Concealing of Deets using Steganography Technique

Sudha S[1], Deebika G[2], Dhivya L[3], Assistant Professor Susan Mano Derry V[4]

[1,2,3]Students, Dept. of Electronics Engineering, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu
[4]Assistant Professor, Dept. of Electronics Engineering, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu

---

Abstract – *The project proposes the enhancement of security system for secret data communication through multi plane image data embedding in image. A given input audio is converted to any one plane process. After plane separation, the data hider will conceal the secret data into the image pixels. The data hiding technique uses the AES replacement algorithm for concealing the secret message bits into the input image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the image pixels STEGO image to get the information about the data. Finally the performance of this proposal in Color Image and data hiding will be analyzed based on audio and data.*

***Key Words*: Security, Multiplane image, AES replacement algorithm, STEGO image, data hiding, audio and data.**

1. INTRODUCTION

Steganography is a method of hiding the information for invisible communication. It is similar to cryptography, where to secure communications from third parties by make the data not understood, steganography techniques is used to hide the message itself from an observer and there is no knowledge of the existence of the message in the first instant. In sometimes, the sended encrypted deets will arise suspicion while invisible deets will not do so. Both can be combined to produce better protection of the deets. In this scenario, the steganography fails and the deets cannot be find if a cryptography technique is used. Hiding deets in audio format inside images is a new hiding technique nowadays. An image with a secret information in the form of audio inside can be easily spread over the World Wide Web or in a news groups. To hide deets inside an image without changing its visible nature, the main source can be changed in noisy areas with many color differences, so minimum attention will be need to the modification.

2. OBJECTIVE

The objective of this project is to provide an efficient deets concealing technique and encryption of the data in which the image and the audio can be retrieved independently without any loss. Hiding deets in image is the most important technique of steganography. The method was to conceal a secret deet in every nth letter of every word of a text message. After the booming of Internet and various types of digital file formats it got reduced in importance. Text steganography using digital files is not used very often because the text files have a very small amount of data redundancies.

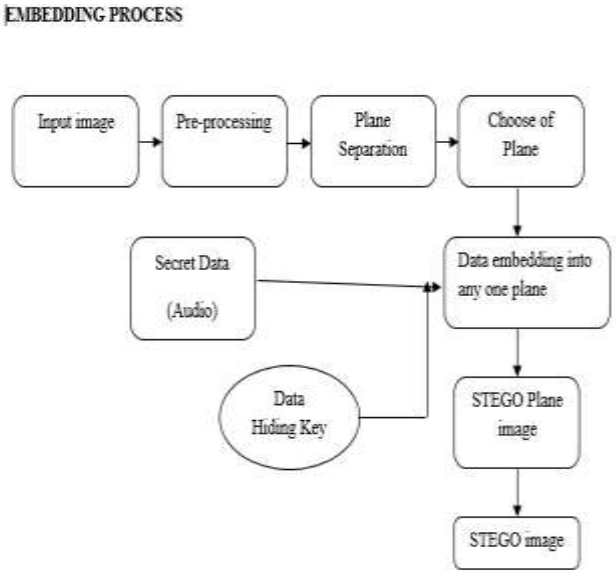
3. EXISTING SYSTEM

Cryptography is an existing physical technique that scrambles the deets by rearranging and substitution of body by making it unreadable to anyone except the authorised person can capable of unscrambling it. With the volume of sensitive Internet transaction that occurs daily, the profit of securing the deets using cryptographic process becoming a major goal for lot of organizations.

4. PROPOSED SYSTEM

Reversible encrypted deets concealing in encrypted audios using chaos encryption, Asymmetric key encryption and adaptive least significant bit replacement technique. Steganography is used to hiding the cover deets in unpredictable multimedia information and is often used in secret communication between unknown parties. Steganography is a method of encryption of hiding of deets among the bits over a cover file, such as a text or an audio file. This method replaced unused or insignificant bits with the secret deets. Steganography is not as robust to attack and hence the embedded deets are vulnerable to crack it.

5. BLOCK DIAGRAM



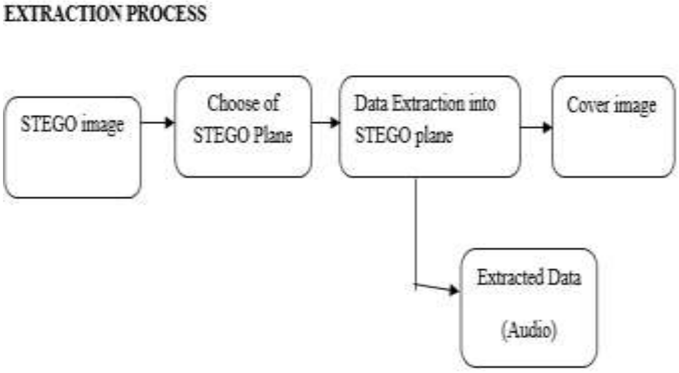


Fig -1: Block diagram

6. SYSTEM DESIGN

6.1. Encryption:

Encoding the contents of the deets in such a way that it conceals its contents from the third person. Cipher text results that it from plain text by applying the key for encryption.

6.2. Decryption:

The process of recovering the cipher text to the plain text.

6.3. Key:

Encryption and decryption process usually make the use of a key, and the coding method in decryption can be done only by knowing the proper key. Hash function generates a digest of the deets. Substitution of cipher text involves by replacing an alphabet with another character of same alphabet set. Mono-alphabet system uses a single alphabet set for the substitution. Poly-alphabet system uses multiple alphabet set for substitution.

7. METHODOLOGY

7.1. Encryption password:

The password doesn't get embed in the image. The password is used to influence how the hidden deets are to be written. Then the end of user want to extract the concealed deet, they must apply the password and the password is used to hide the deets gets read back. If they did not put the correct password, the deets retrieved will not look right. If we put in enough error detective code, you will detect it with relatively more probability whether the deets was retrieved absolutely. The cover image save the messages as a stego file. It will do the similar when user want to extract the deets from stego image. The user needs to give the right password.

7.2 Scanning:

A scanning pattern is a pattern by which the pixels are accessed to embed the deets. Instead of embedding the first k bit in first pixel, second k bits in second pixel and so on, the deet bits are embed in pseudo-random order. We can use three scan methods Raster scan method, snake scan, and Z scan method. Each in both horizontal and vertical position embedding schemes. In Raster horizontal scanning, the concealed deets are embedded in row wise manner. After embedding the deets in a row, the next row is started scanning from the first pixel. In Raster scanning, vertical scanning is done vertical and column wise manner.

7.3. Decryption method:

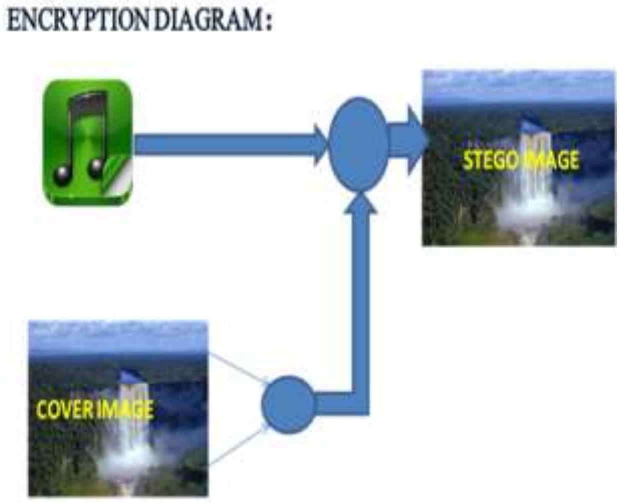
The activity of converting the deets from code into plain text i.e., "a secret key or a password is required for decryption". Decryption is the process for transformation of data that has been unreadable and through encrypt back to its unencrypted form. In decryption of data, the module extracts and convert the garbled deets and transform it to text to audio that are easily understandable and not only by the reader, but it also by the system. Decryption process may be accomplished by manually or automatically. It may be also performed by a set of key or passwords.

7.4. S Box age:

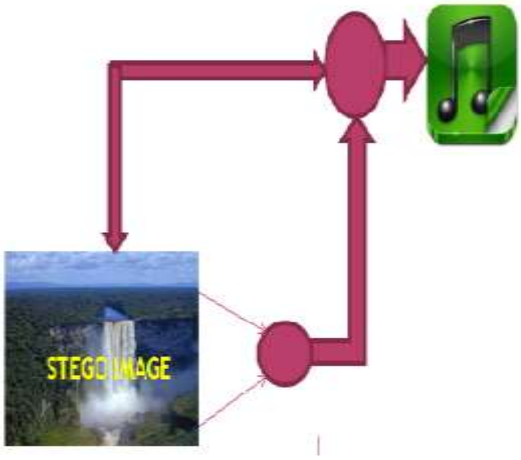
The substitution of bytes one by one of the comparable limited field is finished by the substitution tables. They utilize the extended key capacities for the encryption and decoding for the substitution.

7.5. Discover image:

In the s box age methodology the underlying advance is to locate the opposite augmentation of all the limited field components .The statement of locate the reverse is given in the underlying advance, which is the information parameter. The info byte and the modulo polynomial are to be rearranged by ventures of the reversal method in the posting.



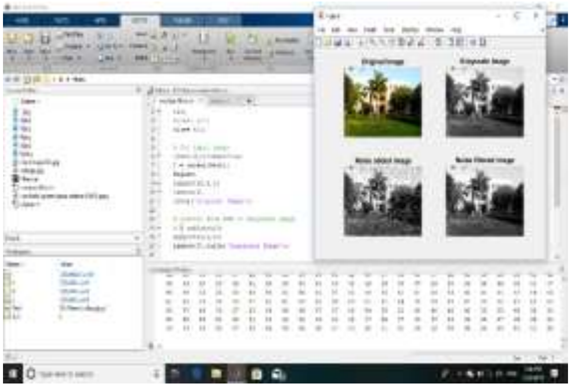
AUDIO OUTPUT:

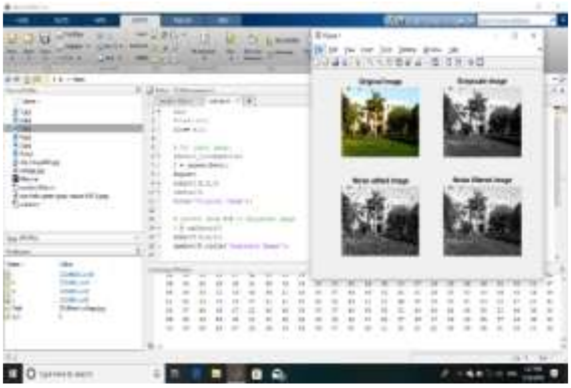


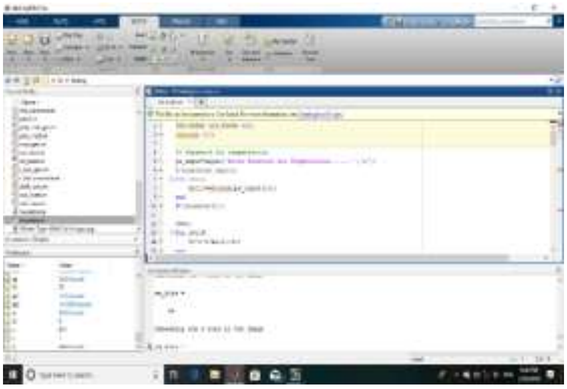
Hardware Requirements

- Processor : Any Processor above 2GHZ
- RAM : 2 GB
- Hard Disk : 250GB
- MATLAB is a logical programming language stage which gives solid scientific help to actualizing of cutting edge calculations. It is hence that MATLAB is generally utilized by the picture handling and PC vision network. New calculations are all around liable to be actualized first in MATLAB, to be sure they may just be accessible in MATLAB.

SAMPLE PICTURES:







3. CONCLUSION

The objective of the proposed steganography calculation decline the blurred pixels in each edge so as to build the installing limit. The proposed calculation is to improve the implanting limit, keeps up the nature of the stego sound progressively productive, basic, fitting and precise than other calculation, just as it makes the mystery information increasingly secure.

REFERENCES

1) R. Anderson and F. Petitcolas, "On the points of confinement of steganography" IEEE Diary of Chose Regions in Correspondences, Vol. 16, No. 4, May 1998.

2) Niels Provos, Dwindle Honeyman,"Hide and Look for: A Prologue to Steganography," IEEE PC society, 2003.

3) K B Raja, Venugopal K R and L M Patnaik, "A Protected Stegonographic Calculation utilizing LSB, DCT and Picture Pressure on Crude Images",Technical Report, Bureau of Software engineering and Building, College Visvesvaraya School of Designing, Bangalore College, December 2004.

4) An outline of picture steganography by T. Morkel, J.H.P. Eloff, M.S. Olivier. Data and PC Security Design (ICSA) Exploration Gathering Branch of Software engineering College of Pretoria, 0002, Pretoria, South Africa.

5) Johnson, N.F. Jajodia, S."Exploring Steganography: Seeing the Inconspicuous", PC Diary, February 1998.

6)"Detecting LSB Steganography in Shading and Dark Scale Pictures" Jessica Fridrich, Miroslav Goljan, and Rui Du State College of New York, Binghamton.

7) Ran-Zan Wang, Chi-Tooth Lin, Ja-Chen Lin,"Hiding information in pictures by ideal tolerably critical piece substitution" IEE Electron. Lett. 36 (25) (2000) 20692070.

8)Hiding information in pictures by basic LSB substitution by Chi-Kwong Chan, L.M. Cheng Bureau of PC Designing and Data Innovation, City College of Hong Kong, Hong Kong Got 17 May 2002.

BIOGRAPHIES

Sudha S
Pursuing Degree in Electronics and Communication Engineering in Jeppiaar SRR Engineering College, Chennai, Tamil Nadu.

Deebika G
Pursuing Degree in Electronics and Communication Engineering in Jeppiaar SRR Engineering College, Chennai, Tamil Nadu.

Dhivya L

Pursuing Degree in Electronics and Communication Engineering in Jeppiaar SRR Engineering College, Chennai, Tamil Nadu.

Susan Mano Derry V

M.E., Assistant Professor ECE in Jeppiaar SRR Engineering college from Tamil Nadu, India.