiver and then it extracts the information using the secret key. Due to this technique of steganography, the information will be noticeable to the predetermined sender and receiver.

II. LITERATURE REVIEW

Due to the high demand of hiding the information inside an image and securing it has been concerned. There are different types of approaches that have already published and some of them are mentioned in this section. In "An analysis of LSB based Image steganography technique", K.Thangadurai [4] in this proposed method**,** both cryptography and steganography techniques use LSB modification technique for hiding the data effectively. In "Reversible Data Hiding", by Zhicheng Ni et at [5] proposed reversible data hiding algorithm have been applied in many different types of images including some of the commonly used images, textual images, etc in Corel Draw database has been always satisfied by its result. In "an overview on Image steganography", by T.Morkel et al [6] which explains different types of strong and weak points respectively, where one technique lacks in payload, another lacks in robustness. In "A New Method in Image steganography with improved image quality", by Atallah M. Al-Shatnawi [8] in this proposed method, it hides the secret message based on the search method where it searches the same bits between the secret message and the image pixel values.

In this paper, proposed a method which provides the technique on digital image, for enhancing both "the security of information of the image and quality of images" and also provides authenticity to the intended user's only by Least Significant Bit technique on the different regions inside the image.

III. LEAST SIGNIFICANT BIT

Least Significant Bit Steganography Technique is one of the important yet, an easiest technique which used for replacing the least bit by 0's or 1's inside the digital image. It's

even referred as substitution based technique.

It's the simplest approach which is the process of replacing the cover image's least bit value with hidden the secret message's bit value. The LSB embedding approach became the easiest. For 8 bits 'Gray-scale' image, LSB is the 8th bit value for each byte of pixels in the image where this bit gets replaced by the bits of secret message. For 24-bits 'RGB' colour image, LSB in each colour channel component of the image gets replaced to the bit of secret message. Since the compression of the PNG image is lossless. LSB steganography is best suitably effective with PNG images for hiding information. The Gray-scale digital image is the image that has the values of pixels that carriers the intensity information.

IV. PROPOSED METHOD

In this Paper, proposed a new and innovative steganographical technique for enhancing the quality of an image as well as securing the secret information from being attacked by the intruders. This secures by providing authenticity to the owner. People frequently transmit digital information like images, texts, audios or videos over the internet. In the digital image there's many different formats, as we know that PNG images has various interesting usage in steganographic systems and operating with this become so easy and efficient. By considering the PNG images which will never optimize in size and by using this steganographic technique based on the LSB approach on each region becomes reliable and efficient and our information will be transparent and it can't be noticeable to anyone except to the authorized only. As the PNG images are in lossless compression that means there is no loss of data while performing the extraction process. By this method, it increases efficiency in terms of security and authenticity. This method provides an efficient way to embed the stego message without any visible distortion and makes it very difficult for the unauthorized user to detect any changes in stego image. In this proposed method, it provides security as it divides the image into four regions and based on key values it embeds the stego text inside the image. It provides authenticity to the owner's information.

V. IMPLEMENTION

In the paper, now we implement the proposed idea for securing the information and providing authenticity for the digital images. In this proposed idea we have used Python programming language as it's easy to implement proffers an effective and efficient way by using different types of modules like Pillow, Numpy, OpenCV, etc for supporting the functionality which helps in concluding the results.

Proposed Algorithms:

A proposed algorithm for embedding and extracting the furtive message inside the image can be explained as:

A. EMBEDDING ALGORITHM:

1. Enter the Image and Stego Text
2. Splits the text and stores in an array.
   text= text.split
3. Now, coverts the image into gray-scale image.
4. Divides the Image into four regions (two rows, two cols) and calculates the coordinates.
   fx1, fx2 = (0, w1), (w2, width)
   fy1, fy2 = (0, h1), (h2, height)
5. Calculating the sum of all the pixel values of each individual region.
6. Calculating the average for each individual region of the image.
   Key = (sum of the pixel values of each region) / no. of pixel of the image
   Hence we obtained the average value for each region which is the key value.
7. Selects the pixels in each region, which satisfy the following condition; inside the cover image embeds the stego bit to the selected pixels. The no. of region of cover image & parts of stego text should be equal. In every region of cover image a part of stego text will be inserted in the binary format.
8. Condition :
   Checks the pixel values > key
9. If the above condition satisfies, it sets LSB (0 or 1) of the selected pixel in the region as per the stego bit value then this process continues until all bits of stego information injected inside the image.
10. After embedding all the words of the given text inside in each regions of the image.
    Finally, we obtain the encoded stego image.

B. EXTRACTING ALGORITHM:

1. Now loading stego image for extracting the information.
2. Reads the stego image and using the average value which performs mathematical functions and selects the pixels in each region which contains the text.
3. Reads the LSB values of each pixel in each region.
4. Checks 8 bits and converts binary code into characters and from character to string.
   if check==8 and value> avg
   Character=character+ LSB;
   final-string= final-string+ character
5. While extracting the secret text bits it checks for the 9th bit whether to continue the process or to stop in each and every region's pixel value of image.
   elif check ==9 and value >avg
   If LSB == "0"
   check=1
   elif LSB =="1"
   returns final-string
6. Finally extracts the text of words one by one from each region of the image.

VI. EXPERIMENTAL RESULTS

The results of this paper are obtained by applying our proposed method on different digital images with different sizes. The result for hiding the text inside the digital

gray-scale image(cover image) of eight-bit PNG. The embedding and extracting operations are done using the python platform.

(A)ORIGINAL-pepper (B) GRAY-SCALE-pepper (C)ENCODED-pepper

(A)ORIGINAL-minion (B) GRAYSCALE-minion (C) ENCODED-minion

Fig 4: In the above we have tested our proposed method on these digital images of 'Pepper' and 'Minion'.

In the above, figure we have obtained the results on a few images by implementing the proposed technique in this paper. In both images in Figs. 4(A) it reads and displays the original images, in Figs. 4(B) it displays the converted form from original to gray-scale image which is used as the cover image and in the Figs 4(C) it results the Encoded stego image where stego text is hidden inside, in a proper way that no one can suspects that it contains any surreptitious information and this stego image will be sent to the intended receiver. By implementing this proposed steganographical technique, it really provided good security for our digital image and there are no splotches seen through human eyes and the stego image looks as similar as our digital cover image that no intruder can guess or get's the idea that there exists any surreptitious message. Now, we shall have a look at the quality of our digital image by checking the image's quality using imperceptibility test on the images.

IMPERCEPTIBLITY TEST (QUALITY MEASURE):

In this, it checks the quality of the image by statistical measurement like Mean Square Error (MSE) and Peak Signal Noise Ratio (PSNR). These measurements are important to know that how much amount of noise is present in the actual contents during the process of concealing the message inside the image. While adding the information, the image may gets modified and it get's degraded. So, an effective embedding system will ensure that there's no significant distortions are present or occurred in the image.

Peak Noise Signal Ratio helps in evaluating the quality of image between the cover image and the encoded stego image it is defined as:

$$PSNR=10\log_{10}(MAX^2/MSE) = 20\log_{10}255/\sqrt{MSE}$$

Where, "255" indicates the maximum possible value of the pixel in a gray-scale image or RGB colour image.

Mean Square Error (MSE) is defined as:

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

Where m and n are the rows and columns in the matrix of an image, "I_1 (m, n)" is the cover image and "I_2 (m, n)" is the encoded stego image. As the noise can results to be either negative or positive value for our digital image. Therefore, we use the summation so that noise with value negative or positive will become as positive. The calculated values are obtained in floating points for digital images; its resultant value is indicated by decibels (dB). After determining, the PSNR and MSE values between the cover image and the encoded stego image then if we get the resultant values "high for PSNR and low for MSE" that indicates the distortion in the image is very less and quality of the image is good. Hence it proves that a discrepancy between the cover image and stego image is highly invisible to human eyes. Due to which is not noticeable by anybody and conveys our secret message to the designated user. In the below table 1 shows the determined values of PSNR & MSE between the cover image and stego image. It clearly shows the dissimilarities between the cover image and the stego image.

TABLE I. QUALITY MEASUREMENT

Cover Images	PSNR (dB)	MSE
Pepper	77.66237	0.293
Minion	83.45129	0.235

TABLE II. COMPARISON OF RESULTS WITH EXISTING METHODS

COVER IMAGES	SOUMEN BHOUMIK'S PSNR [7]	DANISH'S PSNR [9]	STEGANOGRAPHIC TECHNIQUE'S PSNR
IMAGE 1	44.0092	52.00451	77.6623
IMAGE 2	44.0307	48.00232	83.4512

From the above quality measurements, determined the quality of stego images is high and the content inside the image secured in a surreptitious way.

VII. CONCLUSION

The basic goals of Steganography are to address the problem of insecurities of digital content and resolve the issue of quality of an image. In this paper, using python programming language explained the method of securely hiding the information inside the image with the help of Steganography and the purpose of providing security and authentication for our digital image is fulfilled with our proposed method. Now with the help of this innovative technique provides high security while transmitting the information or data where the hidden information inside the image is difficult to determine the presence of a furtive message by an unauthorized person. The advantage of this proposed algorithm will inject a message inside an image by changing the least bit value randomly. This brings the more efficiency as compared to any other technique. The experimental result shows the good quality of encoded stego image with better PSNR and low MSE values.

REFERENCES

1. R.ChandraMouli and N.Memom, "Analysis of LSB based Image Steganography", IEEE ICIP, Oct.-2001.
2. Arun Kumar Singh, Juhi Singh, Dr.Harsh Vikram Singh, "Steganography in Images using LSB Technique", IJLTET, Vol.5 Issue 1 Jan-2015.
3. M.Pavani, S.Naganjaneyulu, C.Nagaraju, "A Survey on LSB Steganography Methods" [IJECS] Vol.02 Issue-Aug-2013.
4. K.Thangadurai and G.Sudha Devi "An Analysis of LSB based Image Steganography techniques" ,[ICCCI-2014],Jan.03-05.
5. Zhicheng Ni , Yung-Qing Shi, Nirwan Ansari and Wei Su, "Reversible Data Hiding", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEM FOR VIDEO TECHNOLOGY, Vol. 16 ,No.03, March-2006.
6. T.Morkel, J.H.P Eloff & M.S Olivier, "OVERVIEW OF IMAGE STEGANOGRAPHY" in proceedings of the 5th annual[ISSA2005], June/July2015.
7. SoumenBhowmik, Arup Kumar Bhaumik, "A New approach in color image steganography with level of perceptibility and security",[ICICPI-2016],Oct-2016.
8. Atallah M. Al-Shatnawi ,"A New Method in Image Steganography with Improved Image Quality" Applied Mathematical Sciences, Vol. 6, March- 2012.
9. Danish Shehzaad, Tamer Dag, "Novel Image Steganography Technique based on Similarity bit pairs", IEEE [ICSGRC-2017], 4-5 Aug.2017.

AUTHORS PROFILE

Dr.B. Vijayakumar is Professor in Computer Science & Engineering in Vidya Jyothi Institute of Technology (VJIT) ,Hyderabad . He has about 23 years of Academic and Industry experience. He is a Life Member of CSI,ISTE,NESA,ISCA. He has more than 50 publications in the field of Image Processing , Digital Watermarking, IoT and Cloud Computing

V. Pooja Shukla is student of M.Tech Computer Science and Engineering (CSE) working under the guidance of Dr B.Vijayakumar in Vidya Jyoti Institute of Technology and , Hyderabad