International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 4th Jan 2016. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-05&issue=ISSUE-01

Title **Simple and secure image Steganography using LSB and Triple XOR using MSB**

Volume 05, Issue 01, Pages: 69-72

Paper Authors
P.Harish, Ganta Ramakrishna Reddy

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

Simple and secure image Steganography using LSB and Triple XOR using MSB

P.Harish[1], Ganta Ramakrishna Reddy[2]
Assistant Professor[1,2]
Department of ECE
Malla Reddy Engineering College(MREC)

Abstract- Least Significant Bit (LSB) is a very popular method in the spatial domain of steganographic images. This method is widely used and continues to be developed to date, because of its advantages in steganographic image quality. However, the traditional LSB method is very simple and predictable. Itneeds a way to improve the security of hidden messages in this way. This research proposes a simple and safe way to hide messages in LSB techniques. Three times the XOR operation is done to encrypt the message before it is embedded on the LSB. To facilitate the process of encryption and decryption of messages, three MSB bits are used as keys in XOR operations. The results of this study prove that this method provides security to messages with very simple operation. The imperceptibility quality of the stego image is also excellent with a PSNR value above 50 dB.

Index Terms- MSB, LSB, PSNR, DCT, DFT

I. INTRODUCTION

Steganography

Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method. Generally, there are three different methods used for hiding information: steganography, cryptography, watermarking. In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical. Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e., its presence is undetectable by sight. Detection of steganography is called Steganalysis. Steganography is of different types:

1. Text steganography
2. Image steganography
3. Audio steganography
4. Video steganography

In all of these methods, the basic principle of steganography is that a secret messageis to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So, itcannot be detected easily to be containing hidden information unless proper decryption is used. Steganography refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eaves-dropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The general idea of hiding some information in digital content has a wider class of applications that go beyond steganography, The techniques involved in such applications are collectively referred to as information hiding.For example, an image printed on a document could be annotated by metadata that could lead a user to its high-resolution version.In general, metadata provides additional information about an image. Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is transformed to another format (e.g., from TIFF to JPEG or to BMP), the metadata is lost. Similarly, cropping or any otherform of image manipulation destroys the metadata.

Finally, metadata can only be attached to an image as long as the image exists in the digital form and is lost once the image is printed. Information hiding allows the metadata to travel with the image regardless of the file format and image state (digital or analog).

A special case of information hiding is digital watermarking. Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

content. The key difference between information hiding and watermarking is the absence of an active adversary. In watermarking applications like copyright protection and authentication, there is an active adversary that would attempt to remove, invalidate or forge watermarks. In information hiding there is no such active adversary as there is no value associated with the act of removing the information hidden inthe content. Nevertheless, information hiding techniques need to be robust against accidental distortions. Unlike information hiding and digital watermarking, the main goal of steganography is to communicate securely in a completely undetectable manner. Although steganography is an ancient art, first used against the Persian by the romans, it has evolved much through the years.

Image Steganography has many applications, especially in today's modern, high- tech world. Privacy and anonymity are a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly.It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also bequite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

II. EXISTING WORK OR LITERATURE SURVEY

There are currently three effective methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the carrier image. Blocking works by breaking up an image into "blocks" and using Discrete Cosine Transforms (DCT). Each block is broken into 64 DCT coefficients that approximate luminance and color—the values of which are modified for hiding messages. Palette Modification replaces the unused colors within an image's color palette with colors that represent the hidden message. With LSB Substitution I could easily change from Image Steganography to Audio Steganography and hide a zip archive instead of a text message. LSB Substitution lends itself to become a very powerful Steganographic method with few limitations. LSB Substitution works by iterating through the pixels of an image and extracting the ARGB values. It then separates the color channels and gets the least significant bit. Meanwhile, it also iterates through the characters of the message setting the bit to its corresponding binary value 3.

III. WRITE DOWN YOUR STUDIES AND FINDINGS(PROPOSED WORK)

There are several Steganographic techniques for image file format which are asfollows:

Steganography can be viewed as akin to cryptography. Both have been usedthroughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not. In an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However, there are often cases when this is not possible, either because you are working for a company that does not allow encrypted email or perhaps the local government does not approve of encrypted communication (a reality in some parts of the world). This is where steganography can come into play. A good steganography system should fulfil the same requirements posed by the "Kerckhoff principle" in cryptography. This means that the security of the system has to be based on the assumption that the "enemy" has full knowledge of the design and implementation details of the steganographic system. The only missing information for the "enemy" is a short easily exchangeable random number sequence, the secret key, and without the secret key, the "enemy" should not have the slightest chance of even becoming suspicious that on an observed communication channel hidden communication might take place. Steganography cannot be detected. Therefore, it is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

Spatial Domain Technique:

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data.

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly.Least Significant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques. Advantages of spatial domain LSB technique are:

1. Degradation of the original image is not easy.
2. Hiding capacity is more i.e., more information can be stored in an image.

Disadvantages of LSB technique are:

1. robustness is low
2. Hidden data can be destroyed by simple attacks.

Masking and Filtering Masking and Filtering:

It is a steganography technique which can be used on gray-scale images. Masking and filtering are similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques: This method is much more robust than LSB replacement with respect to compression. Disadvantages: Techniques can be applied only to gray scale images and restricted to 24 bits.

Transform Domain Technique:

The Frequency domain the message is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against attacks. Transform domain embedding can be termed as a domain of embedding techniquesfor which a number of algorithms have been suggested. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing.

Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are of 3 different types:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

Distortion Techniques:

In this technique, store information by signal distortion and measure the deviation from the original cover in the decoding process. Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. In this technique, a stego-image is created by applying a sequence of modifications to the cover image.

This sequence of modifications is use to match the secret message required to transmit. The message is encoded at pseudo-randomly chosen pixels. If the stego image is different from the cover image at the given message pixel, the message bit is a 1. Otherwise, the message bit is a 0. The encoder can modify the 1 value pixelsin such a manner that the statistical properties of the image are not affected. If an attacker interferes with the stego-image by cropping, scaling or rotating, the receivercan easily detect it.

Characteristics feature of Data Hiding Techniques:

Perceptibility does embed message distort cover medium to a visuallyunacceptable level.

Capacity how much information can be hidden with relative to the change in perceptibility.

Robustness to attacks can embedded data exist manipulation of the stego medium in an effort to destroy, or change the embedded data.

Tamper Resistance Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter a message once it has been embedded in a stego-image.

Image Steganalysis:

Steganalysis is the breaking of steganography and is the science of detecting hiddeninformation. The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

on steganographic algorithms introducing statistical differences between cover and stego image.

IV. RESULTS AND DISCUSSION(IF ANY)

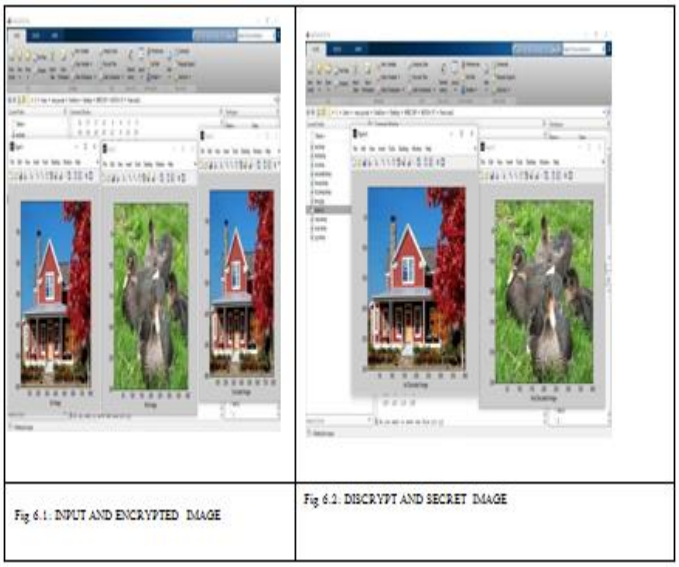

Fig 6.1. INPUT AND ENCRYPTED IMAGE

Fig 6.2. DISCRYPT AND SECRET IMAGE

V. CONCLUSION

The method proposed in this study has an advantage in the aspect of imperceptibility as evidenced by the excellent value of PSNR and MSE. Where allPSNR values are more than 50dB, so does the MSE value not more than 0.3. This method is also very simple and safe because with XOR operation steganography process can be done quickly and easily. With the XOR operator, the embedded bits cannot be directly guessed. Moreover, there are three keys used, with three times the XOR operation. The use of an integrated key in the cover image also keeps the stego file the same size, and no key delivery is required to the receiver so it can speed up the messaging process as the file size is maintained. However, based on histogram analysis there is a distinct pattern difference between the cover image andstego image.

REFERENCES

W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and h. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 15,no. 4, pp. 1987-1995, 2017.

R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICONSONICS), Yogyakarta, 2017.

A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.

G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "HybridMethod using 3-DES, DWT and LSB for Secure Image Steganography Algorithm,"in International Conference on Information Technology, Information System, and Electrical Engineering(ICITISEE), Yogyakarta, 2017.

A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt Method using WaveletTransform and One-Time Pad for Secret Image Delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.

A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali and M. Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing," in International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.