ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

A Review of Data Security through Reversible and Steganography Techniques

Neetu Narware[1], Nitesh Kumar[2], Keshav Mishra[3]

M.Tech Scholar, Department of Electronics and Comm. Engineering, SIRTS Engineering College, Bhopal, India[1]

Assistant Professor, Department of Electronics and Comm. Engineering, SIRTS Engineering College, Bhopal, India[2]

Associate Professor, Department of Electronics and Comm. Engineering, SIRTS Engineering College, Bhopal, India[3]

ABSTRACT: Due to the evolution of digital communication, computer technologies and the internet, the security of information considers as the most challenges in communication to secure useful data. A large variety of reversible and stenographic techniques exists for hiding or secures data such as text, image, audio, video, and protocol, and can be sent to a receiver secretly. This paper reviews various existing approach based on reversible and steganography approaches. Steganography approach is most suitable for bulky data so such approach is used in various applications.

KEYWORDS: Energy efficient algorithm; Manets; total transmission energy; maximum number of hops; network lifetime

I. INTRODUCTION

Reversible data hiding (RDH) is a technique that hides data into a digital media reversibly, which is used to carry additional data with an imperceptible way. With the RDH technique, the hidden messages can be extracted accurately, and the original image can be recovered losslessly. RDH is useful in the applications of labeling digital images. In cloud storage, the server can embed additional data, e.g., timestamps, labels, user information and remarks, into images uploaded by the users. As the messages are attached inside the images, the server can achieve a better management and save the storage overheads. Besides, the original content can be exactly recovered before the users' downloading. [1].

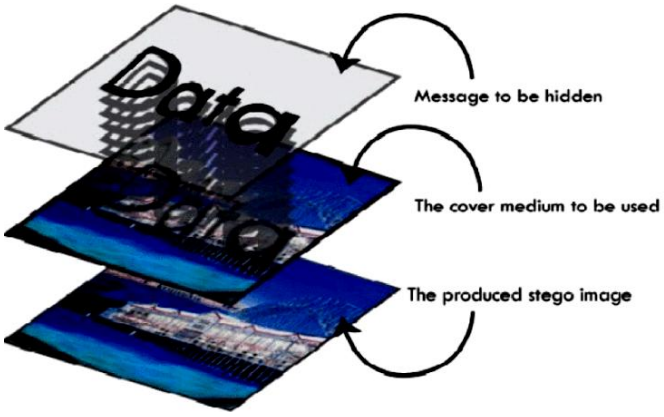

Figure 1: Data Hiding

Steganography is the science of hiding data within other data. These data could be text, image, audio or video. The main aim of steganography is to conceal a secret data into a host media for confidentiality. Therefore, steganography

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

provides secure communication through multimedia. Moreover, steganography can be used as a tool for multimedia encapsulation, in which one media is inserted in another media. Hence, multimedia encapsulation provides secure transfer of its metadata from one device to another. Figure 1 illustrates the main concept of steganography. As shown in the figure, steganography hides secret data, resulting in the bottom stego image, in a way that is not visible by the human eyes [2].

II. RELATED WORK

Q. Ying et al., [2019] Traditional reversible data hiding (RDH) focuses on enlarging the embedding payloads while minimizing the distortion with a criterion of mean square error (MSE). Since imperceptibility can also be achieved via image processing, we propose a novel method of RDH with contrast enhancement (RDH-CE) using histogram shifting. Instead of minimizing the MSE, the proposed method generates marked images with good quality with the sense of structural similarity. The proposed method contains two parts: the baseline embedding and the extensive embedding. In the baseline part, we first merge the least significant bins to reserve spare bins and then embed additional data by a histogram shifting approach using arithmetic encoding. During histogram shifting, we propose to construct the transfer matrix by maximizing the entropy of the histogram. After embedding, the marked image containing additional data has a larger contrast than the original image. In the extensive embedding part, we further propose to concatenate the baseline embedding with an MSE-based embedding. On the recipient side, the additional data can be extracted exactly, and the original image can be recovered losslessly. Comparing with existing RDH-CE approaches, the proposed method can achieve a better embedding payload.[1]

R. Wazirali et al., [2019] In stenography, embedding data within an image has a trade-off between image quality and embedding capacity. Specifically, the more data are concealed within a carrier image, the further distortion the image suffers, causing a decline in the resultant stego image quality. Embedding high capacity of data into an image while preserving the quality of the carrier image can be seen as an optimization problem. In this paper, we propose a novel spatial steganography scheme using genetic algorithms (GAs). Our scheme utilizes new operations to increase least significant bits (LSB) matching between the carrier and the stego image which results in increased embedding capacity and reduced distortion. These operations are optimized pixel scanning in vertical and horizontal directions, circular shifting, flipping secret bits and secret data transposing. We formulate a general GA-based steganography model to search for the optimum solutions. Finally, we use LSB substitution for data embedding. We conduct extensive experimental testing of the proposed scheme and compare it to the state-of-art steganography schemes. The proposed scheme outperforms the relevant GA-based steganography methodologies.[2]

C. Yu, et al., [2018] Reversible data hiding is an important topic of data hiding. This work proposes a novel separable and error-free reversible data hiding in an encrypted image based on two-layer pixel errors. Specifically, the proposed scheme divides the original image into a series of non-overlapped blocks and permutes these blocks. Then, a closed Hilbert curve is used for scanning each block to obtain a one-dimensional pixel sequence. The pixels of the sequence are encrypted with key transmission. During data hiding, each non-overlapped block of the encrypted image is scanned in the closed Hilbert order to generate a one-dimensional encrypted pixel sequence. Finally, it exploits the histogram of two-layer adjacent encrypted pixel errors to embed secret data by histogram shifting and generate a marked encrypted image. Many experiments are carried out, and the results demonstrate that the proposed scheme reaches a high payload and outperforms some reversible data hiding schemes in the encrypted image.[3]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

A. Aryal et al., [2017] This work proposes a Block-Permutation-Based Encryption (BPBE) method with Reversible Data Hiding (RDH). In the proposed algorithm, Histogram Shifting (HS) is used for RDH, and the BPBE method is utilized for encryption. The BPBE method performs four processes for encryption, namely, block scrambling, block rotation/inversion, negative-positive transformation, and the color component shuffling. The proposed algorithm is implemented on the concatenated image from a large database. Therefore, the number of the divided blocks can be increased, and the color scrambling of the encrypted image is increased. Consequently, the resistance against Jigsaw Puzzle Solvers (JPSs) could be improved. This algorithm consists of different hierarchical steps for the data embedding and the encryption. Therefore, the proposed algorithm can be suitable for the hierarchical access control system, where the permission is granted according to the various access rights.[4]

R. J. Mstafa et al., [2017] This work analyze the video steganography technique, which is used to ensure national security and the confidentiality of the information of governmental agencies and enterprises. Videos may be used to transmit secrets and conduct covert communication. As such, we present an algorithm based on a secret sharing scheme and an Error-Correcting Code (ECC), which combines Grey Relational Analysis (GRA) with a partition mode in video compression standard H.264/AVC. First, we process secret information by secret sharing, and then use an ECC to process the obtained information. Moreover, we choose the Discrete Cosine Transform (DCT) blocks using GRA, and then use rules to hide the pretreated information in DCT coefficients of the video frames. Experimental results indicate that our algorithm has good invisibility, better robustness, good anti-steganalysis ability, and little influence on the bit rate of the video carrier. In addition, the bit error rate is low after attacks such as noise, filtering, or frame loss in the simulation environment.[5]

Y. Zhang et al., [2017] Over the past few decades, the art of secretly embedding and communicating digital data has gained enormous attention because of the technological development in both digital contents and communication. The imperceptibility, hiding capacity, and robustness against attacks are three main requirements that any video steganography method should take into consideration. In this paper, a robust and secure video steganographic algorithm in discrete wavelet transform (DWT) and discrete cosine transform (DCT) domains based on the multiple object tracking (MOT) algorithm and error correcting codes is proposed. The secret message is preprocessed by applying both Hamming and Bose, Chaudhuri, and Hocquenghem codes for encoding the secret data. First, motion-based MOT algorithm is implemented on host videos to distinguish the regions of interest in the moving objects. Then, the data hiding process is performed by concealing the secret message into the DWT and DCT coefficients of all motion regions in the video depending on foreground masks. Our experimental results illustrate that the suggested algorithm not only improves the embedding capacity and imperceptibility but also enhances its security and robustness by encoding the secret message and withstanding against various attacks.[6]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

Table 1: Summary of Literature Review

S.No.	Authors	Technique	Description
1	Q. Ying et al.,	Novel method of RDH with contrast enhancement	Achieve a better embedding payload
2	R. Wazirali et al.,	A novel spatial steganography scheme using genetic algorithms	Outperforms the relevant GA-based steganography methodologies
3	C. Yu, et al.,	Novel separable and error-free reversible data hiding	Reaches a high payload
4	A. Aryal et al.,	Block-Permutation-Based Encryption (BPBE) method with Reversible Data Hiding	Suitable for the hierarchical access control system,
5	R. J. Mstafa et al.,	Algorithm based on a secret sharing scheme and an Error-Correcting Code	Good invisibility, better robustness, good anti-steganalysis ability,
6	Y. Zhang et al.,	Robust and secure video steganographic algorithm in discrete wavelet transform	Enhances its security and robustness

III. REVERSIBLE INFORMATION HIDING METHOD

Extra message are insert into some cover media, like military or medical pictures, in an exceedingly reversible manner so the first cover content are often absolutely repaired when extraction of the hidden message is termed reversible information hiding. General signal process generally takes place before encoding or when cryptography. Generally the content owner doesn't believe the supplier of the service, in such cases ability to supply manipulating the plain content secret is undesirable. Thus manipulation on encrypted information once keeping the plain content is allowed. Because of the restricted channel resource a channel supplier with none data of the cryptography key might compress the encrypted information, once the key information to be transmitted. So as to confirm the privacy the content owner ought to cipher the information once it share a secret image with alternative person. Some info's like the origin information, image notation or authentication information, and is wish to be superimposed among the encrypted image by a channel administrator who doesn't understand the first image content. At receiver side it should be additionally expected that the first content are often recovered with none error when cryptography and retrieve of extra message. Meaning a reversible information hiding theme for encrypted image is desirable. Information hiding is that the method of concealing the information into covers media. That is, the information hiding method links a collection of the embedded information and a collection of the quilt media data. In most cases of information hiding, the first image becomes distorted because of information hiding and can't be inverted back to the first media. That is, cover media has permanent distortion even when the hidden knowledge is removed. In some applications, like diagnosis and enforcement it's desired that the first cover media are often recovered expeditiously with no loss. The marking techniques satisfying this demand are referred to as reversible, lossless, distortion-free or invertible information hiding techniques [3].

Reversible information hiding (RDH) Message this could be done by choosing an encoding key that is use to encode the initial data once encrypting the data or information hiding secret is used and this information hiding secret is embedded on the encrypted data with the assistance of information hider block and this encrypted information containing embedded data is forward the channel .This will received by image decoding which will decode the received information and by this decode data the initial data is extracted by activity the reverse operation by using an equivalent encode key[4].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

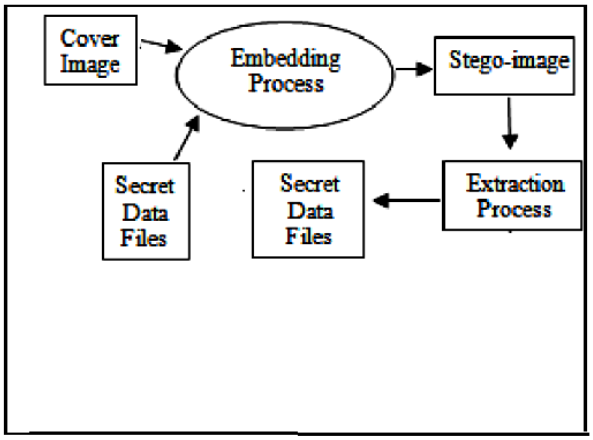

Figure2: Reversible information hiding method

IV. STEGANOGRAPHY METHOD

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[3]

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned both with concealing the fact that a secret message is being sent and its contents.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

Discussions of steganography generally use terminology analogous to and consistent with conventional radio and communications technology. However, some terms appear specifically in software and are easily confused. These are the most relevant ones to digital steganographic systems:

The payload is the data covertly communicated. The carrier is the signal, stream, or data file that hides the payload, which differs from the channel, which typically means the type of input, such as a JPEG image. The resulting signal, stream, or data file with the encoded payload is sometimes called the package, stego file, or covert message. The proportion of bytes, samples, or other signal elements modified to encode the payload is called the encoding density and is typically expressed as a number between 0 and 1. In a set of files, the files that are considered likely to contain a payload are suspects. A suspect identified through some type of statistical analysis can be referred to as a candidate.

V. CONCLUSION AND FUTURE WORK

A study on various reversible data hiding techniques is performed in data hide. Reversible data hiding schemes for encrypted image with a less PSNR computation is analyzed, that consists of image cryptography, data activity and data extraction/ image recovery phases the initial pictures are encrypted by a cryptography strategy. But the reversible and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit:www.ijirset.com

Vol. 8, Issue 12, December 2019

steganography both approach are suitable for bulky data secure in digital communication environment. This paper discussed various previous research works of both techniques. In future both techniques can be used as a cascaded or in hybrid form sothat data would be more secure as well as improvement quality, SNR etc parameters.

REFERENCES

1. Q. Ying, Z. Qian, X. Zhang and D. Ye, "Reversible Data Hiding With Image Enhancement Using Histogram Shifting," in *IEEE Access*, vol. 7, pp. 46506-46521, 2019.
2. R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud and A. Alhindi, "An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms," in *IEEE Access*, vol. 7, pp. 133496-133508, 2019.
3. C. Yu, X. Zhang, Z. Tang and X. Xie, "Separable and Error-Free Reversible Data Hiding in Encrypted Image Based on Two-Layer Pixel Errors," in *IEEE Access*, vol. 6, pp. 76956-76969, 2018.
4. A. Aryal, S. Imaizumi, T. Horiuchi and H. Kiya, "Integrated algorithm for block-permutation-based encryption with reversible data hiding," *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Kuala Lumpur, 2017, pp. 203-208.
5. R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," in *IEEE Access*, vol. 5, pp. 5354-5365, 2017.
6. Y. Zhang, M. Zhang, X. Yang, D. Guo and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC," in *Tsinghua Science and Technology*, vol. 22, no. 2, pp. 198-209, April 2017.
7. Z. Yin, A. Abel, X. Zhang and B. Luo, "Reversible data hiding in encrypted image based on block histogram shifting," *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, 2016, pp. 2129-2133.
8. F. Huang, J. Huang and Y. Shi, "New Framework for Reversible Data Hiding in Encrypted Domain," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2777-2789, Dec. 2016.
9. Z. Qian, X. Zhang and G. Feng, "Reversible Data Hiding in Encrypted Images Based on Progressive Recovery," in *IEEE Signal Processing Letters*, vol. 23, no. 11, pp. 1672-1676, Nov. 2016.
10. Y. Shi, X. Li, X. Zhang, H. Wu and B. Ma, "Reversible data hiding: Advances in the past two decades," in *IEEE Access*, vol. 4, pp. 3210-3237, 2016.
11. W. Zhang, H. Wang, D. Hou and N. Yu, "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation," in *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469-1479, Aug. 2016.