WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

"Steganography A Technique To Hide Information With In Image"

[1]Prof.Nitin Thakre, [2]Sakshi Junghare, [3]Pranali sakhre, [4]Dipti Khawse.

[1]Professor, [2,3,4]Student

[1,2,3,4]Department of Computer Science and Technology

[1,2,3,4]Govindrao wanjari college of engineering and technology Nagpur, India

[2]sakshijunghare3@gmail.com, [3]sakharepranali8@gmail.com,[4]dipti29khawse@gmail.com.

ABSTRACT:

The science and art of covert communication between two parties while attempting to conceal the substance of a message is known as steganography. The skill is keeping the information you embed in your cover photos after you embed it. Steganography is the art and science of concealing messages so that only the sender and recipient are aware of their contents. Regarding the presence of your data. In this article, two different approaches are compared. The first method did not use compression or encryption; it just used the least significant bit (LSB). The LSB approach is employed after the secret message has been encrypted. Additionally, the image is transformed into the frequency domain using a discrete cosine transform (DCT). The DCT algorithm is implemented in the frequency domain, through which the stego image is transformed domain into the spatial domain and the change bits are inserted into the frequency component of the cover image. The LSB algorithm is implemented in the spatial domain, where the loading image bits are inserted into the least significant bits of the coverage image to generate the stego image.

Keywords: Data hiding, Information hiding, LSB, Image steganography.

INTRODUCTION

The development of the computers and rapid growth of internet use due to broadband and expensive computer equipment are hampering the rapid development of steganography. In recent years, convert and secure communication is the basic requirement of people. Therefore, steganography attracts people with concerns about internet safety. Steganography has moved away from the digital strategy of hiding a file in some form of multimedia, such as an image, an audio/video file [1,2].

The purpose of steganography is to hide information embedded in the cover image, encryption converts data into an unreadable form. Typically, users use only one security approach at a time, encryption or steganography. A combination ofsteganography and encryption, this techniques are the most useful and powerful security techniques, they can also play a veryimportant roll in this area.

Basic Model : Theproposed basic steganography model , as shown in Figure 1,contains two files: the first is the cover image and the second is the secret file, which is hidden by the private key in encrypt the secret file.

As shown in Figure one, there are two steps ,the first hides the data (embedding technique)and the second compresses it to reduce the storage space and size of the data The end result of the system is a stego image, a digital image with a secret message hidden within. The stego image is send to the recipient via a public communication channel(internet) where the recipient obtains secret data from the stego image by applying a set of extraction rules with the secret password. LSB Substitution :LSB is one of the earliest techniques encoding tools useful in steganography application [3,4].This method use spatial integration

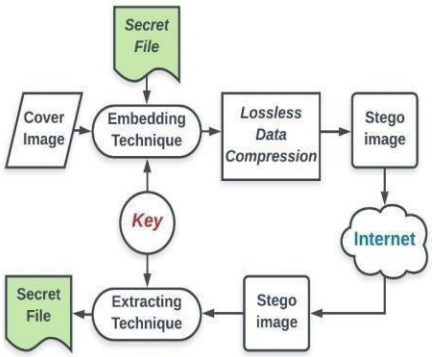


Figure 1:Basic Model

SUMMARY OF THE METHODS

Traditionally , Least Significant bit substitution (LSB) is used for image steganography. Images tend to have higherpixel quality if not all pixels are used. The LSB method assumed that changing some pixel values would not show any visible change. Secret information is converted into binary form. The cover Image is scanned to determined the least significant bits in the techniques and embeds secret data in cover image, slightly modifying the pixels Therefore, it is almost impossible for the human vision system "HVS" to notice this small changes, due to which the possible attacks of opponents have decreased significantly. while this coding method embeds a simple tool in many packages, it has masked some weaknesses for centuries. The weakest are noise, filtering clipping, spatial color transformations, andresampling of LSB approach states . Also , this approach can be compromised by lossy compression algorithms,so the extraction of secret data in application that use compressed video streams cannot be guaranteed**.**

The binary bits of the secret are then replaced in the cover image LSB. The replacement method should be used with caution , since overloading the cover image can result invisible changes that reveal the presence of secret information . With LSB Although this method is a reference, a number of related methods have been proposed. For example , a minor change was made in converting a secretinto binary codes .The Huffman coding method is used to encode the secret into binary bits . The encoded bits are then embedded in the title image using the LSB method . Another versionof the LSB method is used for RGB images. The cover picture consists of 3 channels divided into bits .The secret message is embedded in all three layer in a 2:2:4 ratio forthe R,G and B layers. Not only spatial domainis used, but also quantum imaging.

The frequency domain is used in the quantum image domain, and the pixels intended to affects the color are used ,replacing the LSB cover image with the most significant bits of interesting approach is that it uses audio alongside video images to enhance masking.

In addition to the LSB method, he proposed a combination of Discrete cousin transform (DCT) and discrete wavelet transform (DWT) to hide a secret message in the cover of a video.The MOT method (Multiple Object Tracking) is used to find the area of interest the secret data is the first encrypted and then converted into binary bits before being integrated into thecover foil. Provide a detailed overview of traditional image steganography method.Another classic method in the field of image steganography is the pixel value difference(PVD). PVD works on the differenceof consecutive pixels to find a place to hide thesecret bits, preserving the integrity of then cover image. For every 8 bites, a combination of LSB on the first two bites and PVD on the remaining six bites is designed. Sum othertechniques used are also unprotected steganography where then cover image is not provided but generated from then secretinformation.

Secret information is obtained and relationshipmanagement is performed to create a cover image using the object recognized the method similarly discovery steganography has beenproposed, in which cover image featured has secret bit pattern(LBP) image are hashed first.Later the hashes are matched to create a stego image. Also, instead of LBP you get colored cover photo borders. So the binary bits of secret information are hidden in the edges exposed in the cover images.

TABLE 1. Summary of the details on thetraditional methods.

Methods	Dataset	metrics	Advantages	Dis-advantages
[16]	1 RGB color	PSNR and time	-Less computation time -Robust both in embedding andextracting	-Less secure - Secret Information Text
[17]	Lena and baboon	PSNR andMSR	- Less computation time -Image secret message	-Security is less than a deepLearning methods
[10]	Lena	PSNR	- Less computation time -Image secret message	-Less secure

Algorithm:-

LSB

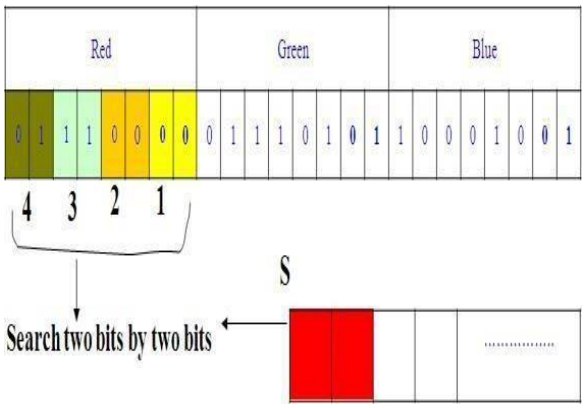
One of the most common techniques in steganography is least significant bit (LSB) insertion. This is known as LSB pixels of thecarrier image .Embedding a message in an image is a simple approach .In this method ,some information of the carrier image pixel is replaced with message information so that it cannot be observed by the human visual system, thus exploiting some of the limitationof the human visual system. Insert LSB depends on the number of the bits in theimage.

In image an 8-bit ,I .H. the 8th bit of each bytein the image modified by 1 bit of the each bytein the image modified by 1 bit of the of the hidden message .And in a 24-bit image , the colors of each component such as RGB (Red,Green, Blue) are changed. Low bit steganography involves operations on the low order bits of a cover image, audio or video.

The least significant is the lowest bit in a series of the binary number .In LSB replacement ,the least significant bits of the pixels are carried by the secret message bits, resulting in an image with a hidden message attached. The integration process varies depending on the number of bits in the image(different for 8 and 24 bit image).

Proposed method

The LSB masking technique consists of directly hiding a secret message in at least twosignificant bits in the image pixels, which degrades the image resolution ,which reducesthe image quality and makes the image vulnerable to attacks, it was attacked and broken.



Therefore, a new technique has been proposedthat will allow you to protect the secret message based on searching for identical values between the secret message and theimage pixels.

The Proposed Masking algorithm

Entries: message to hide and password to encrypt and decrypt ,image.

Output: Stego image boot (secret message support).First scan the image in each line and then encode it in binary format. Hidden message encoding in binary format.

First checks the image in each line and the sizeof the secret message .

Beginning of subheading 1:

Randomly select 1pixel from the image.Divide the image into three parts (red, green and blue part).Hide 2 by 2 bits of the message in each part of the pixel and more or less verifyits identity.

It's identically and true, we set the image withnew values. Otherwise hide in two LSBs and set the image with the new values. Stores the position of hidden bits in the binary table .Endof Sub-iteration 1.

Now put the new value on the image and saveit.

New method in image steganograp

(a) Original image

(b) 3 bit are hidden

THE TERMINOLOGIES USED ARE FOLLOWING

Covered image :A real image that acts as a hidden file medium .

Steganography Image :The information embedded In the cover image are steganography image.

Message :The information actually hidden in images can be an image or image plain text.

Steganography Key: A steganography key is used to extract a message from a steganography image.

Layout Algorithm: The algorithms is used to hide information within in the image.
Detachment Algorithm: An algorithms is used to extract information from a steganography image.
Basically, in a steganography , the information is hidden in the cover image , and this cover image makes up the steganography image .
The recipient receives the steganography image through a known medium and the third party involved in the process has no idea that the steganography image contains a hidden message.

CONCLUSION

Image steganography is a method used to convey secret information by hiding it in a cover image. A review of all related work has led to there general classification into three group. Most traditional steganography methods use LSB substitution and of its variants. Beside LSB,PVD,DCT and EMD are commonly used .The obfuscation
ability of traditional methods is limited because overloading the cover image with more pixel to hide the secret msg can lead to distortions.Image steganography can be viewed as an image reconstruction task that uses the cover image an secret information as inputs to reconstruct a steganography image that is closed to the cover image in terms of similarity.
Traditional method are less secure as they only need to detect the presence of a secret message. The secret message is easy to extract because a statistical method was used for integration.
In summary , the article discusses newer image steganography technique and current trends . This details above records and assessment metrics. This paper also assesses the challenges they face, some discussion of gaps and opportunities or future directions.
It can be concluded that, considering all the challenges and shortcomings, deep learning has great potential in the field of image steganography.

REFFRENCE

1. An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques Mukesh Garg A.P. Gurudev Jangra M.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering &Technol, Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper is Available online at: www.ijarcsse.com
2. International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.6871, Survey Paper on Steganography Namrata Singh Computer Science and engineering ABES Engineering College, Ghaziabad A.K.T.U.
3. American Journal of Engineering Research (AJER) e-ISSN : 2320- 0847 p-ISSN : 2320-0936 Volume-02, Issue-11, pp-122-128 www.ajer.orgSteganography: A Review of Information Security Research and Development in Muslim World YunuraAzuraYunus, SalwaAbRahman, Jamaludin Ibrahim Kuliyyah of Information and Communication Technology International Islamic University Malaysia
4. International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2016,A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar1, Ambika Umashetty2 Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India1 Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi.
5. T. Morkel , J.H.P. Eloff and M.S. Olivier “An Overview of Image Steganography”.
6. SamerAtawneh, Ammar Almomani1 and Putra Sumari, “Steganography in Digital Images: Common Approaches and Tools,”IETE Technical Review, Vol 30, Issue 4, Jul-Aug 2013.
7. Mastering C# (Paperback), SQL Server Bible (Paperback) ,.NET Black Book (Paperback) books.
8. Z. Qu, Z. Cheng, W. Liu, and X. Wang, ‘‘A novel quantum. Z. Qu, Z. Cheng, W. Liu, and X. Wang, ‘‘A novel quantum image steganog- raphy algorithm based on exploiting modification direction,’’ Multimedia Tools Appl., vol. 78, no. 7, pp. 7981–8001, Apr. 2019.
9. S. Wang, J. Sang, X. Song, and X. Niu, ‘‘Least significant qubit (LSQb) information hiding algorithm for quantum image,’’ Measurement, vol. 73, pp. 352–359, Sep. 2015.
10. N. Patel and S. Meena, ‘‘LSB based image steganography using dynamic key cryptography,’’ in Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT), Nov. 2016, pp. 1–5.
11. O. Elharrouss, N. Almaadeed, and S. AlMaadeed, ‘‘An image steganogra- phy approach based on k-least significant bits (k-LSB),’’ in Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 131–135.
12. M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. Srikanth, and M. Reddy, ‘‘Digital video steganography using LSB technique,’’ Red, vol. 100111, Apr. 2020, Art. no. 11001001.
13. S. S. M. Than, ‘‘Secure data transmission in video format based on LSB and Huffman coding,’’ Int. J. Image, Graph. Signal Process., vol. 12, no. 1, p. 10, 2020.
14. M. B. Tuieb, M. Z. Abdullah, and N. S. Abdul-Razaq, ‘‘An efficiency, secured and reversible video steganography approach based on lest sig- nificant,’’ J. Cellular Automata, vol. 16, no. 17, Apr. 2020.
15. K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E.-S.-M. El-Rabaie, and G. M. El-Banby, ‘‘High security data hiding using image cropping and LSB least significant bit steganography,’’ in Proc. 4th IEEE Int.Colloq. Inf. Sci. Technol. (CiSt), Oct. 2016, pp. 400–404.
16. Arya S Soni ‘‘Performance evaluation of secrete image steganog- raphy techniques using least significant bit (LSB) method,’’ Int. J. Comput.Sci. Trends Technol., vol.1.6,no,2,pp.160165,2018