Indian J.Sci.Res. 17(2): 426 - 430, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

A ROBUST ENCRYPTION METHOD FOR SPEECH DATA HIDING USING REVERSIBLE DATA HIDING ALGORITHM

[1]Anushreya Patnaik, [2]Hannah Pauline
[1]IT Department, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad
[2]Department of Electronics and Communication Engineering, SRM University, Chennai

Abstract - In this letter, a novel reversible data hiding (RDH) algorithm is proposed for digital images. Instead of trying to keep the PSNR value high, the proposed algorithm enhances the contrast of a host image to improve its visual quality. The highest two bins in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process. The side information is embedded along with the message bits into the host image so that the original image is completely recoverable. The proposed algorithm was implemented on two sets of images to demonstrate its efficiency. To our best knowledge, it is the first algorithm that achieves image contrast enhancement by RDH. Furthermore, the evaluation results show that the visual quality can be preserved after a considerable amount of message bits have been embedded into the contrast-enhanced images, even better than three specific MATLAB functions used for image contrast enhancement.

Keywords - RDH Algorithm, Contrast of Host Image, Image Contrast Enhancement, Message Bits, MATLAB

I. Introduction

Steganography is an art and science of information hiding and invisible communication. It's unlike cryptography, where the goal is to secure communications from an eavesdropper by make the data not understood, steganography techniques strive to hide the very presence of the message itself from an observer so there is no knowledge of the existence of the message in the first place. In some situations, sending encrypted information will arouse suspicion while invisible information will not do so. Both sciences can be combined to produce better protection of the information. In this case, when the steganography fails and the message cannot be detected if a cryptography technique is used .Hiding information inside images is a popular technique now a days. An image with a secret message inside can easily be spread over the World Wide Web or in a news groups.

To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many colour variations, so less attention will be drawn to the modification. The most common methods to make these alterations involve the usage of the least-significant (LSB).The next interesting application of steganography, in which the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information.

When using a 24bitcolourimage,each bit of red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. Thus 800×600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes)of secret data. But using just3 bit from this huge size of bytes is wasting in size. So the main objective of the present work is how to insert more than one bit a teach byte in one pixel of the cover-image and give us results like the LSB (message to be imperceptible).This objective is satisfied by building new steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel.

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

II. Different Kinds Of Steganography:

[1]Corresponding Author

The four main categories of file formats that can be used for steganography are:

1. Text
2. Images
3. Audio
4. Protocol

Text steganography:

Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

Image steganography:

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 stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

Audio steganography:

Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

Protocol steganography:

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

III. Objective

The objective of this project is to provide an efficient data hiding technique and encryption in which the image and the audio can be retrieved independently.

IV. Over View

which have colour changes can be changed for the cover image .The general technique used to make the changes engaged is the usage of the Least-Significant Bit (LSB), masking, filtering and transformations on the cover image

The main aim of the project is to insert more than one bit at each byte in one pixel of the cover-image and obtain the results like the LSB. This aim can be reached by developing a Steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel. Any type of data can be hidden in a JPG image which has 24-bits by using the Steganography algorithm. The 24 bits has three bytes of RGB colours, each byte has four bits called as Nibbles. The highest value is stored in the left nibble and the lowest value is contained in the right nibble in a byte [1, 2].

At present day, with rapid growth of technology it is much easier to hide messages and on the other way it is difficult to find out that message. As the technology, is increasing exponentially, the high demand or growth for steganography seem vast. The project is focused on the applications that are derived from the use of Communication Engineering.

Steganography Algorithm

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication.

It provides invisible communication. In the present steganography algorithm, two part (data hiding at the sender side and at extracting the receiver side) Page Style

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

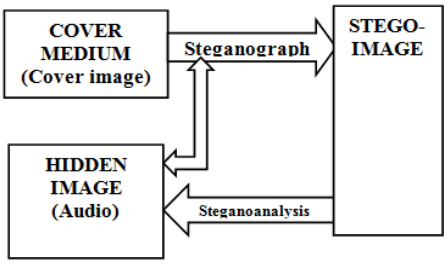

Fig : 1 Characteristics

Though steganography is most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include;

1. Capacity (how much data can be hidden)
2. Invisibility (inability for humans to detect a distortion in the stego-object)
3. Un detect ability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects)
4. Robustness (message's ability to persist despite compression or other common modifications)

An hiding the information v

5. Tamper resistance (message's ability to persist despite active measures to destroy it)
6. Signal to noise ratio (how much data is encoded versus how much unrelated data is encoded).

Architecture Of Stegnography

Block Diagram for the Steganography Algorithm

1. Data hiding
2. Data extraction.

The sender hides the data and the receiver extracts the data which is sent by the sender.

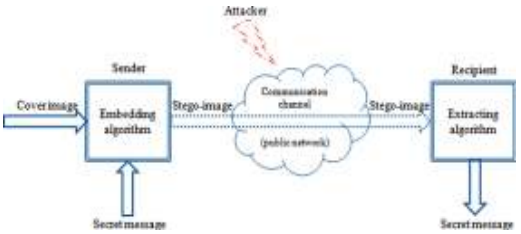

Fig : 2

Fig : 3

Embedding Process

The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end**.**

inputs are required for the embedding process:

1. Secret message - audio file that contains the message you want to transfer

2. Cover Work - used to construct a stegogramme that contains a secret message

DATA HIDING:

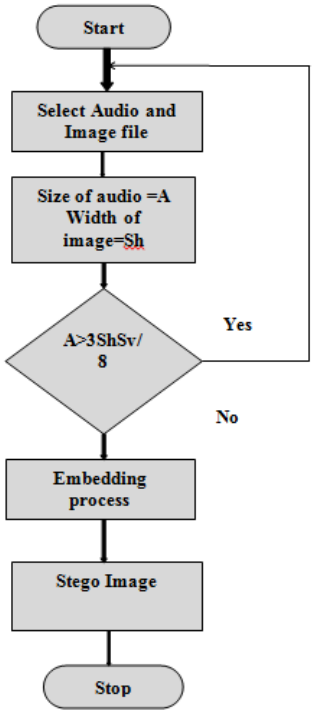

Fig : 4 Adaptive Segmentation

Colour image segmentation its very interesting and intensive topic in image processing .This can viewed as a extension of gray level image segmentation ,there are various methods which can be categorized they are:

1. Cluster based segmentation

2. Contour detection based segmentation

3. Area extraction based segmentation

4. Probabilistic models based segmentation

Hiding With Stegnography Algorithm:

1. Accept encryption password from the sender.
2. Find a maximum size (number of bytes) that is accepted by the cover-image.
3. Perform compression on secret data file to increase the amount of hiding secret data.
4. Perform encryption on secret data file.

MAIN CASE**:**

- JPG image which includes 24– bits (3 bytes of RGB colors), each byte is separated into two nibbles (four bits). The left nibble contains the

highest value in the byte while the right nibble contains the lowest value in the byte.

- The nibble value is fixed by the interval [0, 15], so that we conclude that we have 16 levels of a priority, each one represents one main case (MC) out of 16.

$$MC = round(Byte\ colour/16)+1$$

Where Byte Color ∈{ByteRed,ByteGreen, ByteBlue} represents the value of Color in decimal notation.

SUB CASE:

- Sub-case (SC) concept is used to organize the pixel architect. There are 6 SCs. Every MC have a number of SCs.
- MCcolor = index

Where $1 \leq index \leq 16$ and color∈{R,G, B}

Pixel Selection Style:

The third layer of security is the pixel selection. The Cover-image pixels are selected randomly to place the proper byte at its corresponding pixel to embed the secret data based on the colour characteristics of the cover-image. The selection of the pixels is done by introducing the concept called main cases and sub-cases, which strength the reduction of noise in a stego-image.

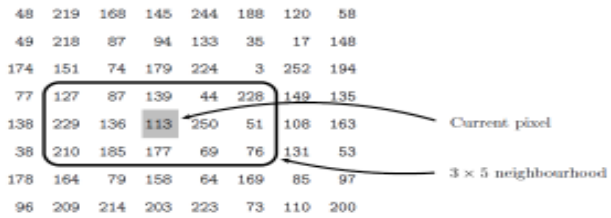

Fig : 5

Visual Attack:

The visual attack is a stego-only-attack that strips away part of the object in way that allows for a human to search for visual anomalies. The most common attack is to display the least significant bit of an object; Digital equipments such as cameras and scanners are not perfect and often leave echoes in the least significant bits. These completely random noises indicate the existence of a hidden message. The average ear can pick up subtle difference in sound. However, this is a very slow and costly attack.

Statistical Attack:

Statistical attack is similar to visual attack. The fact that most programs relies on the assumption that least significant bit of a cover file is random and therefore overwritten with a secret message is not necessarily true. The idea of the statistical attack is to compare the frequency distribution of a potential cover file with the theoretically expected distribution of the cover file. If the new data does not have the same statistical profile as the standard data is expected to have, then it probably contains a hidden message.

V. Conclusions

The proposed method modifies the amplitude of the cover image file to embed the secret message. To increase the security of the proposed scheme, we use a key to adjust the hiding technique. The experiment shows that our method is secure, imperceptible and can be used for hiding data in the image file. In the future research, we plan to use the error correction code to increase the robustness of this scheme.

At the end, feasibility of image Steganography was evaluated by considering it's the pros and cons. In summary, if implemented correctly and in conjunction with cryptographic methods to secure the embedded data before insertion to a cover medium, many of the data hiding methods described above could become powerful tools for the transmission of undetectable and secure communication.

Acknowledgment

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

References

[1] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.

[2] Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1. A steganography algorithm for hiding image in Image by improved lsb substitution by minimizes Detection by vijay kumar sharma, 2vishal shrivastava M.Tech. Scholar, Arya college of Engineering IT, Jaipur , Rajasthan (India).

[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3,

May-Jun 2012, Steganography Using Least Signicant Bit Algorithm.

[4] R.Anderson and F. Petitcolas, ”On the limits of steganography” IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.

[5] NielsProvos, Peter Honeyman, ”Hide and Seek: An Introduction to Steganography,” IEEE computer society,2003.

[6] K B Raja, Venugopal K R and L M Patnaik, ”A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images”,Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.

[7] An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[8] Johnson, N.F. Jajodia, S., ”Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998.

[9] ”Detecting LSB Steganography in Color and Gray-Scale Images” Jessica Fridrich, MiroslavGoljan, and Rui Du State University of New York, Binghamton.

[10] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, ”Hiding data in images by optimal moderately significant-bit replacement” IEE Electron. Lett. 36 (25) (2000) 20692070.

[11] Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[12] ”A Tutorial Review on Steganography” by Samir K Bandyopadhyay, Debnath

[13] Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.

[14] International Journal of Computer Science Engineering Technology (IJC-

[15] SET) ”Modern Steganographic technique: A Survey” by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology .