Reversible Data Hiding In Encrypted Image

Anita Harsoor, Kalpana Hangargi, Prakash Pattan

Abstract: ***Today, digital communication has become an integral part of everyday life. Many applications are based on the Internet and communications must be made in secret. This is especially important when confidential information needs to be exchanged. As a result, the security of information transmitted over public channels is a fundamental problem, and as a result, the confidentiality and integrity of the data is essential to protect against unauthorized access and use. This caused the information concealment area to become unstable. Encryption and steganography are two of the most common methods you can use to ensure safety. With encryption, the data is converted to another form of gibberish and the encrypted data is transmitted. In Steganography, the image is transferred to the image, which is embedded in the image without affecting the quality of the image.This article suggests a new way to embed data into images and edit data using common virtual built-in technologies.***

Index Terms—Data hiding, encrypted image, image recovery, reversible data hiding,Separable Reversible Data Hiding.

I. INTRODUCTION

Computers and the Internet are the main communication medium that connects different parts of the world to one global virtual world in modern society. As a result, people can easily exchange information and distance is no longer a communication barrier. It will probably be a security issue for long distance communications. This is really important for confidential data. The solution to this problem leads to the development of a steganography plan. Steganography is a very powerful security tool that provides a high level of security, especially when associated with encryption. Encryption and steganography are well known and widely used technologies that manipulate information and encrypt or hide each entity. Encryption encrypts the message to make it unintelligible. Steganography hides the message from being seen. While both technologies provide security, research is underway to combine encryption and steganography methods in a single system to enhance privacy and security.

Send feedback
History
Saved
Community.

A. Cryptography and Steganography

Encryption is a method of storing and transferring certain types of data, so that only intended users can read and process it. The cryptographic system can be broadly categorized as a symmetric key system using a single key for both sender and receiver, a public key system using both keys, a public key known to all, and a private key recipient of the message [1] () Is used. Common terms used in encryption are: 1) Plain text
2) Encrypted text
3) Encryption
4) Decryption
5) Key.

For example, if secret data to be transmitted is encrypted, channel providers who have no knowledge of the encryption key tend to compress the encrypted data due to limited channel resources. Encrypted binary images can be compressed without loss by detecting the low density parity check code syndrome [1], but encrypted gray image lossless compression method compatible with sequential decomposition and turbo puncturing codes The flow is developed in [2]. Using the lossy compression method proposed in [3], the encrypted gray image can be effectively compressed by ignoring excessive coarse information from the coefficients generated from the orthogonal transformation. When compressing data, the receiver can reconstruct the main content of the original image by retrieving the count value. Conversion calculations in encrypted domains have also been studied. Based on the similarity characteristics of the basic cryptosystem, a discrete Fourier transform can be implemented in the encrypted domain [4]. In [5], a composite signal representation method that combines multiple signal samples and treats them as a single sample is used to reduce the computational complexity and size of the encrypted data. There is also a certain amount of work on hidden data in encrypted domains. Buyer Cellular Protocol Watermark [6], a digital media product provider, encrypts and integrates original data with an encrypted fingerprint public key switch provided by an encrypted domain buyer. After decrypting with a private key, the buyer can get a watermarked product. This protocol allows the seller to find the version watermark of the buyer, although the buyer does not know the original version. Okamoto-Uchiyama has been proposed to improve the speed of greetings using encryption methods [7]. Encryption of public keys by homomorphic complex signal overload calculation The introduction of a mechanism to express large communication bandwidth is greatly reduced [8]. In this case, the data is encrypted and the confidentiality of the data is protected. For example [9].

II. LITERATURE REVIEW

In paper [1] The Generative Topographic Mapping (GTM) algorithm is proposed as a stochastic reconstruction of the SOM (self-organizing map). The GTM algorithm captures the data structure by modeling nonlinear transformations into a multidimensional data space

Revised Manuscript Received on july 10 , 2019.

Kalpana Hangargi, Computer Science and Engineering, PDACE, Kalaburgi, India.
Dr.Anita Harsoor, Computer Science and Engineering, PDACE,Kalaburgi, India..
Dr.Prakash Pattan, Computer Science and Engineering, PDACE, Kalaburgi, India.

that can be used as a visualization tool in a small dimension of potential variable space. The purpose of this white paper is to extend the GTM algorithm to handle multivariate time series. The standard GTM algorithm assumes that the data is independent samples and equally distributed. However, i.i.d. This assumption is clearly inappropriate for time series. In this paper, we propose an extension of GTM for multivariable time series called GTM-ARHMM, which assumes that the time series are generated by the ARCHMM which is hidden by autoregressive.

In this paper [2], the main motivation in normal steganography is to maintain a high-quality stegano-graphic image without a doubt. Sometimes it is important that the hidden image quality is maintained. The way to get high quality hidden images is the motivation of this work. To solve this problem, prior to the masking procedure, the pixels of the secret image are analyzed to generate an optimal codebook. The most common pixel values are encoded with the shortest code to minimize stego image distortion. In addition to testing the logo for a simple hidden image distortion for evaluation, we also tested high resolution images. Using the proposed method, PSNR values of more than 45.6 dB were obtained in the still image even for high-resolution hidden images. PSNR of confidential images after recovery was more than 50dB. We can conclude that the proposed method can provide good results regardless of the type of hidden image.

In this paper [3], Copyrights Variations (CNVs) are an important genetic component in human disease studies. While re-sequencing the entire high-efficiency genome provides multiple data sources for NVC detection, the computer algorithms must be adapted to different types or sizes of NVCs depending on different experimental models. A hidden Markov model has been implemented to obtain the optimal output and resolution of CNV detection in shallow areas. A new aspect of the algorithm is the inference of the probability of performing deletions jointly in different regions. By integrating all relevant information into the complete model, this method can detect medium depth (100-2000 bp) with low depth (this method applies to simulated data and medium size deletion.

In this paper [4] Steganography, a data concealment technology, is becoming increasingly important for the development of Internet communications. As a result, a variety of steganographic algorithms have recently been proposed (eg, Ni et al.) We developed a lossless data masking algorithm based on histogram modification. To increase the Ni algorithm by random permutation and histogram re-quantization to increase it, it is not easy to break security with a random attack by applying random permutation, and by adopting histogram re-quantization, the integrated capacity can be multiplied by about 3. When we approach, it is visually impossible to distinguish between images and stegoimage.

In this paper [5] The Internet is always vulnerable to unauthorized interception from around the world. The importance of reducing the amount of information detected during transmission is becoming a problem today. Decryption is the solution to the problem, but when the password is decrypted, the secret of the information no longer exists. Data masking for confidentiality, Copyright protection of digital media. Importance is also given to the use of technology used to process information. A traditional LSB modification technique that distributes message bits randomly in an image and makes it more difficult for unauthorized people to retrieve the original message is a secret. We propose a procedure for masking and extracting data for AVI video (audio / video interleaving) incorporating secret message bits into the higher order DCT coefficients. There is confidential information here. Grayscale pixel values are converted to binary values and incorporated into this value from the higher order coefficient values of the DCT of the AVI video image. Data masking and extraction procedures have been successfully tested. Other experiment results are shown here. All experiments are performed using Matlab 2010a simulation software.

III. METHODOLOGY

The proposed method consists of 4 steps. Image encryption, data modification, data integration, image search and data extraction. The content owner encrypts the cover image using an encryption key. The data owner uses the encrypted image to insert information (image or text). The encryption key is securely obtained by the recipient using an appropriate key exchange protocol based on the RSA algorithm. The virtual embedding of information extracts pixel indices corresponding to the bits of data and is performed by the data manager and generates a data extraction key. This extraction key is encrypted using the public key generated by RSA and sent to the recipient. If the recipient has a data extraction key, the original data can be retrieved. If the recipient has an encryption key, the original image can be recovered. If the receiver has two keys, you can get data and images. A block diagram of the transmitter side and the receiver side is shown in Figs.3. 1 and 3.2, respectively

IV. IMPLEMENTATION MODULES

Encryption requires that you apply a special mathematical algorithm that uses a key to transform the data into encrypted code before passing it. Decryption is the reverse of the encryption to retrieve the original data from the encrypted code. In this document, the cover image is encrypted using modular additional encryption technology. The key sequence for encryption is generated using an annotation shift register (FSR).

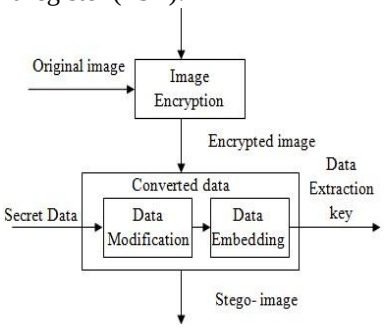

Fig 4.1: Architectural Diagram of the sender side

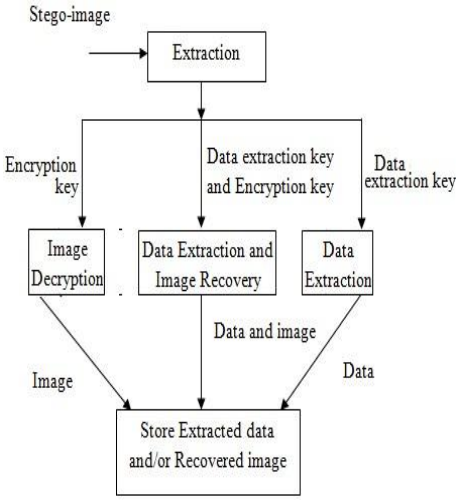

Fig 4.2: Architectural Diagram of the receiver side

Generator FSR uses the initial key called initial value / initial value (IV) to generate the key sequence. The generated initial value is shared between the sender and recipient. Each pixel in the image is encrypted using mod 256 additives to produce encrypted text. On the receiving side, a decryption algorithm is used in which the key sequence is generated by FSR, as mentioned above. The decryption method uses this key sequence as a backward key to recover the original image.

Consider a color image of size M * N. Each pixel has red, green, and blue components with values between [0-256]. Each color component consists of 8 bits and each pixel consists of 24 bits.

The initial start value is regarded as S1 S2 S3 ... Sn. The length varies from 8 to 12 digits. The seed's largest starting value is the encryption value and the new value is calculated. Then move the value to the left and place it on the right.

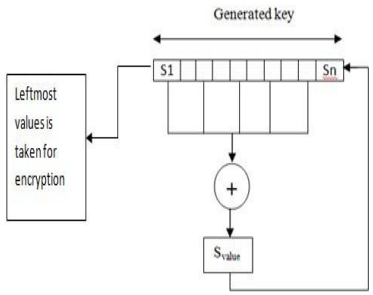

Fig 4.3: Key usage for encryption

A. Data Modification

In this technique, the amount of data that can be masked in the cover image can be increased. In addition, to enhance data protection, this technique incorporates an integrated encryption technique. A 24-bit color image will be used as a cover image, 8 bits each representing three basic colors: red green and blue. The embedding operation will be based on a technique of incorporating messages by bits. All characters in the message will be processed with their 8-bit ASCII codes, and the codes will be converted to 5-bit code using the MLSB technique [8]. Then, the 5-bit code will be integrated into the LSB of the image using the LSB method. When looking for an ASCII representation, we can note that the representation of lowercase letters (hexadecimal) will be between 61h and 7Ah, that of capital letters between 41h and 5Ah and the number between 30h and 30h.In the case of a lowercase letter, if its binary representation is considered to have the last four bits, it will be "0110" or "0111". For capital letters, the last four bits will be "0100" or "0101". As we can see, the last three bits are identical, so we can ignore them. For numbers, the last 4 bits will be identical, so that it can be represented with a single bit. Thus, the last 3 bits can be eliminated. In this way, each character can be represented with 5 bits.

To distinguish between lowercase letters, uppercase letters, numbers, and special characters, you can use a control symbol that defines the status of the next character. For this we use a control symbol that can define the state of the next character. The control symbols will also be 5 bits. In the 5-bit representation if the fifth bit of the character is 1, the first four bits of this character will be between 10h and 1Fh. 1Bh to 1Fh will not be used for any character representation. Therefore, these unused characters will be used to represent the control symbols. The control symbols are lowercase letters, uppercase letters, spaces, numbers and the end of the text, represented by 1Bh, 1Ch, 1Dh, 1Eh and 1Fh respectively. Then, the binary representation of these hexadecimal values will be stored in the LSB of the image.

The following steps are performed by the recipient to retrieve the data or image. This recovery will be based on the key available with the receiver. If the recipient has the data extraction key, he can only get the data embedded in the image. If the recipient only has the encryption key, he can only recover the image. If the recipient has both keys, he can retrieve the data as well as the image.

B. Data modification

The original image is encrypted using an encryption key. Encrypted data is used for data integration. In ordinal virtual integration, no actual embedding is performed. Where ordinal represents the position of the pixel that matches the data. At each pixel, the data is virtually integrated based on the bit values of the data and the LSB bits of the pixel. If the LSB bits of the pixel match the bit values of the data, it indicates that the data has been merged at this pixel in the cryptographic image. The display of the ordinal value of a pixel with virtually embedded data is recorded in a separate location and is considered the key to retrieve data from the receiver. For security reasons, it may be encrypted and sent to the recipient. For incompatibility, select the next pixel for virtual integration. Repeat until the end of the file. Eventually, a Stego image is created and sent to the recipient.

The original data considered in this example is "Hai". After data modification, the expression is as follows.

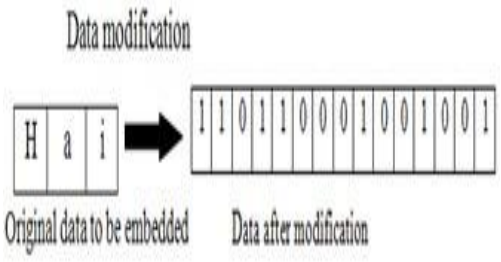

Fig 4.4: Data after modification

C. Image recovery

If the encryption key is available on the recipient side, the encryption key can be used to decrypt the original image.

The sender sends the encryption key to the recipient. This key is used as the start value of the feedback shift register. This initial value is used to generate a pseudorandom number that is added to the pixel value of the image and performs the modular operation with 256. The generated value will be the new pixel value. The same procedure is performed for all pixels in the cover image. Therefore, the image is decrypted. Pseudo-random numbers are generated by subtracting a random number from a starting value. The result is placed at the end of the starting value by moving the starting value to the left.

D. Data extraction

Data extraction is the reverse process of data integration. Initially, the key is included in the encrypted image where the data is displayed. Group LSB bits into 5 bits. Then check 5bits based on this control symbol with control symbols 1B, 1C, 1D and 1E. Finally, the original data is acquired.

V. ALGORITHM

1. Read the input image and input from data modification stage.
2. Read the RGB values of the each pixel of the image.
3. Compare the LSB bit of the pixels with the bit value of the data. 0
4. If matched read the location where it is matched which will be the data extraction key Else Try to find the match of data bits with the LSB bits of the pixels
5. Finally obtain data extraction key which will be locations of the pixel where the data bits are present.

VI. RESULTS AND PERFORMANCE ANALYSIS

Our proposed method is verified using standard gray image and color image with size (256 × 256).

Fig 5(a) shows experimental results of a group of flower images. The original image of Fig. 5 (a) is encrypted using the encryption flow shown in Fig. 5 (a). Points to note, the encryption process is performed in two steps.Fig. 5(b)(1)shows the result of the encrypted operation 1, and Fig. 5 (b) (2) shows the result of the encryption operation 2. Fig. 5(c)shows a generated encrypted image containing secret bits, respectively and extracts hidden text (secret data) shown in Fig 5(d).

Like encryption, decryption is done in two steps. Operation and Operation the results of deference 1-2 are shown in Fig. 5 (d)(1) and Fig. 5(d)(2). Hidden text, hidden text length, the number of bits to use for data masking, the number of hidden ASCII characters is calculated. Since no operational image encryption is performed prior to the encryption key, the coarse image can be reconstructed with high quality. Two aspects of security are considered here. Security image content and supplemental security messages. The content owner does not allow access to the original image serving. The data manager cannot hack the system for messages that contain a partner. The original image is encrypted with the stream encryption using the encryption key.

For the data cache, extra bits are also protected by the establishment key. Data extraction and image reconstruction are separated in this method. There are three cases to be solved here at reception; just use two keys together to integrate and encrypt only the key and key.

Fig 5(a): Original image

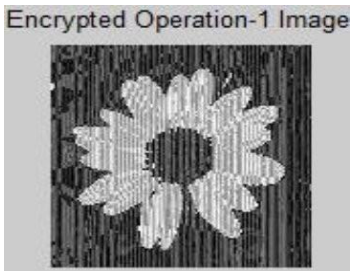

Fig 5(b) (1): Output of encryption opearation-1

Fig 5(b) (2): Output of encryption operation-2

Fig 5(c): Encrypted image contains secret data

Fig5(d): Extracted secret data

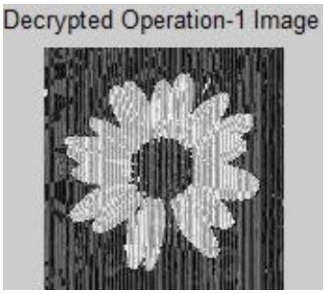

Fig 5(d)(1): Output of decryption-1

Fig 5(d)(2): Output of decryption-2

VII. CONCLUSION AND FUTURE SCOPE

In this paper, we propose a reversible and separable data masking method. That is, the virtual embedding is performed and the data bits are changed before embedding. In the first step, the content owner uses an encryption key to encrypt the cover image. Data Hider does not know the contents of the original image and embeds the data using this encrypted image. Selected data is converted using MLSB technology. The converted data is incorporated into the image using virtual integration technology. After insertion, a data extraction key is generated, encrypted, and sent to the recipient. Only the original image can be recovered if the receiver has only the encryption key and the stereo image. If you only have the data overwrite key and stego image, you can only import the original data from the stego image. If you have both data extraction and encryption keys and a stereo image, you can import both the original image and the data. Thus, there will be a separation at the receiver side, and based on the available keys, the receiver can obtain information. In this article, only the LSB of the pixel is considered in the virtual embedded. Future enhancements can take into account the LSB component of RGB components for the virtual embedding of data.

REFERENCES

1. Nobuhiko Yamaguchi "Visualizing states in autoregressive hidden Markov models using generative topographic mapping" 2012 8th International Conference on Natural Computation29-31 May 2012.
2. Yu-Ching Lu Goutam Chakraborty ; Tzu-Chuen Lu "Hidden content quality aware stego-image hiding method using re-encoding strategy" 2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST)8-10 Nov. 2017.
3. YufengShen ; YiweiGu ; ItsikPe'er "Poster: A Hidden Markov Model for Copy Number Variant prediction from Whole genome resequencing data".
4. C.Y. Teng ; Y.H. Shiau ; C.C. ChenA data hiding algorithm based on histogram re-quantization 5th International Conference on Computer Sciences and Convergence Information Technology 30 Nov.-2 Dec. 2010.
5. 2011 IEEE 1st International Conference on Computational Advances in Bio and Medical Sciences (ICCABS)3-5 Feb. 2011.
6. VandanaThakur ; MonjulSaikiaHiding secret image in video 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)1-2 March 2013
7. T. Filler, J. Judas, J. Fridrich, Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes, Information Forensics and Security, IEEE Transactions on, 6, 920-935 (2011).
8. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
9. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.
10. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst., Video Technol., vol. 16, no. 3, pp. 354–362, 2006.
11. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 1, pp. 187–193, 2010.
12. X. Zhang, "Reversible data hiding in encrypted image," IEEE.Signal Process. Lett.,vol. 18, no. 4, pp. 255–258, Apr. 2011.
13. X. Zhang, C. Qin, and G. Sun, "Reversible data hiding in encrypted images using pseudorandom sequence modulation," in Proc. IWDW 2012, LNCS, vol. 7809, pp. 358–367, 2013.
14. W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett. vol. 19, no. 4, pp. 199– 202, Apr. 2012.
15. W. Hong, T.-S. Chen, J. Chen, Y.-H. Kao, H.-Y. Wu, and M.C. Wu, "Reversible data embedment for encrypted cartoon images using unbalanced bit flipping," in Proc. ICSI 2013, LNCS, vol. 7929, pp. 208–214, 2013.

AUTHORS PROFILE

Kalpana Hangargi currently pursuing M.tech in computer science and Engineering from Dept. of CSE at PDACE Kalaburagi

Dr. Anita Harsoor M.Tech, Ph.D, Associate Professor, Computer Science and Engineering Department have teaching experience of 10 years. Areas of research are Digital Image Processing, Computer Vision, Cloud Computing and pattern Recognition. More than 25 technical papers in national and international Journals and in proceedings of international conference proceedings. One of the publication has been printed as book chapter in SPRINGER Journal.

Dr. Prakash Pattan, M. Tech, Ph.D System Manager (Prof), Computer Science and Engineering Department. His area of research is Digital Image Processing and Computer Vision, Computer Networks, IoT, Big Data Analysis etc. He has published more than 35 technical papers in national and international journals and proceedings of international conferences. Two of his papers are included in the book entitled, "Measuring Shape" authored by Neil Brent and Dr. John C. Russ (CRC Publication).