HIDING TEXT IN A IMAGE USING STEGANOGRAPHY METHOD

V.V. Vinoth [1], Dr. B. Karthik [2]

[1] Research Scholar, Department of ECE, Bharath University, Chennai, India.

[2] Associate Professor, Department of ECE, Bharath University, Chennai, India.

[1] E-mail:vinothvv.velaian@gmail.com

[2] E-mail: karthik.ece@bharathuniv.ac.in

Abstract

Steganography is the artwork of hiding the reality that communication is taking place, by using hiding records in different records. Many exceptional provider file codecs may be used, but digital images are the most famous because of their frequency at the Internet. For hiding secret records in images, there exists a large form of steganographic techniques a few are more complicated than others and all of them have respective sturdy and weak points. Distinctive packages have unique necessities of the steganography method used. For example, a few packages may require absolute invisibility of the name of the game statistics, while others require a bigger secret message to be hidden. This paper intends to provide a top level view of photo steganography,it makes use of and strategies. This paper intends to give an overview of picture steganography, its uses and techniques. It additionally displays how a text report to be hide in a photograph file. Steganography is best method which offer privacy and secrecy both in case of hiding image within picture.

Keywords- **Steganography**

INTRODUCTION

Steganography is the artwork of hiding records to save you their detection through an unauthorized character. The virtual data (bits or symbols) is probably hidden in any digital object, either textual content or photograph. The hidden records should be embedded in photograph, e.g., without causing any sort of picture degradation. Furthermore, as the embedded text length is going large the range of picture distortions is multiplied. Therefore, it is goal is to embed textual content records into a photograph with minimal photograph degradation

Steganography was classified as follows,

1) Text Steganography

2) Image Steganography

3) Audio Steganography

4) Video Steganography

1) Text Steganography**:**

A steganography method that makes use of text as the cover media is known as a textual content steganography. It is one of the most difficult forms of the steganography approach. That is because text documents have a totally small quantity of redundant information to hide a secret message.

2) Audio Steganography:

A steganography approach that makes use of audio as the cover media is referred to as an audio steganography. It's miles the most challenging undertaking in steganography. That is due to the fact the human auditory system (HAS) has a huge dynamic variety that it can concentrate over. As a consequence, even a minute change in audio great also may be detected by using the human ears.

3) Video Steganography:

A steganography technique that uses video as the cover media is called photograph steganography.

4) Image Steganography**:**

A steganography approach that makes use of pictures as the cover media is called an image steganography. Hiding mystery messages in virtual photographs is the maximum broadly used technique as it could take benefit of the restricted energy of the human visible system (HVS) and also due to the fact images have a large amount of redundant facts that can be used to hide a secret message.

2. STEGANOGRAPHY AND CRYPTOGRAPHY

2.1 Pure steganography

Pure steganography is the procedure of embedding the records into the object without the use of any private keys. This form of steganography totally relies upon upon the secrecy.

This kind of steganography makes use of a cover picture in which records is to be embedded, private records to be transmitted, and encryption decryption algorithms to embed the message into image.
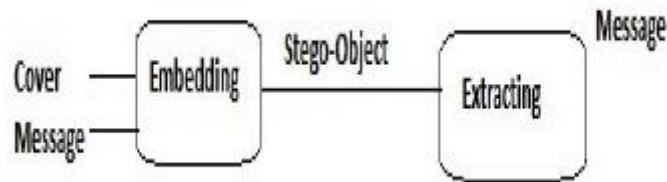

Fig.1 Block diagram of steganographic technique

2.2Cryptography

The science of writing in mystery codes/addresses all of the factors essential for at ease communication over an insecure channel, specifically privateness, confidentiality, key trade, authentication, and non-repudiation. But cryptography does not continually provide secure conversation. The benefit of steganography over cryptography alone is that messages don't attract attention to themselves, to messengers, or to recipients. Whereas the intention of cryptography is to make facts unreadable by way of a third party, the intention of steganography is to cover the records from a third party. Frequently, steganography and cryptography are used together to ensure security of the covert message.

PROPOSED SYSTEM

Hiding facts is the process of embedding data into digital content material. In data hiding, 3 well-known techniques may be used. They're watermarking, steganography and cryptography.

The main gain of steganography set of rules is due to its easy safety mechanism. There are numerous steganography techniques used for hiding information including batch steganography, permutation steganography, least significant bits (LSB), bit-aircraft complexity segmentation (BPCS) and chaos primarily based spread spectrum image steganography (CSSIS). Research in hiding statistics interior photograph the use of steganography method has been carried out by means of many researchers.

Warkentin et al. proposed a method to hide data in the audiovisual documents. In their steganography set of rules, to hide data, the name of the game content material must be

hidden in a cover message. El-Emam, on the other hand, proposed a steganography set of rules to hide a large quantity of facts with excessive protection [5]. His steganography algorithm is primarily based on hiding a big quantity of data (photo, audio, textual content) report inside a colour bitmap (bmp) image.

The encrypt module is used to cover information into the picture; nobody can see that facts or report. This module requires any type of picture and message and gives the best one image file in destination. The decrypt module is used to get the hidden information in an photograph record. It take the picture record as an output, and deliver file at destination folder, one is the same image file and another is the message file that is hidden it that. Earlier than encrypting report internal photo we must save the name size and exact location of picture. We should save document name before document records in LSB layer and save file size and file name size in most right-down pixels of picture. Writing these records is wanted to retrieve file from encrypted image in decryption state.
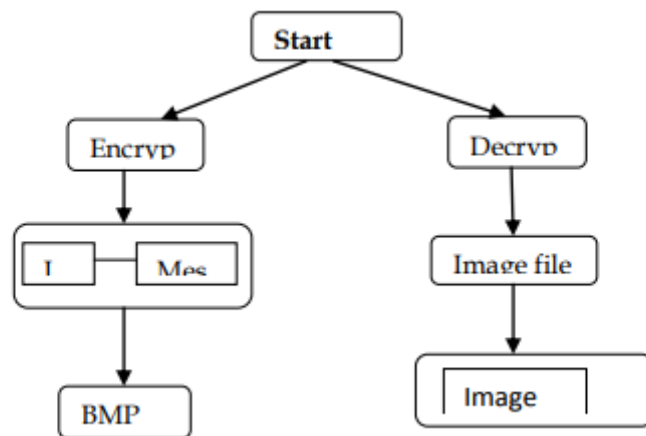

Fig.2Flow diagram of encryption and decryption technique

The executed computer experiments show that simply segment statistics makes feasible to reconstruct image uniquely. The segment of the given image in combination with the averaged amplitude spectrum received from the organization of images offers the first-rate outcomes within the maximum sensible important cases. Therefore, including some element in the phase spectrum of the image one could basically trade the initial image structure [12]. The above phenomenon might be effectively used for image encryption. Moreover, the localized conversation noise is spread over all reconstructed photograph that makes it invisible contrary the above stated technique where localized noise conditions neighbourhood noise associated with blockading effect.
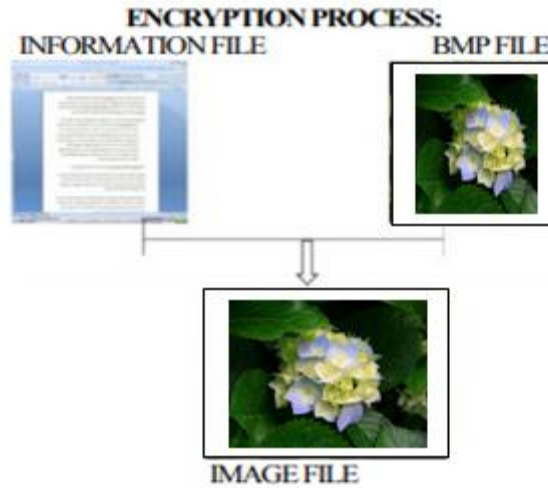
ENCRYPTION PROCESS:

INFORMATION FILE   BMP FILE

IMAGE FILE

Fig.3Encryption technique

DECRYPTION PROCESS:

BMP FILE
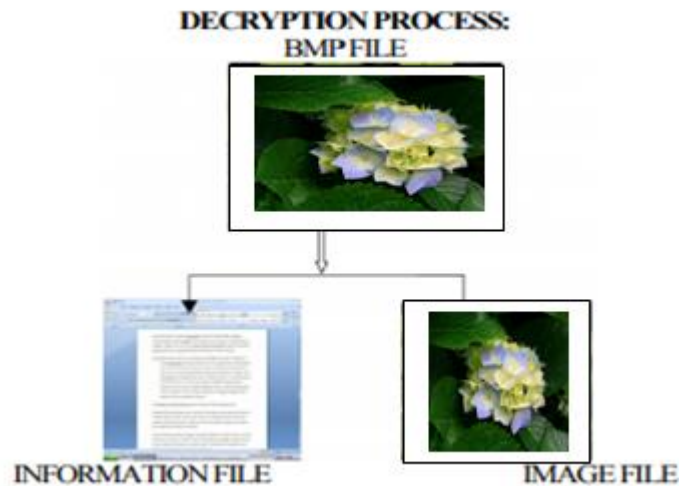
INFORMATION FILE   IMAGE FILE

Fig.4Decryption technique

To send a message, a source text, an image in which the textual content must be embedded, and a key are needed. The key's used to useful resource in encryption and to decide where the information needs to be hidden within the photograph. Either any other photograph or a quick text may be used as a key. To obtain a message, a supply photograph containing the data and the corresponding key are each required. The end result will appear inside the text tab after decoding. Images ought to comprise as many colours as viable. It is likewise excellent if many of the colorations are comparable. At least four colours are required. Microsoft .Net framework prepares a huge amount of device and options for programmers that they simples programming. One of .Net equipment for photographs and photos is auto-converting most sorts of pics to BMP format. I used this tool on this software

called "Steganography" that is written in C#.Net language and you can use this software to hide your statistics in any sort of pics without any changing its format to BMP (software program converts internal it).

CONCLUSION

Steganography is powerful and effective for verbal exchange of secret data. For the image steganography diverse methods have been proposed. On this paper, we advise a method that hides the name of the secret messages inside the picture by the use of mat lab. Mat lab is an always simplest a programming language. It offers more safety for secret communications. Consequently the capacity of the hiding process to hide mystery messages is also excessive inside the proposed approach. In this approach the software program will facilitates to lessen manual time and effort. It additionally gives protection. The proposed machine is consumer-friendly and every aspects of this system can be without difficulty understood and the consumer can operate the device without difficulty. In addition this concept can be implemented to video documents and audio files and also it could be carried out to exclusive kind of documents and different kinds of images.

REFERENCES

[1]   W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems , vol. 35, Issues 3&4 1996 Journal, pp. 313-336.

[2]   T.Moerland, "Steganography and Steganalysis", www.liacs.nl/home/tmoerlan/privtech.pdf, May 15, 2003.

[3]   Jamil, T., "Steganography: The art of hiding information is plain sight", 1999 IEEE Potentials, 18:01.

[4] Moerland, T., "Steganography and Steganalysis", www.liacs.nl/home/   tmoerl/privtech.pdf.   Leiden Institute of Advanced Computing Science.

[5]   NasirMemon R. Chandramouli. Analysis of lsb based image steganography   techniques. In , 2001 Proceedings of IEEE ICIP.

[6]   R. B¨ohme and A. Westfeld.Breaking cauchy model-based JPEG steganography   with   first order statistics. , 2004 9th European Symposium on Research Computer   Security 3193:125–140.

[7]   Silman, J., "Steganography and Steganalysis: An Overview", 2001 SANS Institute.

[8]   Souvik Bhattacharyya. andGautamSanyal. An image based steganography model for   promoting global cyber security. In, 2009 Proceedings of International Conference on   Systemics, Cybernetics and Informatics, Hyderabad, India

[9]   A DWT Based Approach for Image Steganography.(Po-Yueh Chen andHung-Ju Lin)International Journal of Applied Science and Engineering2006.

[10]   Khalil Challita, HikmatFarhat, Combining Steganography and Cryptography:New   Directions, International Journal on New Computer Architecturesand Their Appli- cations (IJNCAA) 1(1): 199-208. The Societyof Digital Information and Wireless   Communications, 2011 (ISSN 2220-9085).

[11]   Steganography: The Art of Hiding Text in Image using MatlabShikhaVidhuKiran   DuttM.tech (cse) Deptt of CSE, JCDV Sirsa& GJU, Lectin deptt of CSE, JCDV   Sirsa& GJU, Hissar, IndiaVolume 4, Issue 9,September 2014 ISSN: 2277 128X)

[12]   A Survey on Image Steganography Algorithms and Evaluation.ArashHabibi   Lashkari,   Azizah Abdul Manaf, Maslin Masrom, and SalwaniMohdDaud.Springer   Verlag Berlin Heidelberg 2011.

[13]   An Information Steganography System Based on Channel EncodingXuan- dong Sun,and Xiao-jingWang.E. Mao, L. Xu, andW. Tian (Eds.):ECICE 2012, AISC 146,   pp.131137.

[14]   Secure Image Hiding Algorithm using Cryptography and SteganographyMs.   HemlataSharma,Ms. MithleshArya, Mr. Dinesh Goyali.IOSRJournal of Computer   Engineering   (IOSR-JCE)   e-ISSN: 2278-0661,ISSN: 2278-8727Volume 14, Issue 5   (Jul. - Aug. 2014), PP 01-06www.iosrjournals.org

[15]   Enhance Security in Steganography with cryptography Chandra PrakashShukla1,   Ramneet   S Chadha2, Abhishek Kumar3 Student,MTech(IT),CDAC Noida , India   International   Journal   of AdvancedResearch in Computer and Communication   Engineering Vol. 3, Issue 3,March 2014.

[16]   Steganography with Cryptography in Android AkshayKandul, AshwinMore, Omkar   Davalbhakta, RushikeshArtamwar, and Dinesh Kulkarni, Springer International   Publishing   Switzerland   2015   S.C. Satapathy et al.(eds.), Proc. of the 3rd Int. Conf. on   Front. of Intel

[17]   A DWT Method for Image Steganography Prof.Barnali Gupta Banik andProf. Samir   K. Bandyopadhyay,University of Calcutta India.Volume 3,Issue 6, June 2013 ISSN: 2277   128X, Steganography and Its Technique:Technical Overview Gulshan   Shrivastava,   AakankshaPandey andKavitaSharma,(2013).

[18]   Souvik Bhattacharyya. AndGautamSanyal. An image based steganographymodel   for romoting global cyber security. In, 2009 Proceedings ofInternational Conference on Systemics, Cybernetics and Informatics,Hyderabad, India.

[19]   A DWT Based Approach for Image Steganography.(Po-Yueh Chen andHung-Ju Lin)International Journal of Applied Science and Engineering2006.

[20]   Khalil Challita, HikmatFarhat, Combining Steganography and Cryptography:New   Directions, International Journal on New Computer Architecturesand Their Appli- cations (IJNCAA) 1(1): 199-208. The Societyof Digital Information and Wireless   Communications, 2011 (ISSN 2220-9085).