Matlab Based Image Hiding Using Steganography Technique

PreetInder Kaur

Department of Computer Science Engineering
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Ada

Department of Computer Science Engineering
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Abstract- Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image without causing statistically significant modification to the cover image. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. This paper intends to give an overview of image steganography, its uses and techniques.

Keywords – Image, Steganography, Video, Information.

I. INTRODUCTION

Steganography is the practice of concealing messages or information within other non-secret text or data. Hiding of information or message is achieved through hiding information in other information, thus hiding the existence of the transmitted information. The word steganography is derived from the Greek words “stegos” means “cover or protected” and “graphei” means “writing” defining it as “concealed writing or covered writing”. Cryptography and steganography are different, but both targets at security. Steganography differs from cryptography in the sense that where cryptography concentrates on keeping the contents of a message secret, steganography concentrates on keeping the existence of a message secret.

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. A basic steganographic system is shown in figure1.

In Steganography, the multimedia files such as image, video, audio, etc is used to attach the secret data. The unique feature of the Steganography considering cryptography is that unauthorized individuals are not aware of the hidden data in the Stego-media. Initial Steganography techniques have been first applied to images; however, the video streams have attracted a lot attention recently since they can assure a large amount of capacity increase for hidden/secret data. The hidden data can be embedded either into image or into audio part of the video streams.

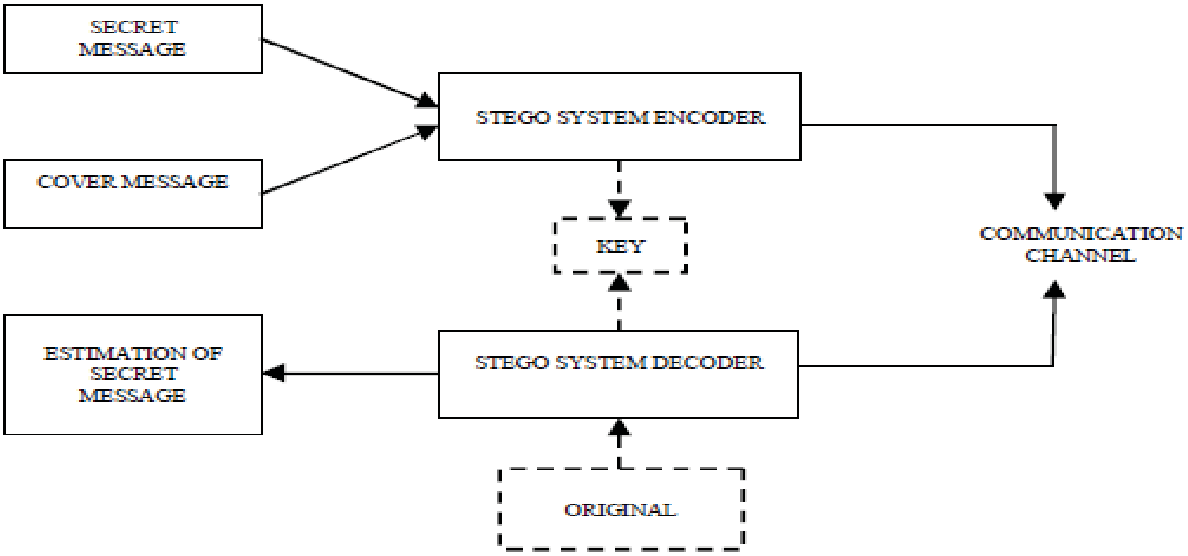

Figure 1. A Basic Steganographic Architecture

II. LITERATURE REVIEW

Rohit G Bal, Dr P Ezhilarasu in 2014[1] in “An Efficient Safe and Secured Video Steganography Using Shadow Derivation” discussed that Steganography is the art of hiding the fact that communication is taking place, by concealing information in other information. This paper focus on Secret sharing technique is used to hide information. Secret sharing is a technique for splitting a message into several parts so that all parts are sufficient to recover the message. The current study presents the design and implementation of a steganographic procedure that can automatically analyze a video and hide images efficiently and effectively inside it for application in a digital records environment. Video Fragmentation is used to extract frames (convert video into images) from video for carrier. The secret color image pixels will be converted to m-ary notational system. The (t-1) digits of secret color image pixels are generated using reversible polynomial function. Reversible polynomial function and the participant’s numerical key are used to generate secret shares. The secret image and the cover image is embedded together to construct a stego image. All stego images are embedded to construct video. The reversible image sharing process is used to reconstruct the secret image and cover video. The secret is obtained by the Lagrange’s formula generated from the sufficient secret shares. Quantization process is applied to enhance the nature of the cover video. This proposed system investigates the problem of occurrence of meaningless and the large distortions in the reconstructed shadows. Existing solutions are either limited to a small amount of data. Hence, this paper proposes several solutions for color image pixels that reveals the secret image without loss and preserves the cover image using quantization. This methodology can be further enhanced for 3D images and can be used for embedding text.

Anil Kumar, Rohini Sharma in 2013 [2] in “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique” implemented a secured Hash based LSB technique for image steganography. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes their technique secure and more efficient. This technique also applies a cryptographic method RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that’s why they used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes their technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

Bhavana.S and K.L.Sudha[3] in 2012 in “Text Steganography using LSB Insertion Method Along With Chaos Theory” discussed that the art of information hiding has been around nearly as long as the need for covert communication. Steganography, the concealing of information, arose early on as an extremely useful method for covert information transmission. Steganography is the art of hiding secret message within a larger image or message such that the hidden message or an image is undetectable; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscure. The goal of a steganographic method is to minimize the visually apparent and statistical differences between the cover data and a steganogram while maximizing the size of the payload. Current digital image steganography presents the challenge of hiding message in a digital image in a way that is robust to image manipulation and attack. This paper explains about how a secret message can be hidden into an image using least significant bit insertion method along with chaos. The chaos system is highly sensitive to initial values and parameters of the system. The proposed algorithm provides security and maintains secrecy of the secret message and provides more randomness since they are using chaos which is sensitivity to initial conditions. The performance analysis is being done. The PSNR value is also being calculated.

Krati vyas, B.L.Pal in 2014 in[4] “A Proposed Method in Image Steganography to Improve Image Quality With LSB Technique” presented, implemented and analyzed a new A new Steganography technique. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This paper work concluded that the LSB hiding method is the worst case of the proposed method. In their paper work they propose a new approach which give good quality of the image after encoding the original image by using the LSB technique because LSB technique has a drawback it affects the resolution the original image after encoding, so that image quality go burst. The future work on this project is to improve the compression ratio of the image to the text. The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn"t change much and is negligible.

Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal & Paramartha Dutta[5] in 2014 in “A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain” proposed a secure LSB technique for image steganography using the concept of non-linear dynamic system (chaos) in this paper. The chaotic system is highly sensitive to initial values and parameter of the system. The proposed algorithm provides added security to the base steganography technique. Application of separate chaotic sequence for encryption of each part of secret image provides an added security from attacks. The proposed technique uses host image files in spatial domain to hide the presence of sensitive information regardless its format.The proposed technique is applied to JPEG files; however it can work with any other formats. Further work includes adapting the free parameters of the logistic chaotic map using soft computing techniques as chaotic systems are highly sensitive to initial conditions.

Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav [6] in 2012 in “Steganography using Least Signicant Bit Algorithm” discussed that the proposed approach in this paper uses a steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured. The main intention of the project is to develop a steganographic application that provides good security. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when they embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel. They used the Least Significant Bit algorithm in this paper for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms. The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size as well as the carrier image size. The future work on this paper is to improve the compression ratio. The security using Least Significant Bit Algorithm is good but theycan improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

Masud et al. [7] has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. In designing of robust and secure image steganography based on LSB insertion and RSA encryption technique has been used.

Weiqi Luo et al. [8] proposed a LSB matching revisited image steganography and edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image.

Mohmmad A.Ahmed et al. [9] proposed a method in which a message hidden inside an image by using the Least Significant Bit technique and after creation of the hidden message, the image will pass it in hash function to obtain hashing value using the MD5 technique. Two steganography technique proposed for hiding image in an image using LSB method for 24 bit color images. In a hash based approach proposed for secure keyless steganography in lossless RGB images that an improved steganography approach for hiding text messages in lossless RGB images.

Anderson and Petitcolas [10] posed many of the open problems resolved in this article regarding to steganography. In particular, they pointed out that it was unclear how to prove the security of a steganographic protocol. They also posed the open question of bounding the bandwidth that can be securely achieved over a given cover channel. Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exist to implement video steganography. In a hash based least significant bit technique for video steganography has been proposed. Where the secret information is embedded in the LSB of the cover frames and a hash function is used to select the position of insertion in LSB bits.

Mozo A.J. et al.[11] “Video Steganography using Flash Video (FLV)”successfully deals with the demands of using video steganography on FLV. The project focused on FLV files because of their relatively small size compared to other video file formats, their simplicity in structure, and their popularity in video-hosting websites. This allow doctors and medical personnel to embed multiple medical records such aselectrocardiogram signals, ultrasound files, medical prescriptions, urinalysis, and may more medical files into single video file (FLV).

Hussein A. et al. [12] “Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error “deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis. There is new method to hide the data in motion vectors of MPEG-2 compressed video. The results of this paper are evaluated on two metrics: quality distortion to reconstructed video and data size increase of the compressed video.

III. PROBLEM FORMULATION

The aim of stegnography is to hide the data over an image using least significant steganographic algorithm and to send the stego file to the destination where the retrieving of the secret data is done.

The proposed method should provide better security while transferring the data or messages from one end to the other end. The main objective of this thesis is to hide the message or a secret data into an image which acts as a carrier file having secret data and to transmit to the destination securely without any modification. If any distortions occur in the image or on its resolution while inserting the secret message into the image, there may be a chance for an unauthorised person to modify the data. So, the data encryption into an image and decryption and steganography plays an important role.

Existing Techniques Used

There are a large number of cryptographic and Steganographic methods that most of us are familiar with. The most widely used two techniques are:

- RSA Algorithm
- LSB Insertion Method

1. RSA Algorithm

The algorithm was given by three MIT’s Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure.

2. Least Significant Bit (LSB) Insertion Method

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image. For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

REFERENCES

[1] Rohit G Bal and P Ezhilarasu(2014), "An Efficient Safe and Secured Video Steganography Using Shadow Derivation", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3.

[2] Anil Kumar and Rohini Sharma(2013), "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7.

[3] Bhavana.S and K.L.Sudha, "Text Steganography using LSB Insertion Method Along With Chaos Theory".

[4] Krati vyas and B.L.Pal(2014), "A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1.

[5] Debiprasad Bandyopadhyay , Kousik Dasgupta , J. K. Mandal and Paramartha Dutta(2014), "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1.

[6] Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav(2012), "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp. 338-341.

[7] S. M. Masud Karim, Md. Saifur Rahman and Md. Ismail Hossain(2011)"A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24.

[8] Weiqi Luo, Fangjun Huang, Jiwu Huang(2010), "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214.

[9] Mohammad A. Ahmad, Dr. Imad Alshaikhli and Sondos O. Alhussainan(2012), "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research, Vol. 2, Issue No.3, Pages No. 127-139.

[10] Ross J. Anderson, Fabien A. P. Petitcolas(1998), "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481.

[11] Mozo AJ., and Obien M.E., C.J. Rigor(2009), "Video Steganography using Flash Video (FLV)" I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore.

[12] Hussein A. Aly (2011)", Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" IEEE transactions on information forensics and security, vol. 6, no. 1.Heba Khudhair Abass(2013), "A Study of Digital Image Fusion Techniques Based on Contrast and Correlation Measures".