IJRECE VOL. 4 ISSUE 2 APR.-JUNE 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.1.2800.6001

Various Data Hiding Techniques for Secure Transmission: Review

Gurjeet Kaur[1], Rupinder Kaur[2]
[1]*Student, M.Tech (scholar), Doaba Institute of Engineering and Technology, Kharar*
[2]*Assistant Professor, Doaba Institute of Engineering and Technology, Kharar*

Abstract - Steganography process is the most ancient process specially used for hiding an image in the second image. First time use of steganography can be traced in 440 BC when Herodotus mentions two examples in his history. A simple technique of steganography is established on adjusting the least important bit layer of images, known as the LSB technique. The LSB method directly embeds the undergroundinformation within the pixels of the hiding place image. In some cases LSB of pixels visited in accidental or in certain spaces of image and occasionallyincrease or decrement the pixel value. Some of the recent research planned the nature of the stego and optional new procedures for increasing the capacity. A good technique of image steganography goals at three features. First one is size (the extreme data that can be stored inside cover image). Second one is the inaudibility (the visual excellence of stego-image afterward data hiding) and the last is robustness. The main impartial of Steganography is to interconnectstrongly in such a manner that the true information is not evident to the witness.

I. INTRODUCTION TO STEGANOGRAPHY

The practice or technique of concealing some significant and crucial data within other trivial data is called Steganography. Steganography basically works on the principle of Security through Obscurity. The most extensively practiced form of steganography is Visual steganography and is usually achieved through image files. Our focus will be on image files to accomplish visual steganography. [1] Steganography is the discipline that involves collaboratingtop-secretinfo in ansuitable multimedia transporter, e.g., video image, audio files. The media by or deprived ofsecretedinfo are named Stego Media and Cover Broadcasting, correspondingly. Steganography can encounter both legal and unlawfulcomforts, e.g., civilians might use it for defensive privacy while radicals may use it for spreading terroristic information.

Steganography and Cryptography are partners in the detective expertise family. Cryptography scrambles a message so it cannot be unwritten. Steganography hides the memo so it cann't be unspoken.[2]

Types of steganography: Steganography can use for almost all digital file formats, but the formats those are with extraordinary degree of dismissal are more appropriate. Redundancy can be distinct as the bits of an object that deliver correctness far greater than essential for the object's use and exhibition. The terminated bits of an objective are those bits that can be altered without the modification being sensed easily [4]. Image and audio files especially comply with this need, while investigation has also exposed other file formats that can be used for info hiding. There are four groupings of file arrangements that can be used for Steganography exposed in fig 2. [3]

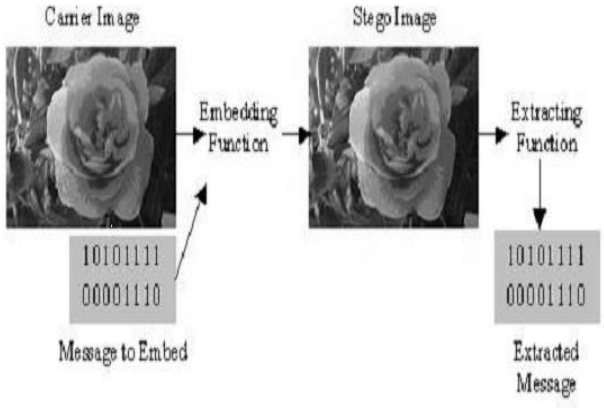

Fig.1: Image Steganography

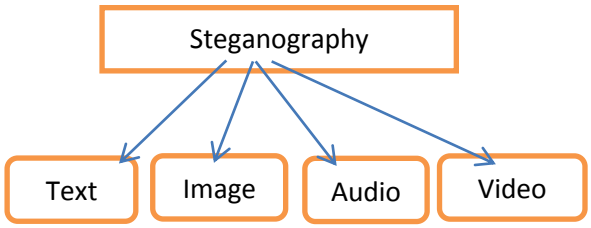

Fig.2: Types of Steganography

Text Steganography: In this method the cover manuscript is twisted by producing random character sequences, changing words inside a text, by context-free syntaxes or by changing the arranging of anpresent text to hide the information. The cover text produced by this method can succeed for verbal steganography if script is linguistically ambitious.

Image Steganography: The image Steganography procedure is additionalprevalent in recent year than other steganography possibly since of the flood of electric image information

DOI: 10.13140/RG.2.1.2800.6001

obtainablethrough the arrival of digital cameras and extraordinary speed internet delivery. It can include hiding information in the obviouslyhappened noise within the picture. Most varieties of information comprise some thoughtful of sound. Noise mentions to the inadequacies characteristic in the procedure of translation an analog picture as aelectronicimage. In Image steganographycontainer hide memo in pixels of an image. An image steganographic scheme is one type of steganographicschemes, wherever the secret memo is hidden in a digital image with certain hiding method

Audio Steganography: The hiding of memos inside audio "noise" is additional area of info hiding that trusts on using an existing source as a space in which to hide info. Audio steganography can be difficult and can be valuable for conveying covert info in an innocuous protectionsound signal.[4]

Video Steganography: This is a method to hide any kind of files or infohooked on digital video arrangement. Video (mixture of pictures) is used as transferor for hidden info. Usually discrete cosine transforms (DCT) alteration standards (e.g., 8.667 to 9) which are used to hide the information in each of the images inside the video, which is not visible by the human iris. Video steganography uses such as H.264, AVI, Mp4, MPEG or other video setups.[5]

Types of Image steganography Techniques: This method can be divided into following domains.

Spatial Domain Methods: There are varioustypes of spatial steganography, all straight change certain bits in the image pixel standards in hiding information. Smallest significant bit (LSB)-based steganography is unique of the modestmethods that hides aundisclosed message inside the LSBs of pixel standardsdevoid of introducing many perceptible distortions. Variations in the significance of the LSB are unnoticeable for human eyes.

General advantages of spatial domain LSB technique are:

1. There is fewercasual for degradation of the novel image.
2. More information can be stored in an image.

Disadvantages of LSB method are:

1. Fewer robust, the hidden information can be misplaced with image manipulation.
2. Concealedinformation can be easily damaged by unassuming attacks.

Transform Domain Method: This is additional compound technique of hiding information in an image. Various algorithms and alterations are used on the image to hide info in it. Transform domain embedding can be termed as a domain of implantingmethods for which aamount of algorithms have been optional. The process of embedding data in the frequency sphere of a signal is considerablyrobust than embedding principles that operate in the time domain. Most of the robust steganography schemescurrently operate within the convert domain Transform domain techniques have an advantage over spatial domain methods as they hide info in parts of the image that are less exposed to compression, cropping, and image dispensation. Certain transform domain systems do not seem dependent on the image format and they may outrun lossless and lossy format conversions. [5]

Masking and Filtering: These techniques hide information by marking an image, in the similartechnique as to paper watermarks. These procedures embed the info in the more significant areas than just hiding it hooked on the noise level. The unseenmemo is more indispensable to the cover picture. Watermarking approaches can be practicaldeprived of the fear of picture destruction due to resident compression as they are additional integrated into the image.

Advantages of Covering and filtering Procedures: This method is abundant more strong than LSB replacement with respect to density since the info is hidden in the noticeable parts of the image.

Disadvantages: Techniques can be applied individual to gray scale imageries and limited to 24 bits.

Distortion Techniques: Distortion techniques need knowledge of the inventive cover image throughout the decoding procedure where the decoder purposes to check for differences between the original protection image and the distorted protection image in instruction to repair the secret message. The encoder adds a sequence of changes to the hiding place image. So, info is described as existence stored by signal distortion .Using this technique, a stego-object is created by spreadingaarrangement of alterations to the cover image. This arrangement of adjustments is use to match the top-secret message required to communicate .The memo is encoded at pseudo-randomly selected pixels. If the stego-image is unlike from the hiding residence image at the assumedmemo pixel, the memo bit is a "1." otherwise, the message bit is a "0." The encoder container adjusts the "1" worth pixels in such a manner that the arithmeticalpossessions of the image are not overstated.Though, the essential for distribution the cover image restrictions the welfares of this method.[6]

II. RELATED WORK

BingwenFeng et.al in 2014[7] described as, a binary image steganography arrangement that goals to minimize the implanting distortion on the texture is presented. They extracted the complement, revolution, and reflecting invariant local texture designs from the binary image first. The weighted sum of crmiLTPvariations when tossing one pixel is then working to measure the spinning alteration corresponding to that pixel.

VojtˇechHolub et.al in 2014[8] proposed a worldwide distortion design called worldwide wavelet qualified distortion that can be applied for entrenching in an arbitrary domain. The embedding distortion was computed as a sum of comparative

DOI: 10.13140/RG.2.1.2800.6001

changes of constants in a manoeuvring filter bank rottenness of the hiding place image. The directionality militaries the implantingvariations to such parts of the hiding place object that are problematic to model in multiple directions, such as traces or noisy regions, while avoiding smooth districts or clean edges.

Saiful Islam et.al in 2014[9] proposed a novel steganography method, where edges in the cover image have been used to surround messages. Amount of data to be embedded plays a significant role on the selection of edges, i.e., the more the quantity of data to be embedded, larger the use of weedier edges for embedding.

Dr.DiwediSamidha et.al in 2013[10]in this proposed many steganography methods can be used like Least Significant Bit, layout organization schemes, substituting individual l's or individual zero's from subordinate nibble from the byte are unhurried for hiding secret message in an image. Along with these systems, some more methods were proposed, grounded on selection of random pixels from an image and again secret data is hidden in accidental bits of these randomly designated pixels.

GeHuayong et.al in 2011[11] reviewed steganography and steganalysis based on digital image. Perception and principle of steganography and steganalysis were demonstrated. Spatial domain and transform domain inserting methods are generalized.

G. Prashanti et.al in 2015[12]In this paper, offers a analysis of recent realizations of LSB based spatial domain steganography that have an better steganography's ultimate objects, which are undetectable, robustness and capacity of hidden data. These methods can help researchers in empathetic about image steganography and numerous techniques of hiding data in an image. Laterally with this, two new methods are planned one for hiding secret message into cover image and the second is smacking a grey scale secret image into another grey scale image.

Rupesh Gupta et.al in 2014[13] In this paper, planned and they worked but as the impostors are acting quickly to hack information developers are also imaginary to invent new techniques to stop hacker's purposes. As per the basic information more is the PSNR value and lesser is the MSE consequences are better so, here in this paper they are signifying a new technique by examining three major safety systems that is cryptography, steganography and watermarking that will not only hide the evidence but produce better consequences.

Carlos Munuera et.al in 2014[14] In this paper describes as learning the application of Show codes to wet paper steganography. To that end, they suggest the use of decoding algorithms that do not verify the smallest distance property and current one of these algorithms. They revision its properties and show outcomes of some numerical experimentations.

Difference between Water marking, Steganography, Cryptography:

There are severalalterationsamong Steganography and Water marking, cryptography. The assessmentamong cryptography and Steganography is exemplified from the following:

Steganography:

1. Unknown message passing
2. Steganography prevents the discovery of existence of communication
3. Little known knowledge technology
4. Steganography does not alter the structure of the secret message

Cryptography:

1. Known message passing
2. Encryption prevents unauthorized persons from discovering the contents of communication
3. It is common technology
4. Cryptography alters the structure of the secret message [15]

Water marking:

1. compensated prediction, DCT
2. Yes, as actual message is hiding by some watermark
3. Capacity depends on the size of hidden data
4. Not easy to detect
5. Extend information and become an attribute of the cover image[16]

III. CONCLUSION

The different procedures of steganography. Each technique has a process of embedding for itself. Each processhave some advantages, and also disadvantages in contrast with other procedures of steganography. So it is not possible to say that a specified method is the best and finest off all. It is unbearable to determine the nastiest one we surveyed various types of steganography. We studied the various techniques. We can just compare them form different aspects, which results in determining a suitable method for a specific usage.

IV. REFERENCE

[1] Ahmed, Arif, NishantAgarwal, and Sean Banerjee. "Image steganography by closest pixel-pair mapping." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[2] Das, Rig, and ThemrichonTuithung. "A novel steganography method for image based on Huffman Encoding." Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on.IEEE, 2012.

DOI: 10.13140/RG.2.1.2800.6001

[3] Shelke, Falesh M., Ashwini A. Dongre, and Pravin D. Soni. "Comparison of different techniques for Steganography in images." International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN(2014): 2319-4847.
[4] Kaur, Navneet, and Sunny Behal. "A Survey on various types of Steganography and Analysis of Hiding Techniques."
[5] Hussain, Mehdi, and MureedHussain. "A survey of image steganography techniques." (2013).
[6] Mandal, Pratap Chandra. "Modern Steganographic technique: A survey."International Journal of Computer Science & Engineering Technology (IJCSET) 3.9 (2012): 444-448.
[7] (Feng, Bingwen, Wei Lu, and Wei Sun. "Secure binary image steganography based on minimizing the distortion on the texture." Information Forensics and Security, IEEE Transactions on 10.2 (2015): 243-255.)
[8] (Holub, Vojtěch, Jessica Fridrich, and TomášDenemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014.1 (2014): 1-13.)
[9] (Islam, Saiful, Mangat R. Modi, and Phalguni Gupta."Edge-based image steganography." EURASIP Journal on Information Security 2014.1 (2014): 1-14.)
[10] (Samidha, Diwedi, and Deepak Agrawal."Random image steganography in spatial domain." Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on. IEEE, 2013.)
[11] (Huayong, Ge, Huang Mingsheng, and Wang Qian. "Steganography and Steganalysis based on digital image." Image and Signal Processing (CISP), 2011 4th International Congress on.Vol.1.IEEE, 2011.)
[12] (Prashanti, G., and K. Sandhyarani. "A New Approach for Data Hiding with LSB Steganography." Springer International Publishing,Vol 2 ,2015.)
[13] (Gupta Rajesh, and TanuPreet Singh. "New proposed practice for secure image combing cryptography,steganography and watermarking based on various parameters." Contemporary Computing and Informatics (IC3I), 2014 International Conference on.IEEE, 2014.)
[14] (Munuera, Carlos. "Hamming codes for wet paper steganography." Designs, Codes and Cryptography 76.1 (2015): 101-111.)
[15] Thangadurai, K., and G. Sudha Devi. "An analysis of LSB based image steganography techniques." Computer Communication and Informatics (ICCCI), 2014 International Conference on.IEEE, 2014.
[16] Desai, Hardikkumar V. "Steganography, Cryptography, Watermarking: A Comparitive Study." Journal of Global Research in Computer Science 3.12 (2013): 33-35.