International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 190-194 www.ijaem.net ISSN: 2395-5252

A Review Paper on an Efficient Data Hiding Based on Most Significant Bit in Image

Ms. More S. M

Submitted: 01-07-2022 Revised: 04-07-2022 Accepted: 08-07-2022

ABSTRACT: In last few decades data hiding is crucial work. A lot of agencies are work to different technology to develop new concept for data hiding. To share public or private sector sensitive information we must implement few data manipulating technology. In Technology primary is 1. Cryptography, 2.Steganography, 3. Digital signature and last one is watermarking. To main aim protect sensitive information to t hacker, spammer, or any unknown person who cannot part of data. To increase data hiding ratio and share data with security we survey on existing techniques where we find image steganography using LSB techniques. But it techniques has generate noise of image where hacker can easily analyze or thinking here something is wrong. So we study on image steganography in various techniques.

I. INTRODUCTION

In computer vision depends upon machine language. the machine language is combination of one and zero. In computer every bit or letter has contain a specific ascii value which can convert into machine language for understand computer. In starting phase develop the 8bit length ascii value computer. it increase continuously and currently 64 bit version are available. The all computer techniques depends upon one,zero (1,0) binary value. So any person find any algorithm or techniques to work on machine learning language with different software or different object oriented a language.

So we are say to hide data then we compulsory thing to manipulate sensitive information and changes in ascii value to convert normal text to abnormal text. To generate abnormal text we implement some Gate like AND gate, NAND gate, Negation etc. To using all gate , implement different types of concept. The data hiding has mainly 4 techniques are available.

1. Cryptography:

The cryptography has available plaintext and cipher text value. Plain text has owner original value which can hide. The Cipher text is a text which generate processing on plain text. To processing generate different algorithm are available AES (Advance Encryption diagram.) , DES, ECC etc. In cryptography has one concept which is called as key generation. Without using key generation not a single algorithm can run. In starting phase 8 bit key generationalgorithm available. The currently in market 256 bit key available.

2. Steganography:

In steganography has large amount of data hide into respected image. The hide information to calculate image size and calculate how many text are hide. The data processing is calculate how many pixel are available and how many textual data bit is hide using LSB Techniques.

The Main drawback of steganography image has lengthy. Because textual data convert into ASCII value as well as binary value. Using LSB Techniques replace every binary value bit into every pixel. So as a common calculation every single character convert into 8bit length binary value. If we replace value into pixel then required 8 pixel in image. So image pixel size required long.

3. Digital Signature:

It is mathematicalcalculation used to authenticity and integrity checking of document, file, and software details. It is ensure electronic document authentic. Authentic means we are know who is created document and its has not altered the owner of document. The signature has used to public key encryption using RSA algorithm. Its has a public key available to owner which is encrypted file and decrypted. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 190-194 www.ijaem.net ISSN: 2395-5252

electronic document, transaction or message, as well as acknowledging informed consent by the signer.

4. Watermarking:

Watermarking and steganography concept are same but it has a small differences. A both are hide information in sound, image and video as multimedia data. But steganography are hide information in invisible format. If any user hide information then it cannot seen to other but it available. Same things is reverse in watermarking concept data are combine and which can easily show the user. for example two images are combine and generate third combine image. Generate a classic video which collection of different and images and any music sound. These are all combine into watermarking. But watermarking concept are not hiding process so we cannot continue.

II. RELATED WORK

Digital image sometimes needs to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. an algorithm to reversibly embed secret data in encrypted images is presented, which consists of image encryption, data embedding and data extraction three phases. A stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels, which results in high-level of security. The data-hider can embed the secret data into the encrypted image by using histogram shifting and difference expansion, even though he does not know the original image content. Since the embedding process is done on encrypted data, our scheme preserves the confidentiality of content. Two capacity dependent parameters are introduced to flexibly adjust the embedding capacity according to the specific application at hand. Data extraction is separable from image decryption, i.e., the additional data can be extracted either in encrypted domain or decrypted domain.

Instead of embedding data in encrypted images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating errors. A benchmark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the original image. Moreover, the data extraction and image recovery are free of errors for all images.

A RDH method for encrypted images by shifting the encrypted histogram of predicted errors, and achieves excellent performance in three aspects: complete reversibility, higher PSNR under given embedding rate, separability between data extraction and image decryption. Our method can work on two schemes independently in order to suit different application prospects by extracting the data from the encrypted image or from the decrypted image.

A novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separability property of RDH methods in encrypted images. Compared to state-of-the-art alternatives, the room vacated for data hiding by our method is much larger used. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. The data extraction and cover image recovery are separable, and are free of any error. Experimental results on three datasets have demonstrated that our average MER can reach 1.7 times as large as the previous best alternative method provides.

Introduces two reversible data hidingapproaches in encrypted images by using prediction error: a joint method and a separable method. For the first method, data extraction and image recovery algorithms are performed jointly. While comparing to related joint methods improved reversibility, smaller number of incorrect extracted bits, better visual quality of lossy reconstructed image are obtained by the proposed method, especially when high embedding rate is used. For the second method, data extraction and image recovery algorithms are separable.

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

An efficient RDH scheme based on pairwise PEE is proposed. The pairwise PEE is a novel reversible mapping that utilizes the correlations among predictionerrors. With the help of this type of correlations, the distortion can be controlled at a low level, and thereby the proposed

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 190-194 www.ijaem.net ISSN: 2395-5252

scheme outperforms some state-of-the-art RDH.

We have focused on proposing a novel RGVSS scheme by skillfully designing a procedure of distinguishing different light transmissions on shared images based on the pixel values of the logo image. The proposed FRGVSS scheme was aimed at solving the problem of pixel expansion and unfriendly management to meaningful shared images.

A generalized LDE framework was proposed by incorporating merits of the GSQH and the histogram-based embedding. In comparison with the existing LDE methods, the proposed one has better utilized the statistical characteristics of images and achieved better adaptability, flexible capacity control, and higher security. Thorough experimental studies show that this framework performs better than the conventional LDE methods based on the GH, and the method simply using the AADH.

The consecutive higher bit-planes having compression ratio less than 1 while using run-length coding with Elias-Gamma encoding scheme is considered. The compressed bits will be pseudorandomly distributed in the same bit-plane, and the space created as a result of compression has been used to hide the secret message bits. Finally, the modified bit-planes are combined to generate the encrypted image. Experimental study shows that the proposed scheme outperforms the existing schemes in terms of embedding rate without compromising encryption efficiency.

A novel scheme of reversible data hiding (RDH) in encrypted images using distributed source coding (DSC). After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make room for the secret data. The selected bit series is Slepian-Wolf encoded using low density parity check (LDPC) codes. On the receiver side, the secret bits can be extracted if the image receiver has the embedding key only. In case the receiver has the encryption key only, he/she can recover the original image approximately with high quality using an image estimation algorithm. If the receiver has both the embedding and encryption keys, he/she can extract the secret data and perfectly recover the original image using the distributed source decoding.

A video in which data is embedded is referred as a cover video and the video which is used for carrying secret data is termed as stego video. Video Steganography consists of the reversible and irreversible scheme. The reversible scheme has the ability to embed the secret data into a video and then recover the video devoid of losing any information when the secret data is extracted. The robustness of video code streams are maintained by designing Enhanced Most Significant Bit Irreversible method. After improving the robustness value, polynomial hashing in AIRFT technique achieves higher security on video steganography. Vector quantization model improves the performance level on video code streams without compromising the video quality. Our research work on steganography focuses on images, audio, and video as cover media.

Introducing new challenge is always as important as keeping it unreachable to the hacker. In proposed work security is enhanced by encrypting data and then embedding the encrypted form of data. Reserve Room before encryption gives an added advantage for enough space for data hiding. Haar wavelet is best suitable wavelet amongst other wavelet like symlet, bior, coiflet and contourlet, when the input image is encrypted image rather than a plain image. The quality of image has been evaluated by performance analysis like MSE, PSNR and hiding capacity on different types of color images and results were compared.

III. METHODOLOGY

1.File Store

This is first phase after the user authentication from the system. The file will be stored on the local file system. User can upload the images which he wants to store in to system and going to be used for storing the secrete information.High quality images are used.

2. Encryption

The next and important phase is encryption of message. The messages are encrypted by using encryption algorithms such as AES.

3.Key Generation

By using public keys then new secrete key will be generated and which used to encrypt the message.

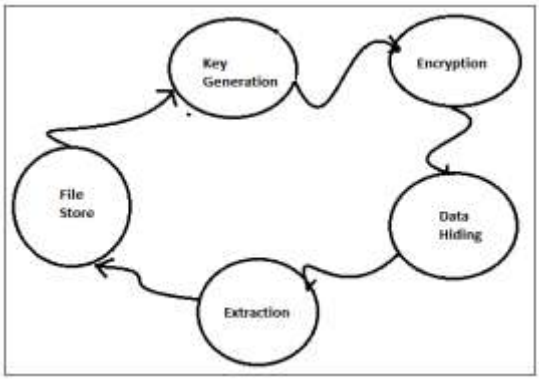

fig 1. Methodology

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 190-194 www.ijaem.net ISSN: 2395-5252

4.Data Hiding

Embedding of secrete information into images is called data hiding.Our proposed methodology used to more secure embedded data to hiding data implement Steganography plus cryptography concepts. We implement RDHEI means Reverse Data Hiding in Encrypted Images. Here we propose a new reversible method based on MSB (most significant bit) prediction with a very high capacity. We present two approaches, these are: high capacity reversible data hiding approach with correction of prediction errors (CPEHCRDH) and high capacity reversible data hiding approach with embedded prediction errors (EPE-HCRDH).

5.Extraction

The Extraction is done by using the reverse processing used at time data hiding phase.

6.Image Recovery:

In after recover message we get the encrypted format images. We apply decryption of AES algorithm to recover image. To recover image we implement private key which generated to key generation algorithm for encrypted image. In decryption process loss some pixel of image and we got 70% recover image.

IV. CONCLUSION

The data hiding is more sensitive issue in last few years. Every people want to our personal space share data or confidential. In existing survey we find out some interesting techniques which are work properly but its has some disadvantages. 1. In multimedia encryption process data has loss. 2. In steganography process data is recover but in multimedia has find some noise to hacker easily analysis something is wrong. 3. If we use steganography + cryptography process then data cannot recover 100%, Some data are loss. 4. Watermarking techniques is good but it has not data hiding concept it just data combining concept.

REFERENCES

[1]. Dawen Xu a,n, Rangding Wang, "Separable and error-free reversible data hiding in encrypted images", School of Electronics and Information Engineering, Ningbo University of Technology, Ningbo 315016, China.

[2]. Weiming Zhang n , Kede Ma, Nenghai Yu, "Reversibility improved data hiding in encrypted images", School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China.

[3]. Xiaochun Cao, Senior Member, IEEE, Ling Du, Xingxing Wei, Dan Meng, Member, IEEE,andXiaojieGuo, Member, IEEE, "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation", IEEE TRANSACTIONS ON CYBERNETICS 2015.

[4]. Xiaotian Wu a, Wei Sun, "High-capacity reversible data hiding in encrypted images by prediction error", School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China.

[5]. Wien Hong, Tung-Shou Chen, and Han-Yan Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 4, APRIL 2012.

[6]. 6.Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li, " Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, MARCH 2013.

[7]. Bo Ou, Xiaolong Li, Yao Zhao, Senior Member, IEEE, Rongrong Ni, Member, IEEE, and Yun-Qing Shi, Fellow, IEEE, "Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 12, DECEMBER 2013.

[8]. Tzung-Her Chen and Kai-Hsiang Tsao, "User-Friendly Random-Grid-Based Visual Secret Sharing", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 11, NOVEMBER 2011.

[9]. Xinbo Gao, Senior Member, IEEE, Lingling An, Yuan Yuan, Senior Member, IEEE, Dacheng Tao, Member IEEE, and Xuelong Li, Senior Member, IEEE, "Lossless Data Embedding Using Generalized Statistical Quantity Histogram", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 8, AUGUST 2011.

[10]. V. M. Manikandan and V. Masilamani, "A Novel Reversible Data Hiding Scheme that Provides Image Encryption", Journal of Image and Graphics, Vol. 6, No. 1, June 2018.

[11]. Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Encrypted Images With Distributed Source Encoding", 26(4):1-1 · January 2015.

[12]. Pankajgarg, "High capacity data hiding techniques for digital images", 2014.
[13]. Dr. Umadevi, "Video steganography technique for robust multimedia communications using emsbi, airft and apvq method", International Journal of Advance Engineering and Research Development Volume 4, Issue 11, November -2017
[14]. Khan AmrinNaaz, Imdad Rizvi, M.M. Kadam,"Performance Analysis on Different Images using Reversible Data Hiding Technique and its Application", International Journal of Computer Applications,Volume 129 – No.16, November2015
[15]. T. S.Sandeep #1 , J. Shankar babu *2, Dr.N. Sudhakar Reddy, "A Pragmatic Approach in Lossless Data Hiding for JPEG Images", International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 1- Jan 2014.