ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Research on Analysis of Different Image Steganography Techniques

Ms. Anshu Sharma*, Dr. Deepti Sharmas
Department Of Computer Science, Lingayas University, Faridabad, India
anshu.atri25@gmail.com

Abstract

Steganography means the process of thrashing information by embedding messages within other. Information can be in the form of text, audio, video. There are several approaches for the categorization of Steganography Techniques. There are various Steganography techniques present in the market but the end user who is not a technical expert often confuses in the choice of which tool to use and what are the advantages and disadvantages associated with the various techniques. So, in this paper a detailed survey is done by combining various Steganography with Cryptography techniques.

Keywords: Data Hiding, Image Steganography, AES, DES, LSB (Least Significant Bit).

Introductions

Information Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are being used frequently interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. However, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take electronic, print or other forms. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Confidential information about a business‘s customers or finances or new product line can fall into the hands of a competitor. Such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization including: securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

Information Hiding Techniques

The introduction of the various processes of the last decades have continuously pointed out towards the security requirement levels, especially since the massive utilization of personal computers, networks and the internet with its availability. Many techniques have been developed for avoiding theft of data, controlling quantities of possible copies.

These techniques used for data hiding are:

- Cryptography
- Digital Watermarking
- Steganography

Figure: Information Hiding Technique

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Cryptography

Cryptography[1] is the practice and study of hiding information. The word is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. In modern times, cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies. It's examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

Steganography

Steganography[2] is the art of hiding the fact that communication is taking place, by hiding information in other information. It is the art of concealing a message in a cover without leaving a remarkable track on the original message.

"Steganos" = covered
"Graphie" = writing

Its ancient origins can be traced back to 440 BC.1In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who used steganography first time.[5]

The goal of Steganography[3] is to hide messages inside the images in such a way that does not allow any "enemy" to even detect that there is a secret message present in the image.

Type of Steganography:

There are 4 different types of steganography

i. Text
ii. Image
iii. Audio
iv. Video
v. Protocol

Text Steganography using digital files is not used very often since text files have a very small amount of redundant data. ***Audio/Video Steganography*** is very complex in use.

Image Steganography is widely use for hiding process of data. Because it is quite simple and secure way to transfer the information over the internet.

Image steganography has following types:

a. Transform domain
i. Jpeg
b. Spread spectrum
ii. Patch work
a. Image domain
i. LSB and MSB in BMP
ii. LSB and MSB in JPG

It is most efficient (in term of data hiding) method of image steganography.

Because the intensity of image is only change by 1 or 0 after
hiding the information.

Change in intensity is either 0 or 1 because the change at last bit.

Figure 1.2: Categories of Steganography

Hiding information in text is historically the most important method of Steganography.

An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the internet and all the different digital file formats that it has decreased in importance. Text Steganography using digital files is not used very often since text files have a very small amount of redundant data. Given the proliferation of digital images, especially on the internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for Steganography. In this paper, an image steganographic technique has been proposed.

Materials and methods

Proposed Work

The aim of proposed system is to compare different technique to choose the best one among them. The proposed system can overcome all the limitations of the existing system. In our system we are introducing the entire three concepts to secure the information which is send by the user.

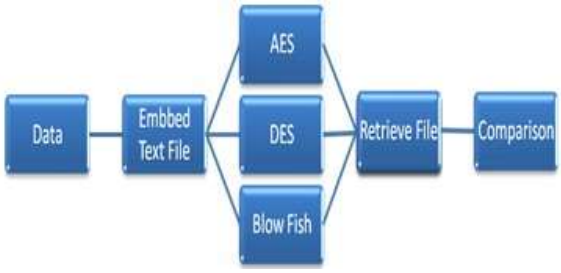
There are various Steganography techniques present in the market but the end user who is not a technical expert often confuses in the choice of which tool to use and what are the advantages and disadvantages associated with the various techniques. For the sake of end user, to make him able to choose the best technique for himself, an analysis needs to done for various techniques illustrating various positive and negative aspects of that technique.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Proposed Model

The aim of proposed system is to compare different technique to choose the best one among them. The proposed system can overcome all the limitations of the existing system. Here we have used LSB Technique for embedding the Text message and the three techniques i.e AES, DES and Blow fish for encrypting and Decrypting the Information before sending it to the client.

Figure: Model of proposed work



Results and discussion

Steganography can be defined as the process of hiding information by embedding messages within other; Information can be in the form of text, audio, video. There are several approaches for the Classification of Steganography Techniques. There are various Steganography techniques present in the market but the end user who is not a technical expert often confuses in the choice of which tool to use and what are the advantages and disadvantages associated with the various techniques. Moreover various techniques have different payload carrying capacity. Apart from this a user needs to take care of various nuts and bolts of the technique with respect to his needs and requirements and thereafter choose the most appropriate technique for user. So, in this paper I have analyzed the embedding of Text message in the Image File and then Encrypted that file using various Encryption and Decryption Technique.

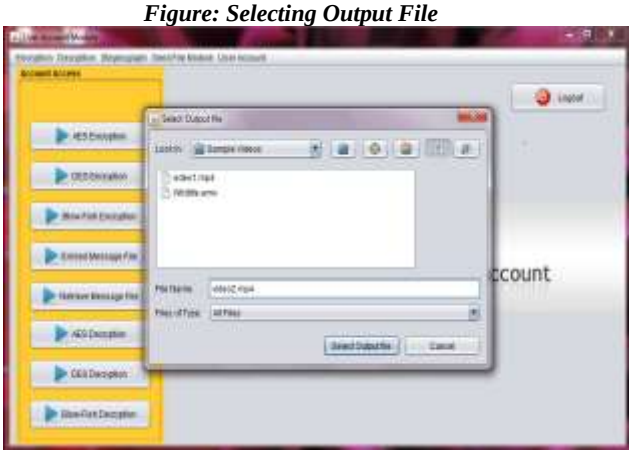
Embedding Text File

To Embed a Text File in a Given Video File, the user will click on the Embed Message File Button. The Select Master File Dialog Box Will appears from where we will select the Master File where Message is to be hidden.

Figure: Selecting Master File

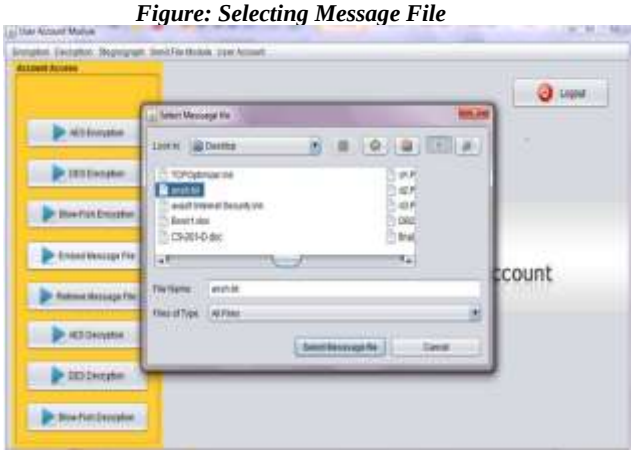
Next, the user would be prompted to name the output file through Select Output File dialog box.

Figure: Selecting Output File



Then, the user needs to select the text file to be hidden, the Select Message File Dialog Box.

Figure: Selecting Message File

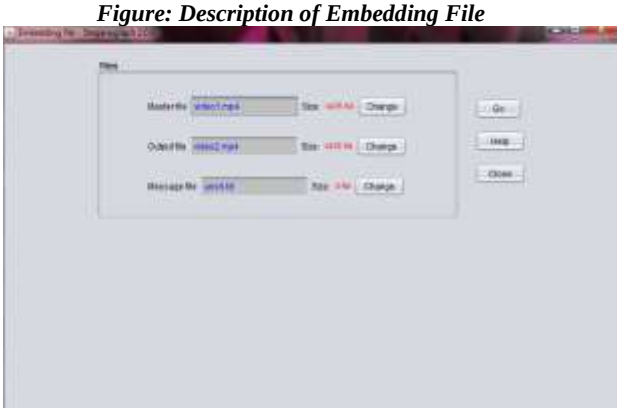


Once the file will be hidden, prompt will appear showing the Master File, Output File and Hidden Message File. This step is used to embedding the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

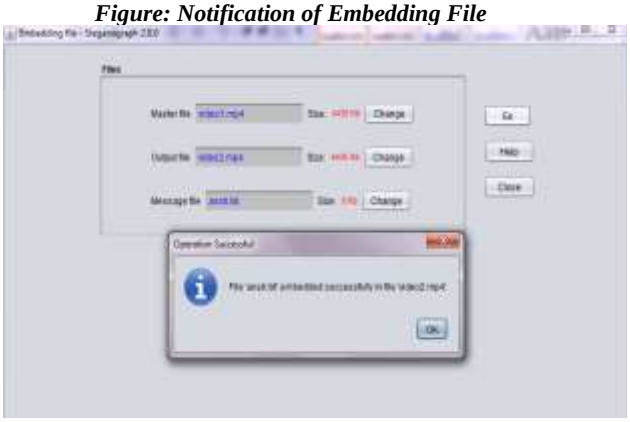
selected file in the given video file. We can also apply any Changes if needed.

Figure: Description of Embedding File



When we click on the Go Button, the following notification would appear once the file is embedded successfully.

Figure: Notification of Embedding File



The embedded file can be then be encrypted and decrypted using various encryption and Decryption technique. Here we have used three main Techniques namely

- AES Encryption and Decryption
- DES Encryption and Decryption
- Blow-Fish Encryption and Decryption

AES Encryption and Decryption

Firstly, for AES Encryption, the user needs to select the Source File and Destination File using the browse option and then give the required key which is used to encrypt the file in which message is Hidden.

Figure: AES Encryption

Once encrypted by AES Encryption, the following notification would appear indicating the file is successfully encrypted.

Figure: File encrypted using AES Technique

The Encrypted file then can be decrypted by the client using AES Decryption. The user will select the Source File and Destination File using the browse option and then use the same key which needs to decrypt the message by which message is Encrypted.

Figure: AES Decryption

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

As we click on the Decrypt Button, the following notification would appear indicating the file is successfully decrypted.

Figure: File decrypted using AES Technique

DES Encryption and Decryption

For DES Encryption, the user needs to select the Source File and Destination File using the browse option and then give the required key which is used to encrypt the file in which message is Hidden.

Figure: DES Encryption

Once encrypted by DES Encryption, the following notification would appear indicating successful encryption.

Figure: File encrypted using DES Technique

The Encrypted file then can be decrypted by the client using AES Decryption. The user will select the Source File and Destination File using the browse option and then use the same key which needs to decrypt the message by which message is Encrypted.

Figure: DES Decryption

As we click on the Decrypt Button, the following notification would appear indicating successful decryption.

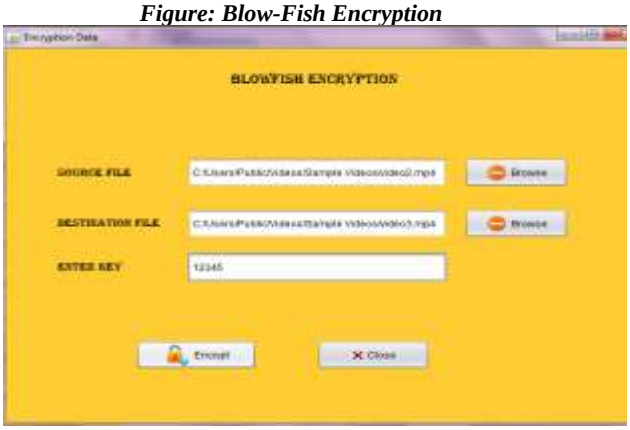
Figure: File decrypted using DES Technique

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Blow Fish Encryption and Decryption

Firstly, for AES Encryption, the user needs to select the Source File and Destination File using the browse option and then give the required key which is used to encrypt the file in which message is Hidden.

Figure: Blow-Fish Encryption

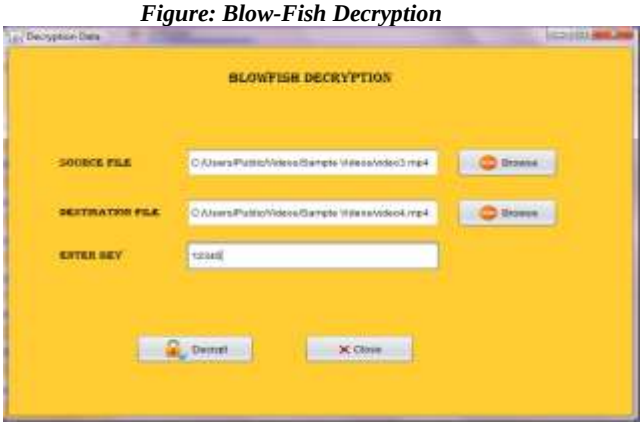


Once encrypted by AES Encryption, the following notification would appear indicating the file is successfully encrypted.

Figure: File encrypted using Blow-Fish Technique

The Encrypted file then can be decrypted by the client using AES Decryption. The user will select the Source File and Destination File using the browse option and then use the same key which needs to decrypt the message by which message is Encrypted

Figure: Blow-Fish Decryption



As we click on the Decrypt Button, the following notification would appear indicating the file is successfully decrypted.

Figure: File decrypted using Blow-Fish Technique

Retrieving Text File

The data which was embedded and encrypted by various algorithms can then be retrieved by the user using the Retrieve Message File tool. Once we click on it The Dilog Box will appear from where we will select the File from which Client will retrieve the Message

Figure: Selecting Master File

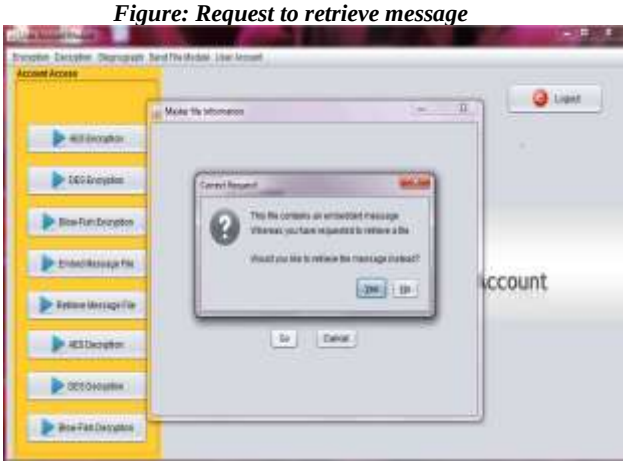
ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The Following dialog box would appear once the user proceeds with the retrieval process of the data which was embedded Showing the Master File and also the Steganography used.

Figure: Master File Information

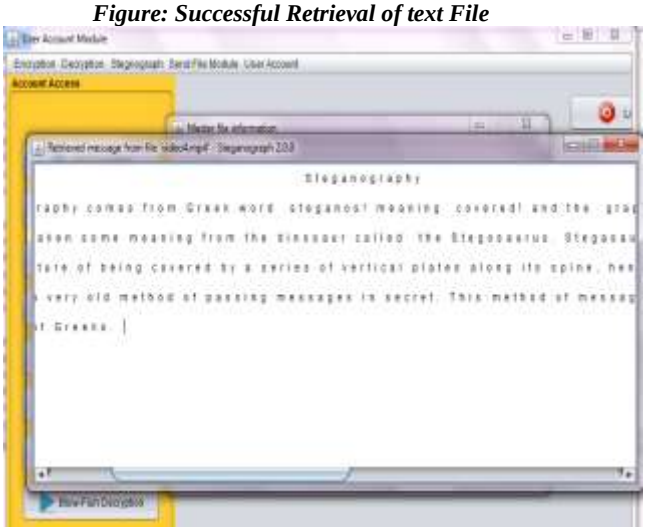
As Client will click on the Go Button, Dilog box will appear showing that File Contains the Hidden Message, if we want to Retrieve the Message then Click yes.

Figure: Request to retrieve message



The Hidden Message File will be Successfully Retrieved.

Figure: Successful Retrieval of text File



Conclusion

There are several approaches for the Classification of Steganography Techniques. Most of them can be seen under substitution systems. Such methods try to substitute the redundant bits of the signal into a secret message but the main disadvantage is weakness against cover Modifications and we didn't find the detailed Comparison of different Image Steganography techniques. There are various Steganography techniques present in the market but the end user who is not a technical expert often confuses in the choice of which tool to use and what are the advantages and disadvantages associated with the various techniques. So, For the sake of end user, to make him able to choose the best technique for himself, the detailed Comparison needs to done for various techniques illustrating various positive and negative aspects of that technique and also how various techniques can be combined to provide more security by combining cryptography with steganographic techniques.

References

1. *W. Stallings, —Cryptography and Network Security: Principles and Practice, N Prentice- Hall, New Jersey, 1999*
2. *J. Caldwell, —Steganography, United States Air Force, http://www.stsc.hill.af.mil/crosstalk/2003/06 /caldwell.pdf, June 2003.*
3. *Eric Cole, Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication",Wiley Publishing Inc. (2003).*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

4. *David Kahn,"The History of Steganography", Proc. of First Int. Workshop on Information Hiding,*
5. *Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7*
6. *Benderr, D. Gruhl, N. Morimoto and A.Lu, "Techniques for Data Hiding", IBM System"s Journal, Volume 35, Issue 3 and 4, 1996, p.p., 313-336.*