International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review on Various Approaches for Data Hiding

Sukhjinder Pal Kaur[1], Sonika Jindal[2]

[1]Research Scholar, Department of Computer Science & Engineering., SBSSTC, Ferozepur, Punjab, India

[2]Associate Professor, Department of Computer Science & Engineering, SBSSTC, Ferozepur, Punjab, India

Abstract: ***The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused datain regular computer files (such as graphics, sound, text or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.***

Keywords: image stegnography, RGB, Least Significant Bit, Intermediate Significant Bit.

1. Introduction

1.1 Stegnography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing defining it as "covered writing". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message.

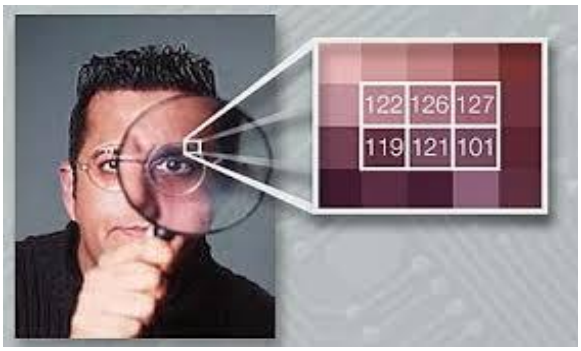


Figure 1.1: Stenography

1.2 Different kind of Stenography

1.2.1Text stenography: Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

1.2.2 Image stenography: Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is Send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of steno image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

1.2.3 Audio stenography: Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

1.2.4 Protocol steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

1.3 Applications of Steganography

Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.

Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganography techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files

because of a watermark, Steganography methods can be used to hide this.

E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.

Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.

The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

2. Review of Literature

Androutsos, D et al [1] "Efficient image database filtering using color vector techniques" With the widespread availability of personal computers and the staggering amount of digital imagery available, recent investigation has focused on the storage, query and retrieval of images from large image databases. Queries of color, shape, texture, etc., are then performed directly on these indices to find valid images. The authors propose a new indexing technique which calculates the multidimensional histogram of the directional detail in a given image. They apply wavelet theory and multi resolution analysis to extract the directional information from an image and then map this information into 3-dimensional vectors. Histograms of these vectors are then calculated at different levels of resolution, allowing progressive image query using color histogram techniques to be directly applied.

Behera, S.K. et al [2]"Color Guided Color Image Steganography", Author use one component case: here we have 3 ways to determine the bits * 3 ways to decide the component R, G or B. this results in 9 cases. Using two component case: here we have 3 ways to determine the bits * 3 ways to decide the component RG, RG or GB. This results in 9 cases. Using three component case: here we have 3 ways to determine the bits * one way to decide the component which is RGB. This results in 3 cases. The average capacity ratio is around 1/7 or 14% of the original cover media size. The secret data is scattered throughout the whole image. Also, extracting the secret data without the knowledge of seeds is almost impossible. The capacity of the triple technique is higher than the previous techniques. By using this algorithm, the ratio between the number of bits used inside a pixel to hide part of the secret message.

Bailey and Curran [3]"Visual cryptographic steganography in images "Author described an image based multi-bit steganography technique to increase capacity hiding secrets in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the simplest of this, where it inserts the secret message data into one MLSB (lower order bit) of the image pixels, which is undetectable. Hide and Seek is an example of this technique. Note that if this bit insertion is performed into the higher order bit (most significant bit), the value of the pixel will show a great detectable change spoiling its security. It is known that insertion of hidden bits into lowest order MLSB in all color RGB channels of the image pixels is unnoticeable. In the Stego-2bits method two bits of lower order MLSB in RGB image steganography is used; Stego-2bits doubled the capacity of message hiding with negligible security reduction. The capacity can be enhanced more as in Stego-3bits and even more in stego-4bits, which are jeopardizing security accordingly. Weakness of this technique is that the hidden bits are simply revealed because of the sequential storage of data.

Chapman, M. Davida G, and Rennhard M. et al [4] "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" Author want to propose that most of the data hiding methods in image steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each pixel is replaced to hide bits of the secret message. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits. The hidden information can easily be uncovered using many known statistical steganalysis techniques, such as the X2 that can detect the concealed data inside the image with its original size.

Gutub, A. et al [5] 2001 "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", Author want to say that steganography utilizing RGB images as cover media. The technique uses least two significant bits of one of the channels Red, Green or Blue as an indicator of secret data existence in the other two channels. The indicator channel is chosen in sequence from R, G and B, i.e. RGB, RBG, GBR, GRB, BRG and BGR. However the indicator LSB bits are naturally available random, based on image profile and its properties.

3. Approaches Used

Least significant bit:LSB can also stand for least significant byte. The meaning is parallel to the above: it is the byte in that position of a multi-byte number which has the least potential value. If the abbreviation's meaning least significant byte isn't obvious from context, it should be stated explicitly to avoid confusion with least significant bit.To avoid this ambiguity, the less abbreviated terms "lsbit" or "lsbyte" are often used.In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes

referred to as the *right-most bit*, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the *ones* (right-most) position.

Most significant bit: In computing, the mostsignificant bit (MSB, also called the high-order bit) is the bit position in a binary number having the greatest value. The MSB is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits further to the left.The MSB can also correspond to the sign bit of a signed binary number in one's or two's complement notation, "1" meaning negative and "0" meaning positive.It is common to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used.This may be one of the reasons why the term *MSB* is often used instead of a bit number, although the primary reason is probably that different number representations use different numbers of bits.

JPEG Image Stegnography Technique: Originally it was thought that Steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. One of the key characteristics of Steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be damaged. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. Still, properties of the compression algorithm have been exploited in order to develop a steganography algorithm for JPEGs. One of these properties of JPEG is exploited to make the changes to the image unseen to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable and understandable. **Spread Spectrum Image Stegnography Technique:** The Spread Spectrum Image Steganography (SSIS) of the present invention is a data hiding/secret communication steganographic system which uses digital imagery as a cover signal. Spread spectrum provides the ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer. The message is recovered with lowest error probability due the use of error control coding. Spread spectrum image steganography payload is, at a minimum, an order of magnitude greater than of existing watermarking techniques. Furthermore, the original image is not needed to extract the hidden message. The proposed receiver need only possess a key in order to reveal the secret message. The existence of the hidden information is virtually undetectable by human or computer analysis. at last, SSIS provides resiliency to transmission noise, like which found in a wireless environment and low levels of compression.

4. Methodology

Steganography is done for secure transmission of data on network. Various phases for data steganography are described below.

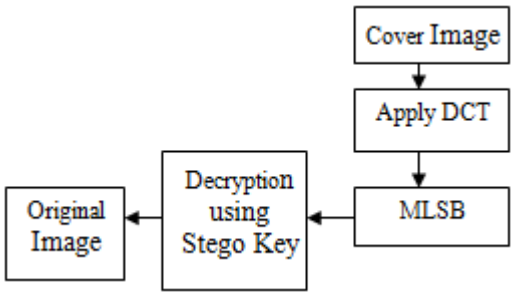
Phase 1: Select on cover image for data embedding cover image should be a color image containing red, green and blue pixels.

Phase 2: In the second phase apply modified least significant bits

- Decompose the cover image into different bands i.e. LL,LH,HH,HL
- Convert into integer value using threshold
- Embed the secret message in the middle using modified MLSB
- Obtain stego-image.

Phase 3: In this phase extract secret data using the stego-key and convert the duplicate message into original message. This recovery of the duplicate audio/vedio/image can be done using encoding key. In the last we get the original message.

4.1 Flow of Work



5. Conclusion

Steganography is a technique for the secure transmission of data over the network. The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. In this process image is divided into different regions for the detection of least significant bits available in different images. Image pixel available in the image is a combination of three different colors red, green and blue. In the proposed work, the modified least significant bit is implemented. The main motivation behind the work which is done is to make LSB more detectable and more secure and also the data that is sent behind the audio/video is in more quantity as compared to LSB and ISB. Modifications over traditional LSB method are introduced to increase the amount of data that can be hided in the cover image. In addition, to increase data protection our algorithm have a built in encryption technique. As LSB the output image of algorithm will look identical to the cover image.We are using LSB and MLSB, ISB approaches for secure the data transmission.

References

[1] Androutsos, D "Efficient image database filtering using colour vector techniques", IEEE Conf. on Electrical and Computer Engineering, 1997, pp 827 - 830 vol.2.
[2] Behera, S.K. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology**,** Vol. 1, No. 1, pp. 16-23, IEEE, 2010.
[3] Bailey, K. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications,Vol. 30, No. 1**,** pp. 55-88,IEEE,2006.
[4] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf
[5] Gutub, A. "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E**.,** pp. 154-159,IEEE,2008.
[6] Gutub, A. "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence,Vol. 2, No.1, pp. 193-198,IEEE,2010.
[7] Liberda, O "Data processing in studying the temporomandibular joint, using MR imaging and sonographic techniques", IEEE conf. on Digital Signal Processing, 2009, pp 1 – 6.
[8] Marwaha, P. "Visual cryptographic steganography in images", Second International conference on Computing, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
[9] Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher", International Conference on Computing, Communication and Sensor Network (CCSN), pp 0975-888, IEEE, 2012.
[10] Singh, V. "A methodological survey of image segmentation using soft computing techniques", IEEE Conf. on Computer Engineering and Applications (ICACEA), 2015, ppm 419 – 422.