Image Steganography and Data Security Approaches: A Review

Ankur Gupta
Assistant Professor in Computer Science
R. S. D. College, Ferozepur City.

Received Dec. 01, 2017 Accepted Jan. 01, 2018

ABSTRACT *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. In this process image is divided into different regions for the detection of least significant bits available in different images. The no. of bits that can be utilized for image enhancement depend upon the pixel intensity the low intensity pixel utilizes less no. of bits and pixel having a high intensity utilized maximum bits in the process of hiding the image. The issue in this is security for prevention image from stegnalysis attack and the secret data is available in such a manner as it transmitted.in this paper a review on various approaches have been done that has been used for embedding of secret information behind the cover object.*

Keywords: *Image Stegnography, LSB, MLSB, Blowfish.*

1. INTRODUCTION

1.1 Steganography

Steganography is the workmanship and investigation of imperceptible correspondence. This is refined through concealing data in other data, accordingly concealing the presence of the imparted data.

Steganography varies from cryptography as in where cryptography concentrates on keeping the substance of a message mystery, Steganography concentrates on keeping the presence of a message mystery. Steganography and cryptography are both approaches to secure data from undesirable gatherings yet not one or the other innovation alone is flawless and can be bargained. Once the vicinity of shrouded data is uncovered or even suspected, the motivation behind Steganography is part of the way crushed. The quality of Steganography can in this manner be enhanced by joining it with cryptography.

The sort of data covered up in items when utilizing watermarking is typically a signature to connote root or proprietorship with the end goal of copyright insurance [6]. With fingerprinting then again, distinctive, exceptional imprints are inserted in different duplicates of the transporter protest that are supplied to diverse clients.

1.2 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 Image Definition: To a PC, a picture is an accumulation of numbers that constitute diverse light intensities in distinctive regions of the picture. This numeric representation structures a network and the individual focuses are referred to as pixels. Most pictures on the Internet comprises of a rectangular guide of the picture's pixels (spoken to as bits) where each pixel is found and its shading. These pixels are shown on a level plane line by column. The quantity of bits in a shading plan, called the bit profundity, alludes to the quantity of bits utilized for every pixel. The littlest bit profundity in present shading plans is 8, implying that there are 8 bits used to portray the shading of every pixel. Monochrome and grey scale pictures utilize 8 bits for every pixel and have the capacity to show 256 diverse hues or shades of dark. Advanced shading pictures are regularly put away in 24-bit documents and utilize the RGB shading model, otherwise called genuine nature. All shading varieties for the pixels of a 24-bit picture are determined from three essential hues: red, green and blue, and every essential shading is spoken to by 8 bits. Subsequently in one given pixel, there can be 256 separate amounts of red, green and blue, signifying more than 16-million blends, bringing about more than 16-million colours. Of course the bigger measure of colours that can be shown, the bigger the record size.

1.4 Image Compression: At the point when working with bigger pictures of more noteworthy bit depth, the pictures have a tendency to end up excessively extensive to transmit more than a standard Internet association. To show a picture in a sensible measure of time, methods must be consolidated to decrease the picture's record size. These strategies make utilization of numerical recipes to examine what's more consolidate picture information, bringing about littler document sizes. This methodology is called pressure. In pictures there are two sorts of pressure: lossy and lossless. Both routines spare storage room, however the methodology that they execute vary. Lossy pressure makes littler records via tossing overabundance picture information from the first picture. It evacuates subtle elements that are excessively little for the human eye to separate, bringing about close estimates of the first picture, albeit not a careful copy. A case of a picture design that uses this pressure system is JPEG (Joint Photographic Experts Group) Lossless pressure, then again, never expels any data from the first picture, however speaks to information in scientific equations. The first picture's uprightness is kept up and the decompressed picture yield is a little bit at a time indistinguishable to the first picture information. Pressure assumes a critical part in picking which steganography calculation to utilize. Lossy pressure methods bring about littler picture record sizes, yet it builds the likelihood that the inserted message may be mostly lost because of the way that abundance picture information will be evacuated. Lossless pressure however, keeps the first advanced picture in place without the shot of lost, despite the fact that is does not pack the picture to such a little document size. Diverse steganography calculations have been produced for both of these pressure sorts

1.5 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.

2. REVIEW OF LITERATURE

Bandyopadhyay, S.K. et al [11] "Network Based Public Key Method for Steganography" Steganography (a harsh Greek interpretation of the term Steganography is mystery written work) has been utilized as a part of different structures for a long time. It has discovered use in differently in military, political, individual and licensed innovation applications. Quickly expressed, steganography is the term connected to any number of procedures that will shroud a message inside an article, where the concealed message won't be obvious to an onlooker. The first stenographic applications utilized "invalid figures", or clear content. An invalid figure passes on that the message has not been encoded at all, whether it is utilizing essential character moving, substitution or propelled advanced encryption calculation. Thus, the message is regularly in plain view yet for a reason can either not be caught as being available or can't be seen once recognized. As is regular with cryptography, steganography has itsestablishes in military and government applications and has propelled in creativity and multifaceted nature. In this paper, Network Based Public Key Method for Steganography is proposed under RSA cryptographic suspicions.

Changder, S et al [12] "A Greedy Approach to Text Steganography Using Properties of Sentences" Steganography is the art of secured or hidden written work. The reason for steganography is secret correspondence to conceal the presence of a message from a mediator. Computerized Steganography calculations have been produced by utilizing messages, pictures and sound and so forth as the spread media. This paper displays another approach on content steganography through Indian Languages. Considering the properties of a sentence, for example, number of words, number of characters, number of vowels and so forth and utilizing the vicinity of excess gimmick code capable characters in Indian Languages, this methodology shrouds the message into a pure spread record containing Indian writings. This methodology likewise introduces the extraction of message from the created spread record by applying the opposite strategy for covering up. The methodology shows agreeable results on applying to some theme of day by day daily paper in Indian Languages like Bengali.

GeHuayong et al [13] "Steganography and steganalysis based on digital image" With the quick advancement of steganography, steganalysis has progressed rapidly. Fight in the middle of steganography and steganalysis has turned into an essential issue in data security going for a generally utilized spread media, i.e., computerized picture, this article audits steganography and steganalysis taking into account advanced picture. Idea and standard of steganography and steganalysis are represented. Spatial space and change area implanting systems are summed up. Also the late advances in steganalysis are reiterated. At that point the execution particular of picture steganography is examined. At long last some new pattern and issues confronted are likewise talked about.

Selvi, G.K et al [14] "Steganography using edge adaptive image" The development of rapid PC systems and that of the Internet, specifically, has expanded the simplicity of Information Communication. Incidentally, the foundation for the advancement is likewise of the misgiving - utilization of advanced arranged information. In examination with Analog media, Digital media offers a few unique favorable circumstances, for example, superb, simple altering, high devotion replicating, layering and so forth. Anyway this sort progression in the field of information correspondence in other sense has trekked the apprehension of getting the information snooped at the time of sending it from the sender to the recipient. Thus, Information Security is turning into an indivisible piece of Data Communication. To address this Information Security Steganography assumes a critical part. Steganography is the workmanship and art of composing concealed messages in such a route, to the point that nobody separated from the sender and planned beneficiary even acknowledges there is a shrouded message. This paper is an exercise survey of the steganography systems showed up in the writing. Different picture steganography systems have been proposed. In this paper, we research steganography procedures and steganalysis methods. We express a set of criteria to examine and assess the qualities and shortcomings of the exhibited strategies. The minimum huge bit (LSB) insertion strategy is the most widely recognized and simplest system for inserting messages in a picture with high limit, while it is perceptible by measurable examination, for example, RS and Chi-square examinations. This paper has proposed a novel LSB picture steganography calculation that can viably oppose picture steganalysis in light of factual investigation.

Md. Rashedul Islam et al [15] "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" In Steganography, the aggregate message will be undetectable into a spread media, for example, content, sound, feature, and picture in which assailants don't have any thought regarding the first message that the media contain and which calculation utilization to install or concentrate it. In this paper, the proposed system has concentrated on Bitmap picture as it is uncompressed and helpful than some other picture organization to actualize LSB Steganography technique. For better security AES cryptography procedure has additionally been utilized as a part of the proposed system. Before applying the Steganography method, AES cryptography will change the mystery message into figure content to guarantee two layer security of the message. In the proposed procedure, another Steganography method is being created to conceal huge information in Bitmap picture utilizing sifting based calculation, which utilizes MSB bits for sifting reason. This strategy utilizes the idea of status checking for insertion and recovery of message. This strategy is a change of Least Significant Bit (LSB) strategy for concealing data in pictures. It is being anticipated that the proposed strategy will ready to shroud substantial information in a solitary picture holding the favorable circumstances and disposing of the drawbacks of the conventional LSB system. Different sizes of information are put away inside the pictures and the PSNR are additionally computed for each of the pictures tried. In light of the PSNR esteem, the Stego picture has higher PSNR esteem when contrasted with other strategy. Consequently the proposed Steganography strategy is extremely effective to conceal the mystery data inside a picture.

Proposed system has been tried effectively on a. wav record at an examining recurrence of 8000 examples/second with each one example containing 8 bits.

Yang Ren-er et al [16] "Image Steganography Combined with DES Encryption Pre-processing" With a specific end goal to enhance the security of steganography, this paper mulled over picture steganography joined with preprocessing of DES encryption. At the point when transmitting the mystery data, firstly, encode the data expected to cover up by DES encryption is scrambled, and afterward is composed in the picture through the LSB steganography. Encryption calculation enhances the least matching execution between the picture and the mystery data by changing the measurable attributes of the mystery data to upgrade the opposition to recognition of the picture steganography.

3. 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. Therefore, a system named Video Steganography System to embed secret image is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image. It is a common, simple approach to embedding information in a cover image [1]. The least significant bit (in other words, the 8th bit) of some or all the bits inside an image is changed to a bit of the secret message the technique for increased capacity of information hiding in LSB„s method gives better performance in all the parameters and is a safe technique for embedding secret messages.[3]For example a grid for 3 pixels of a 24- bit image can be follows:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is embedded into the Least Significant Bit of this part of the image, the resulting grid is as follows:
(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

Although the number was embedded into the first 8 bits of the grid, only the 3 underlines bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

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). Although a few CPU manufacturers assign bit numbers the opposite way the *MSB* unambiguously remains the *most* significant bit. 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.

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.

BLOWFISH ALGORITHM: Blowfish isa symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention.Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

4. CONCLUSION

Image stenography is another approach which utilizes an image for the secure transmission of data by hiding it behind a cover image. Today Security is a major issue. The issue of security has been resolved by using encryption for the security issue occurred in stagnlysis attack. The embedding of the image has been done by using MLSB for data embedding according to pixel intensity value. Here fuzzy based classifier is used for prediction of least significant bits that provides minimum distortion. Blowfish is used for encryption purpose. On the basis of study of different data security and data embedding approach we can conclude that encryption must be used for data encryption for privacy and efficientembeddingapproach for data hiding.

REFRENCES

1. W. Wang, and J. Jingling, “Multi-spectral Image Fusion based on the characteristic of Imaging System", *International Conference on Information and Automation,* pp. 643-647, 2013.
2. Taherdangkoo, M “Segmentation of MR brain images using FCM improved by artificial bee colony (ABC) algorithm” IEEE Conf. on Information Technology and Applications in Biomedicine (ITAB), 2010, pp. 1 – 5.
3. Yu Li “Image Segmentation Using FCM Optimized by Quantum Immune Clone Algorithm”, IEEE Conf. on Intelligent Systems Design and Engineering Applications (ISDEA), 2014, pp. 537 – 540.
4. Beevi, S.Z “A robust fuzzy clustering technique with spatial neighborhood information for effective medical image segmentation: An efficient variant of fuzzy clustering technique with spatial information for effective noisy medical image segmentation”, IEEE Conf on Computing Communication and Networking Technologies (ICCCNT), 2010, pp. 1 – 8.
5. Qin Xinqiang; ZhengJiaoyue; Hu Gang “Image fusion method based on the local neighborhood feature and no subsampledcontourlet transform”, Image, Vision and Computing (ICIVC), 2017, pp. 2-10.
6. Qamar Nawaz; Xiao Bin; Li Weisheng; Isma Hamid “Multi-modal medical image fusion using 2DPCA”, **:** Image, Vision and Computing (ICIVC), 2017, pp 200-212.
7. M. Hossny; S. Nahavandi; D. Creighton; C. Lim; A. Bhatti “Enhanced decision fusion of semantically segmented images via local majority saliency map”, Electronics Letters, 2017, pp. 1036 – 1038.
8. A. Noskov; A. Priorov “Application of rank correlation at multi-focused image fusion quality assessment”, Systems of Signal Synchronization, Generating and Processing in Telecommunications, 2017, pp. 500-512.
9. XinChen;Jun Wu;ShaoyanSun;Qi Tian “Multi-index fusion via similarity matrix pooling for image retrieval”, Communications (ICC), 2017 IEEE International Conference, 2017, pp. 234-247.
10. Yu Liu; Xun Chen; Juan Cheng;Hu Peng “A medical image fusion method based on convolutional neural networks”, Information Fusion (Fusion), 2017 20th International Conference, 2017, pp. 20-34.
11. Chunyu Wei; Bingyin Zhou; Wei Guo “A three scale image transformation for infrared and visible image fusion”, Information Fusion (Fusion), 2017, pp. 110-124.
12. Yong Yang; Min Ding; Shuying Huang; YueQue “Multi-focus Image Fusion via Clustering PCA Based Joint Dictionary Learning”, IEEE Access, 2017, pp. 1-5.
13. K C Haritha; G Jeyakumar;S Thangavelu “Image fusion using evolutionary algorithms: A survey”,Advanced Computing and Communication Systems (ICACCS),2017, pp. 32-40.
14. ChaobenDu;SheshengGao“Image Segmentation-Based Multi-Focus Image Fusion Through Multi-Scale Convolutional Neural Network”, 2017, pp.15750 – 15761.
15. AyushDogra; BhawnaGoyal; Sunil Agrawal “From Multi-Scale Decomposition to Non-Multi-Scale Decomposition Methods: A Comprehensive Survey of Image Fusion Techniques and Its Applications”, pp.16040 – 16067.