© 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Brief Study on Various Approaches of Image Steganography

Varun Maini
Assistant Professor, Department of Computer Science & Applications, S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India

ABSTRACT

Steganography is the process that has been used for data hiding behind the cover object. In the process of steganography various types of steganography has been used so that information can be easily transmitted in secret manner. In this paper various approaches that have been used for data hiding process behind the images have been discussed. In the process of image steganography various approaches that are based on least significant bits, Random pixel based, interpolation based and AI based approaches have been used. In this paper a brief study has been discussed about these approaches that can be used for data hiding. Data integrity is the major concern in image steganography process. this has been achieved on the basis of different security measurements that are encryption of the secret information or interpolation of the secret information.

Keywords : Steganography, LSB, MSB, AI and Interpolation

I. INTRODUCTION

1.1 Steganography: Steganography is gotten from the Greek words "segos" signifying "spread" and "raffia" signifying composition characterizing it as "secured written work". In picture Steganography the data is shrouded only in pictures. The thought and practice of concealing data has a long history. In Histories the Greek history specialist Herodotus composes of an aristocrat, Hostages, who expected to speak with his child in-law in Greece. He shaved the leader of one of his most trusted slaves and tattooed the message onto the slave's scalp. At the point when the slave's hair developed back the slave was dispatched with the shrouded message. In the Second World War the Microdot system was produced by the Germans. Two different innovations that are nearly identified with Steganography are watermarking and fingerprinting. These innovations are principally concerned with the assurance of protected innovation, in this way the calculations have diverse prerequisites than Steganography.

1.2 Uses of Steganography

- Steganography can be an answer which makes it conceivable to send news and data without being controlled and without the apprehension of the messages being blocked and followed back to us.
- It is additionally conceivable to just utilize steganography to store data on an area. Case in point, a few data sources like our private keeping money data, some military privileged insights, can be put away in a spread source.
- Steganography can likewise be utilized to execute watermarking. Despite the fact that the idea of watermarking is not so much steganography, there are a few steganographic systems that are being utilized to store watermarks in information. The fundamental contrast is on aim, while the reason for steganography is concealing data, watermarking is just broadening the spread source with additional data. Since individuals won't acknowledge detectable changes in pictures, sound or feature records on account of a watermark, steganography systems can be utilized to conceal this.

- E-business takes into consideration an intriguing utilization of steganography. In current e-business exchanges, most clients are ensured by a username and secret word, with no genuine technique for confirming that the client is the genuine card holder. Biometric unique finger impression filtering, joined with extraordinary session IDs inserted into the unique mark pictures by means of steganography, take into consideration an exceptionally secure choice to open ecommerce exchange check.
- Matched with existing specialized systems, steganography can be utilized to do concealed trades. Governments are keen on two sorts of concealed interchanges: those that help national security and those that don't. Computerized steganography gives incomprehensible potential for both sorts. Organizations may have comparative concerns with respect to insider facts or new item data.
- The transportation of delicate information is an alternate key utilization of steganography. A potential issue with cryptography is that meddlers know they have a scrambled message when they see one. Steganography permits to transport of delicate information past meddlers without them knowing any touchy information has passed them. The thought of utilizing steganography as a part of information transportation can be connected to pretty much any information transportation strategy, from E-Mail to pictures on Internet site.

1.3 Different kind of Steganography

1.3.1 Text 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.

1.3.2 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

1.3.3 Audio stenography

Audio steganography 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.

1.3.4 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.

1.3.5 Video Steganography

Video Steganography is a method to conceal any sort of records into a convey Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file. This venture is the application created to insert any sort of data (File) in an alternate document, which is called transporter record. The bearer document must be a feature record. It is concerned with inserting data in a harmless spread media in a protected and powerful way. This framework makes the Files more secure by utilizing the ideas Steganography and Cryptography

1.4 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.
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography,

there are several stenographic 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.

- 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.
- 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.
- 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
- 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.

II. REVIEW OF LITERATURE

Khan S. et al (2016) "Analysis of Data hiding in R, G and B Channels of Color Image using Various Number of LSBs" In today's world of fast communication, to insure the security and integrity of information is a big challenge. Data hiding also known as Steganography is one of the fields that deal in methods related information security and hide secret information and message other information. This paper elucidates the effect of data hiding in different number of least significant bits in the primary colors of RGB color image. These individual color channels are analyzed at different hiding capacity level and its has been observed that high quality Stego images with PNSR 30dB and above can been obtained by hiding secret information in 5 least significant bits of red, green and blue channels, specially the green and blue channels give a very high visual quality. The individual channels can hide 20% data, i.e. one fifth of the overall size of cover image, with undetectable changes in cover image.

Joshi et al (2016) "New Approach toward Data Hiding Using XOR for Image Steganography" with the growth in internet usage, there is proportional growth in security and privacy demands. In this paper, a three bit XOR steganography system for concealing messages into gray Images is projected. In this method, last three bits of pixel value offer 100 percentage of message addition. This new technique uses the XOR operation between the message and original image. If the intruder extracts the last three bits, he would not be able to find the meaning of the message as the message is in decoded form. The maximum no of bit which is to be hidden using this method is equal to the R*C*3, where R and C is the rows and column of the image. The time complexity Is also calculated which is equal to O(1). Later on the method is analyzed on the bases of PSNR, MSE, L2RAT and

MAXERR. The projected technique is also matched with other similar techniques to show the superiority.

Behera, S. K. et. Al. (2010) "Color Guided Color Image 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.

Mahmoud Ankeet. al. (2010) "Pixel Indicator High Capacity Technique for RGB Image Based Steganography" in this paper author want to say that the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G green) and z-axis can be for B (blue). Embedding data into an image often changes the color. Frequencies in a predictable way and also gives redundancy in formats like bmp. To remove this predictability, we will embed the cipher in the image in an encrypted form using a reference database instead of direct bit variations. Also only jpeg image will be used as it reflects the least impact of Steganography.

Gutub A. et. al. (2010) "Pixel Indicator Technique for RGB Image Steganography" in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. The sequence of the algorithm is given below. The first 8 bytes at the beginning of the image are used to store the size of the hidden message, which is also used to define the beginning of the indicator channel sequence. These 8 bytes consumes all LSBs of the RGB channels, assuming it is enough to store the size of the hidden bits. To choose the first indicator channel, the size stored in the first 8 bytes is used. The indicator choice is assumed as the first level, followed by the data hiding channels as second level. All six possible selections are obtained from the length of message (N), which will control the sequence.

III. APPROACHES USED

LSB (Least Significant Bit): 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) positioned and Technology. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

MSB (Most significant bit)

Most significant 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. Normally, this is simply the exponent for the corresponding bit weight in base-2 (such as in 2^{31}...20).

MLSB: Image segmentation is the process that uses to partition cover image into a set of sub images depending on a new hypothesis. Different methods proposed by many researchers had been implemented to achieve image segmentation based on the value of intensity, similarity, and variance between neighboring bytes. In the proposed algorithm, the hypothesis that is created is based on cipher key with three operations to make hard to detect the segments edges from the attacker.

Genetic Algorithm: The genetic algorithm usage the three main phases first selection, cross over and mutation. But the involved operators are usages the random selection process for searching the key data. Therefore the recovery of original data which is hidden in image is suspected. Thus need to add some heuristics during selection process to obtain the fixed set of pixels by evaluation of row and column pixels [3].Objective function is used when someone uses Genetic Algorithm to optimize the parameters of system or in complex search process. The area of interest here is to perform uniform single point crossover to generate complex cipher. Therefore here no objective function is used.

IV. CONCLUSION

Image steganography has been used in secret information transmission so that information can be transmitted in secure and secret manner. On the basis of image steganography process secret information has been converted into binary sequence and that has been embedded with pixels bits of the cover image. Vaious approaches have been developed that has been used for process of data hiding. In this paper a review has been done on the approaches that can be used for data hiding process. Security from intrusion or malicious attacks can be achieved through artificial intelligence processes and through encryption based approaches. On the basis s of review of various image steganography approaches we can conclude that LSB based and AI based approaches provide better steganography as compare to existing approaches. These approaches have major advantage is that these does not affect the quality of the image.

V. REFERENCES

[1]. Sahib Khan, “Analysis of Data hiding in R, G and B Channels of Color Image using Various Number of LSBs”, IEEE Conf. on Color image, 2016, pp 34-45.

[2]. Kamaldeep Joshi “New Approach toward Data Hiding Using XOR for Image Steganography”, IEEE Conf. on XOR, 2016, pp 129-137.

[3]. Getup, A. “Pixel Indicator Technique for RGB Image Steganography”, Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1,IEEE,2010, pp. 193-198.

[4]. P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," 2010 Second International conference on Computing, Communication and Networking Technologies, Karur, 2010, pp. 1-6.

[5]. Bailey, K. “An evaluation of image based Steganography methods”, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, IEEE, 2006, pp. 55-88.

[6]. Mahata, S.K. “A Novel Approach of Steganography using Hill Cipher”, International Conference on Computing, Communication and Sensor Network (CCSN), IEEE, 2012, pp. 0975-888.

[7]. 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.

[8]. Mehboob, B. "A Steganography implementation", Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, ISSN 978-1-4244-2427-6, IEEE, 2008, pp.1–5.

[9]. Marwaha, P. "Visual cryptographic Steganography in images", Second International conference on Computing, Communication and Networking Technologies, IEEE, 2010, . 34-39.

[10]. Bailey, K. "An evaluation of image based Steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, IEEE, 2006, pp. 55-88.

[11]. Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher", International Conference on Computing, Communication and Sensor Network (CCSN), IEEE, 2012, pp. 0975-888.

[12]. Saravanan, V, Neeraja, A. "Security issues in computer networks and steganography", IEEE 7th International Conference on Intelligent Systems and Control, pp. 363-366, 2013.

Author Profile

Varun Maini received his M.C.A. degree from Lovely Professional University, Jalandhar, and Punjab, India in 2010 He is currently an Assistant Professor in S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India with Five years of experience. He has also Qualified UGC-NET in the subject of Computer Science & Applications. His areas of interest Includes Database, Cloud Computing, Image Processing and Networking.