Impact Factor: 4.14 (Calculated by SJIF-2015)

e- ISSN: 2348-4470
p- ISSN: 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

Steganography Using Reversible Texture Synthesis

Steganographic techniques to improve safety of confidential data

Trupti Bhosale, Sayali Dhumal,Pravin Ghadge,Omkar Jarande

[1,2,3,4]*Computer Department Zeal college*

ABSTRACT:-*Steganography is the method of hiding a secret information in a specified medium like image, video, Audio. It can be used to carry out hidden exchanges of information and to provide privacy for the user. This can be achieved by taking any multimedia as a carrier.The data transmission is not secure because of attacks by intruder or attacker,So stegnography is attractive solution for this problem.The secret information should be embedded in the carrier medium in such a way that the attackers could not be able to find the existence of it.the security of the secret data and stego image or video quality should be maintained in both the embedding and recovering process.*

Keywords**:** *Steganography, audio steganography, bitwise operator, data embedding, DES algorithm, texture synthesis*

I. INTRODUCTION

Steganography means "Covered Writing" which is derived from the Greek language. The main purpose of steganography is to send secret or confidential message under the cover of a carrier signal. Two main properties of any steganographic technique are good imperceptibility and sufficient data capacity. Good imperceptibility ensures that the embedded message is difficult to detect. Steganography and cryptography are mainly used for security, but both are different. The main goal of cryptography is to communicate securely by changing the data into a form that an attacker cannot understand. The steganography techniques are used to hide the presence of the message and make it difficult for attackers to find the occurrence of the message. The research on steganography concentrates on images, audio, and video as cover media .The basic idea behind cryptography is that you can keep a message a secret by encoding it so that no one can read it. If a good cipher is used, it is likely that no one, not even a government entity, will be able to read it. Then the information is embedded into a cipher text. This is done according to the embedding algorithm and a secret key that performs the actions of the embedding process. This process outputs a steganogram that has the information hidden inside.

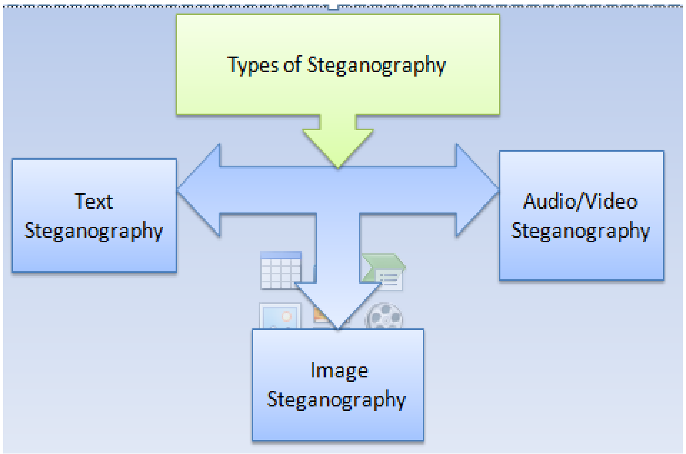


IMAGE STEGANOGRAPHY

An image in which data is embedded is called as a cover image andthe image which is used for carrying secret data is termed as stego image. A good data hiding method should be
capable of evading visual and statistical detection while providing an adjustable payload. Impossibilities of data hiding is commonly achieved by exploiting the weakness of the human auditory and visual systems, using the techniques, for example changing the least-significant bits of pixels of cover image to embed information , or shifting lines, words, or characters by a small amount in an image containing text. Other works hide information by adding redundant data, or making use of alternative representations of electronic data. For example hidden information can be added in a text document by adding tabs and spaces at the end of the line. The different combinations of the color palette entries in a GIF

image can be used to embed secret data into the image file. Sometimes the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, after the hidden data have been extracted out some permanent distortion has been occurred to the cover media. Reversible Steganography scheme has the ability to embed the secret data into a host image and then recover the host image without losing any information when the secret data is extracted. This should be overcome by using some techniques. Reversible steganography is also known as reversible data hiding. No modification is done in the digital representation of the cover image when reversible data hiding method is used. The Reversible data hiding is used in the field of medical, military, legal applications etc.

AUDIO STEGANOGRAPHY

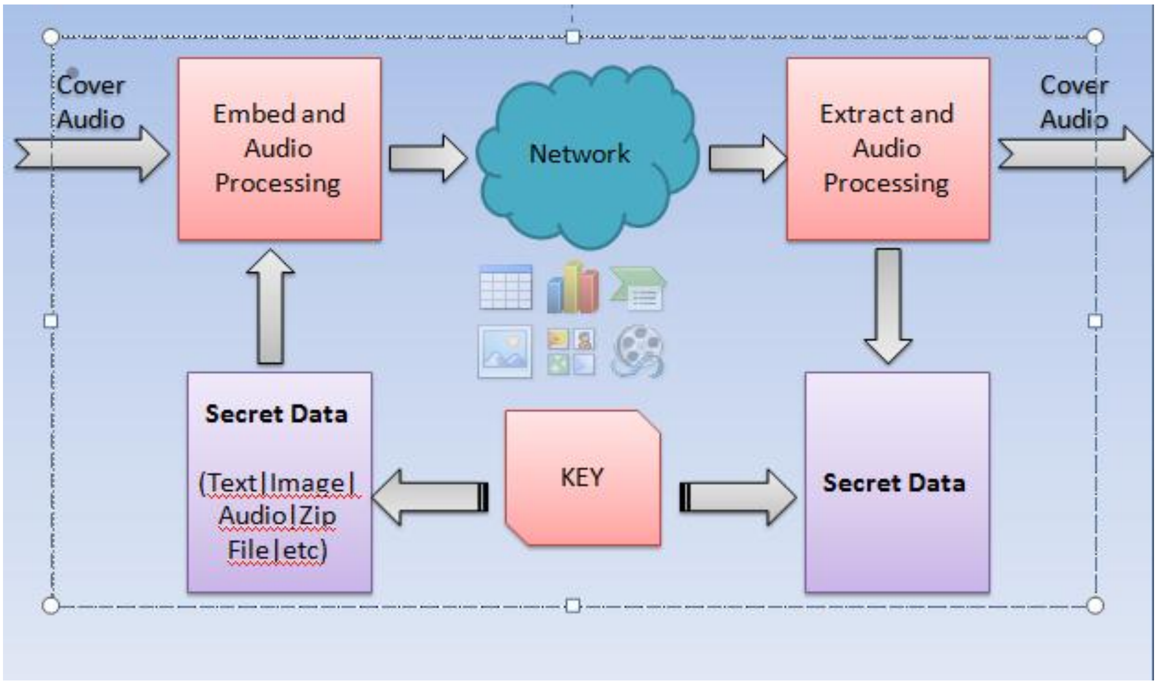
Hiding the messages into digital sound is called as audio Steganography. It is a more difficult process than embedding messages in other media. Using audio steganography uses can hide the message in MP3 like sound files. The Human auditory system (HAS) has the feature to get exploited in the process of audio Steganography. Auditory perception uses critical band analysis in the inner ear where a frequency to location transformation takes place along the basilar membrane. Received sound's power spectra is not represented on a linear frequency scale but on limited frequency bands called critical bands.

VIDEO STEGANOGRAPHY

Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. The least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. In this project, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation.

II. PROPOSED SYSTEM

This system will do the analysis and encrypt the secret message in cover media with the help of efficient algorithm. System we will be using input and output buffer for encrypting and decrypting our information. This system will provide a good and a efficient method for embedding the data from attackers and sent safely to its destination. This proposed system will not make the change in the size of the file after encoding of data in an audio file. Encryption and Decryption techniques are used to make the security in data transmission.


Cover Audio
Embed and Audio Processing
Network
Extract and Audio Processing
Cover Audio
Secret Data
(Text|Image|Audio|Zip File|etc)
KEY
Secret Data

DES (Digital Encryption Standard):

1) DES is used to do Encryption and decryption of data in 64-bit block of cipher text.
2) DES has 16 rounds, means the algorithm is repeated 16 times to get the cipher text
3) It has been observed that the number of rounds is proportionally exponential to the amount of time required to find a key.
4) If the number of rounds increases, the security of the algorithm will increase exponentially
5) This project "DES (Digital Encryption Standard)" is based on client server technology
6) The sender will send the encrypted file using internet connection. On the other side the receiver will receive the file and decrypts the file by using the same private key used by the sender.

More security = **Bitwise operator:**
1) Shift the bits slightly (>> and << bitwise operators) as determined by characters in the key
2) Sorts out the problem of having an odd or even number of bits
3) Takes the byte[] array as encrypted message, and divide it in two halves around i.e. a b c d e f would become d e f a b c
4) If a long key is to be used then only some of the Key is right, then first part of cipher text will still be decrypted.
5) Shuffles the file Bytes in the blocks of key.length(). This method is powerful and good for encryption. The problem is contradiction with the fact, that sometimes, when a short text-file is encrypted, some of the 'central' text is still partially scrambled.
6) The keyStream() function accepts the user key and Make it large up to (key.length()*key.length() + key.length())*128,This will surely improve the security issues.

III. CONCLUSION

Steganography especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. These methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of computer era. Although the techniques are still not used very often, the possibilities are endless. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly.

IV. REFERENCES

[1] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26-34, 1998.
[2] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," Security & Privacy, IEEE, vol. 1, no. 3, pp. 32-44, 2003.
[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.
[4] Y.-M. Cheng and C.-M. Wang, "A high-capacity steganographic approach for 3D polygonal meshes," The Visual Computer, vol. 22, no. 9, pp.845-855, 2006.
[5] S.-C. Liu and W.-H. Tsai, "Line-based cubism-like image—A new type of art image and its application to lossless data hiding," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1448-1458, 2012.