IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013
ISSN: 2320 - 8791
www.ijreat.org

FORUM BASED SECURED INFORMATION SHARING USING STEGANOGRAPHY

K.Kavitha[1] R.Paveethira[2] and S.Yamuna[3]

[1, 2, 3] Department of Computer Science and Engineering
SNS College of Engineering, Coimbatore

ABSTRACT

Steganography and steganalysis are important topics in information hiding. Steganography refers to the technology of hiding data into digital media without drawing any suspicion, while steganalysis is the art of detecting the presence of steganography. The proposed system lets user hide data in more than a single carrier file. When hidden data are split among a set of carrier files you get a carrier chain, with no enforced hidden data theoretical size limit. The proposed for Text Documents and Language Coding files uses snow to conceal messages in ASCII text by appending whitespaces to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected. Encrypts the content using AES. The proposed system creates a Knowledge sharing forum. This project is a online web App which is similar to online forum sites where users will discuss on multiple topics.etc. In present scenario internet had became one of the fast growing communication hub where users want to share and discuss information with others from all over the world and gain knowledge.

Keywords: Steganalysis, Carrier file, Stego-medium, Cover medium.

1. Introduction

Steganography comes from the Greek and literally means, "Covered Writing". It is one of various data hiding techniques, which aims at transmitting a message on a channel where some other kind of information is already being transmitted. This distinguishes steganography from covert channel techniques, which instead of trying to transmit data between two entities that were unconnected before.

The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. The only missing information for the enemy is the short easily exchangeable random number sequence, the secret key, 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 is closely related to the problem of hidden channels secure operating system design, a term which refers to all communication paths that cannot easily be restricted by access control mechanisms. In an ideal world we would all be able to sent openly encrypted mail or files to each other with no fear of reprisals. However there are often cases when this is possible, either because the working company does not allow encrypted email or the local government does not approve of encrypt communication (a reality in some parts of the world). This is where steganography can come into play.

Data hiding techniques can also be classified with respect to the extraction process: Cover Escrow methods need both the original piece of information and the encoded one in the order to extract the embedded data. Blind or Oblivious schemes can recover the hidden message by means only of the encoded data.

Steganography has developed a lot in recent years, because digital techniques allow new ways of hiding information's inside other information's, and this can be valuable in a lot of situations. The first to employ hidden communications techniques with radio transmissions were the armies,

because of the strategic importance of secure communication and the need to conceal the source as much as possible.

Nowadays, new constraints in using strong encryption for messages are added by international laws, so if two peers want to use it, they can resort in hiding the communication into casual looking data. This problem has become more and more important just in these days, after the international Wassenaar agreement, with which around thirty of the major with respect to technology countries in the world

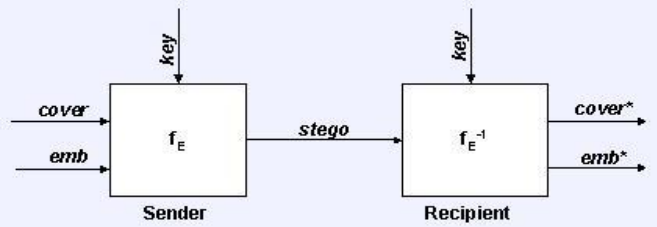
decided to apply restrictions in cryptography export similar to the user ones. Another application of steganography is the protection of sensitive data. A file system can be hidden in random looking files in a hard disk, needing a key to extract the original files. This can protect from physical attacks to people in order to get their passwords, because maybe the attacker cannot even know the some files are in that disk.

The major concern of steganography is stealth, because if an attacker, either passive or active, can detect the presence of the message, from that point he can try to extract it and, if encrypted, to decrypt it. The resistance to attempt at destruction or noise is not required, since we consider the sender and the receiver equally interested in exchanging messages, so that they will try to transmit the stego-medium in the best way they can. If the stego-data can be transmitted over the selected channel, and this is usually the case with all the media that are used, like images or sounds, then the embedded data will be preserved along with them. Thus, data hiding techniques for steganography must focus on the maximum strength against detection and extraction.

As a second request, we would prefer a high data rate, because we will usually want to be able to exchange any amount of data, from simple messages to top secret images. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message, this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obsecured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

Steganographic messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stegotext. For example, the letter size, spacing, typeface, or other characteristics of a cover text can be manipulated to carry the hidden message, only the recipient (who must know the technique used) can recover the message and then decrypt it. Steganography uses in electronic communication

include steganographic coding inside of a transport layer, such as an MP# file, or a protocol, such as UDP.



fE : steganographic function "embedding"
fE-1 : steganographic function "extracting"
cover : cover data in which *emb* will be hidden
stego : cover data with the hidden message

2. Proposed System

The project 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

Encryption is the process of encoding a message in such a way as to hide its contents. Modern Cryptography includes several secure algorithms for encrypting and decrypting

messages. They are all based on the use of secrets called **keys.** A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key.

The larger the cover message is (in data content terms -- number of bits) relative to the hidden message, the easier it is to hide the latter. For this reason, digital pictures (which contain large amounts of data) are used to hide messages on the Internet and on other communication media. It is not clear how commonly this is actually done. For example, a 24-bit bitmap will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 28 different values of blue. The difference between say 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Therefore, the least significant bit can be used (more or less undetectably) for something else other than color information. If we do it with the green and red as well we can get one letter of ASCII text for every three pixels.

Stated somewhat more formally, the objective for making steganographic encoding difficult to detect is to ensure that the changes to the carrier (the original signal) due to the inject the payload (the signal to covertly embed) are visually (and ideally, statistically) negligible, that is to say, the changes are indistinguishable from the noise floor of the carrier.

2.1 Steganography Terms

Carrier File – A file which has hidden information inside of it.

Steganalysis – The process of detecting hidden information inside of a file.

Stego-Medium– The medium in which the information is hidden.

Redundant Bits– Pieces of information inside a file which can be overwritten or altered without damaging the file.

Payload – The information which is the be concealed.

2.2 Process Description

The following formula provides a very generic description of the pieces of the steganography process:

Cover medium + hidden data + stegokey = stegomedium

In this context, the covermedium is the file in which we will hide the hidden data, which may also be encrypted using the stegokey. The resultant file is the stegomedium (which will, ofcourse be the same type of file as the cover medium). The cover medium (and, thus the stegomedium) are typically image or audio files or text file.

3. System Implementation

3.1 USER ACCOUNT CONTROLLER

This is a web service part which contains the code logic and data base to be accessed by other websites. Coded logic contains the following parts

User Profile

This is used to manage the user profile data onto the database. This assigns a unique account ID to each user.

Registration

This contains a Registration form which gets user input and stores them into the database.

Edit\Delete

User profile modifying is done in this module.

User Data

This module stores the user profile and their website information on the database in addition to their account details. User uploaded data's and their website resource access limits are stored.

Activity Session

This module creates and manages the user activity details in the website.

Session Information

This module stores the details about their session with their login details includes time and type of login onto the website.

3.2 Forum Engine

This module creates a simple, fast and lightweight forum, which allows attaching various extensions to it. This makes it possible for you to have a discussion board, which can be fine-tuned to meet all your requirements perfectly. Created using ASP.NET 2.0 technology. The Forum can be used to launch a website on any particular topic and the users should be able to browse all the content related to the topic in the form of Discussions, Question and Answers, links to other blogs, etc. It will provide rich content site for any site owner targeting to run a site for their product or idea.

The UI will be much richer than the traditional forum sites where there is a Category, and then discussion or threads within a category. In Sub Forum users can post discussions or comments and provide Tags that will help searchers narrow down the posts by tags instead of categories only.

The forum will be Web 2.0 friendly. That means it will have search engine friendly URLs, logins for different login providers, Avatars, OpenID, etc. It will also have an easy to customize site layout that developers and designers can build against easily. The use of AJAX and jQuery will be used to provide a rich user interface for readers and posters and admins.

Forum Features

- Navigation in forums, topics and tags.
- SEO friendly
- Rss feeds and short urls
- Fast quoting
- Full Web administration
- SQL Server database
- Copy and paste installation
- Visual layout and easy theming
- Accessible HTML mark-up and non-intrusive JavaScript
- Alternate Mobile layout template.

3.3 Stego Engine

3.3.1 Encryption

Encryption includes a message or a file encrypting. Encryption involves converting the messages to be hidden into a cipher text. Encryption can be done by passing a secret key. Secret key can be used for encryption of the message to be hidden. It provides security by converting it into a cipher text, which will be difficult for hackers to decrypt. Moreover if the message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message.

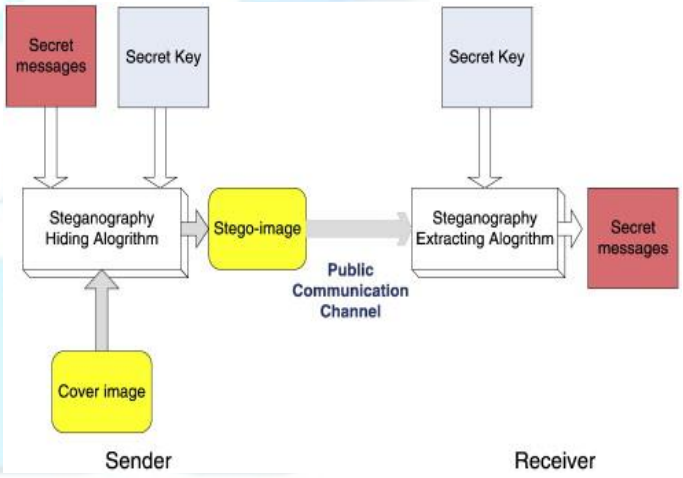


Fig: Encryption and Decryption process

3.3.2 Encoding of the Image Steganography

The encoding process can be described as follows:

a. Choose an initial partition, the original image area is most convenient one used. Specify the control

error; its effective range for generally image is between 2 and 6. Here we use E=4. Suppose the Bivariate Polynomial is f(x,y)+ax+by+cxy+d, get the partition grids of Image A by following the non-uniform rectangular partition algorithm mentioned above.

b. Put the partition grids of Image A onto Image B ang read the gray values of {z} and {z'} for both images over the grids and record of each rectangular sub-area.

c. Hide all of the partition codes and its corresponding gray difference {h} into the four lowest significant bits of each gray byte of Image B. For RGB image, apply the above algorithm three times for R, G and B components separately.

3.3.3 Encoding of the Video Steganography

a. Extract each frame from video stream F and H to RF, GF, BF and RH, GH, BH correspondingly as some static images.

b. For each group of {RF, RH}, {GF, GH}, and {BF, BH}, apply the above image steganography algorithm to hide {RH, GH, BH} into {RF, GF,BF} to form {R2F, G2F, B2F}. Here we should choose a suitable control error so that the length of the partitioning codes does not excess the embedding space of the host. Usually, the control error of 6 is chosen and then the non-uniform rectangular partition is performed, if the embedding length requirement is reached although this may further reduce the reconstruction quality.

c. Reform each set of {R2F, G2F and B2F} to the whole video stream F2 with the codes of the hidden video stream.

4. Encryption And Decryption

4.1 Hide Message

Hiding message is the most important module of steganography. It involves embedding the message into the cover text. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these values often range from 0-255. In order to hide the message, and data is first converted into byte format and stored in a byte array. The message is then encrypted and then embeds each bits into the LSB position of each pixel position. The least significant (rightmost) bit of each 8-bit byte has been co-opted to hide a text message.

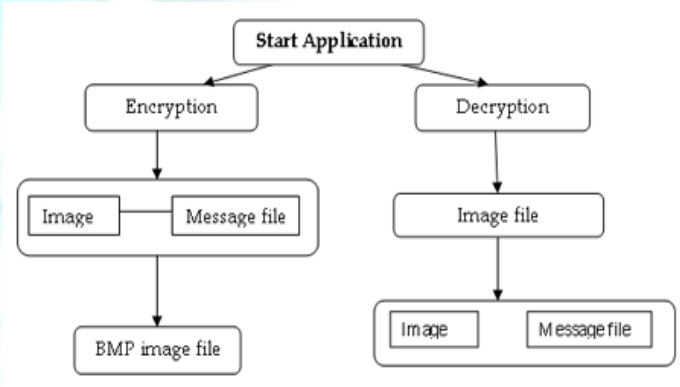


Fig: Encryption and Decryption process for image

4.2 Publisher And Steganalysis

4.2.1 Retrieve Message

It involves retrieving the embed message from the file independent of the file format. Once the message has been retrieved it has to be converted into original message or file. This can be done by reading the embedded data from the master file. The read data will be in the bytes format. This message has to be converted into the suitable output file format.

A. Decoding of the Image steganography

When receiving Image B, follow the decoding process below to extract the hidden image:

a. Extact the codes from Image B. Those are partition number and their corresponding gray difference set of {h}.

b. With the set of {h}, calculate the gray values 1 4 z~z of four vertexes of each sub-area in A. With the set of {z}, solve for the coefficients a,b,c,d of each plane Z+ax+by+cxy+d in each partitioned sub-area.

c. According to each set of {a,b,c,d} and plane coordinates, each sub-area can be re-constructed. All reconstructed sub-areas form the whole original image area A finally.

B. Decoding of the Video Steganography

When receiving the video stream F2, the hidden video can be constructed by following the decoding process below:

a. Divide each frame of the video stream F2 and F into static-image group {R2F, G2F, B2F} and {RF, GF, BF}.

b. Apply the decoding process of image steganography algorithm to extract each hidden frame from {R2F, G2F, B2F} and {RF, GF, BF} to {R2H, G2H, B2H}.

c. Reform each set of {R2H, G2H, B2H} to the whole reconstructed hidden video stream H2.

To test our proposed method to see whether it indeed achieved its objective, we used two sets of images in our experiment.

(a) (b)

New proposed:

The experimental results confirmed that our method could effectively protect host image quality and shorten the overall hiding time when it enhanced the security of the secret image.

5.Conclusion

Image can be partitioned adaptively by following the non-uniform rectangular partition algorithm. The partition codes obtained can be used to reconstruct the original image approximately. A novel image steganography algorithm is designed based on the non-uniform rectangular partition algorithm. Different initial partitions, bivariate polynomials and control errors lead different combination of them as the security key to enhance the security of the steganography algorithm. This paper proposes a novel secure large capacity uncompressed video steganography algorithm. Experimental results show that there is no obvious visual distortion happening in the host video stream while the quality of the reconstructed video stream is also acceptable for the practical use.

Acknowledgement

The authors would like to thank Director cum secretary, Correspondent and Principal of SNS College of Engineering, Coimbatore for their motivation and constant encouragement. The authors would like to thank the faculty Members of Department of Computer and Engineering for the critical review of the manuscript and for their valuable input and fruitful discussions. Also we take privilege in extending gratitude to their family members and friends who rendered their support throughout this research work.

References

[1] Ross J. Anderson and Fabien A.P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.

[2] T Mrkel,JHPEloff and MS Olivier ."An Overview of Image Steganography," in Proceedings of the fifth annual Information Security South Africa Conference, 2005.

[3] MrithaRamalingam, "Stego Machine Video Steganography using Modified LSB Algorithm", in World Academy of Science, Engineering and Technology 74 2011, pp. 502-505, 2011.

[4] Y. C Tseng and H. K Pan, "Data Hiding in 2-color Image" in IEEE Transactions on computers, Vol. 51, No. 7, pp. 873-878, July 2002.

[5] W. Zeng, H. Ai and R. Hu, "A Novel Steganalysis Algorithm of Phase Coding in Audio Signal," Proceedings of the 6th International Conference on Advanced Language Processing and Web Information Technology, pp. 261 – 264, August 2007.

[6] SLSB: Improving the Steganographic Algorithm LSB Juan José Roque, JesúsMaríaMinguet Vol.71,No. 9, pp. 873-878, July 2004.

[7] Farid, H.: "Detecting hidden messages using higher-order statistical models". Proc. IEEE International Conference on Image Processing (ICIP '02), vol. 2, Rochester, NY, USA. 905–908 September (2002)