GALGOTIAS UNIVERSITY

School of Computng Science and Engineering

PROJECT

Image Steganography with 3 way Encryption

Group –BT3104

Group Members:

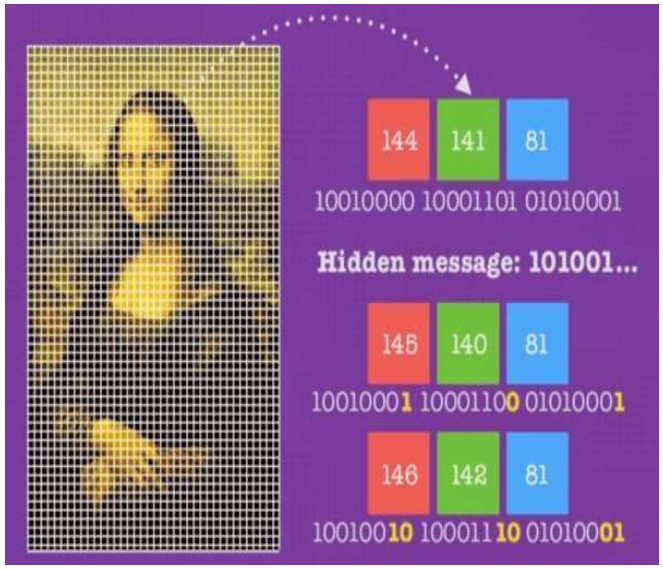
1)Vansham Rastogi (19SCSE1010113)
2)Satyam Kr.Tiwari (19SCSE1010314)

Guide Name:

Mr.S.Rakesh

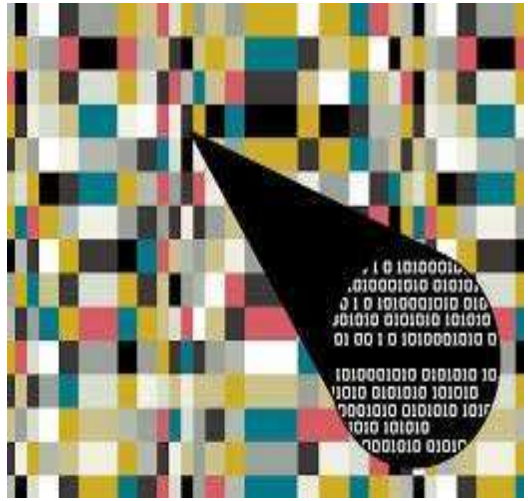
Steganography

- Steganography is the science and practise of concealing information within items in such a way that the viewer believes the object is empty. Simply described, it is the act of concealing information such that only the intended recipient sees it.
- Steganography is the technique of hiding private or sensitive information within something that appears to be nothing be a usual image.
- Steganography involves hiding Text so it appears that to be a normal image or other file.
- If a person views that object which has hidden information inside, he or she will have no idea that there is any secret information.



How Image steganography works?

- It lets user to send text as secrete message inside an image file, user uploads the image and enters the text to send secretly, and gives a key or a pass word to lock the text, what this key does is it encrypts the text, so that even if it is hacked by hacker he will not be able to read the text.
- We will need the key to decrypt the hidden text.
- User then sends the image and key to the receiver and receiver first opens the image, and then he enters the key or password for decryption of text, he then press decrypt key to get secret text of the sender.
- By using this method we can double ensure that our secret message is sent secretly without outside interference of hackers or crackers.
- If sender sends this image in public others will not know what is it, and it will be received by receiver.



What does this system consist of?

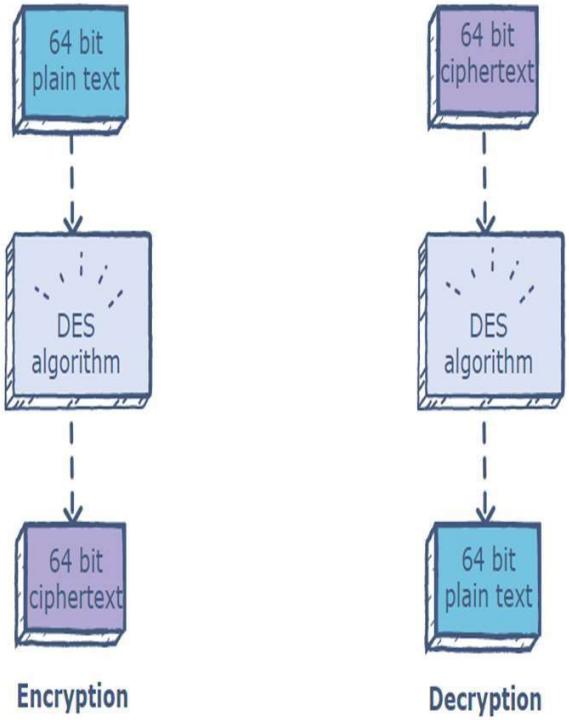
1. **Registration:**
- To access the core system, user first need to register themselves by providing required details.
2. **Login:**
- After registration, user may login into the system.
3. **Algorithm Selection:**
- Here, user will select the algorithm such as DES (Data Encryption Standard), AES (Advance Encryption Standard) or LSB (Least Significant Bit) for encrypting data into image file.
4. **Image Selection:**
- Here, User selects an image for sending a secret message.
5. **Entering Text:**
- Here, User enter/inputs the text that is to be hidden in the image.
6. **Setting Password and Encrypting the Data:**
- User sets a password and use the encryption technique to encrypt the data.
7. **Sharing:**
- After hiding the text with the encryption technique, user saves the image a then sends it to the other party i.e. Receiver.

{1st Way Encryption Method}

Data Encryption Standard[DES]

Data Encryption Standard (DES) is a block cipher algorithm that takes plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits. It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.

With DES, two parties share secret keys that are used to protect data and keys that are exchanged on the network. The sharing of secret keys establishes a secure communications channel. The only way to protect the security of the data in a shared secret key cryptographic system is to protect the secrecy of the secret key. ICSF also supports triple DES encryption for data privacy. TDES triple-length keys use three, single-length keys to encipher and decipher the data. This results in a stronger form of cryptography than that available with single DES encipher.

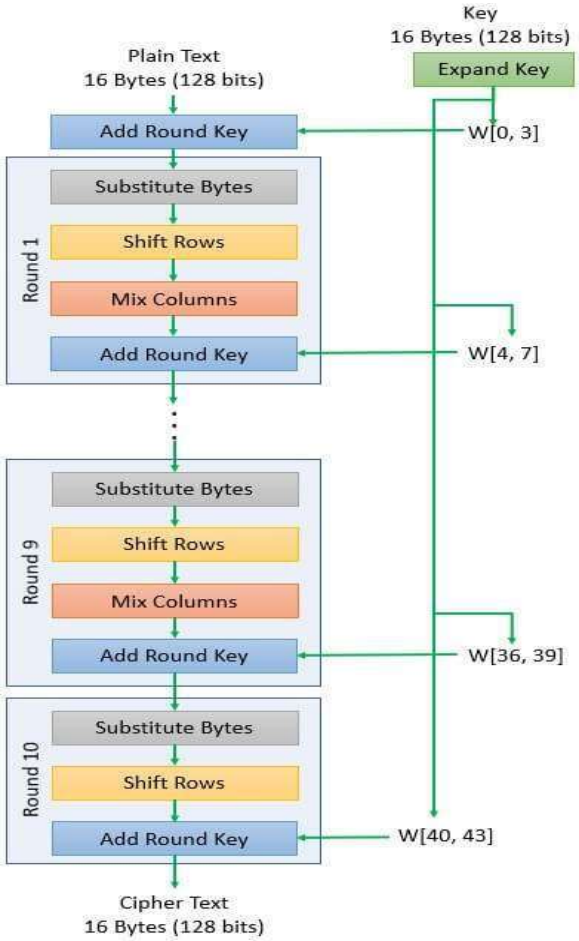


{2nd Way Encryption Method}

Advanced Encryption Standard (AES)

The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard.

The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 258-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.



{3RD Way Encryption Method}

Least Significant Bit [LSB]

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

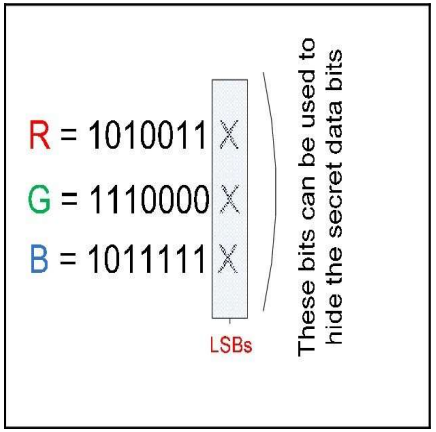


Illustration of Steganography through Block Diagram

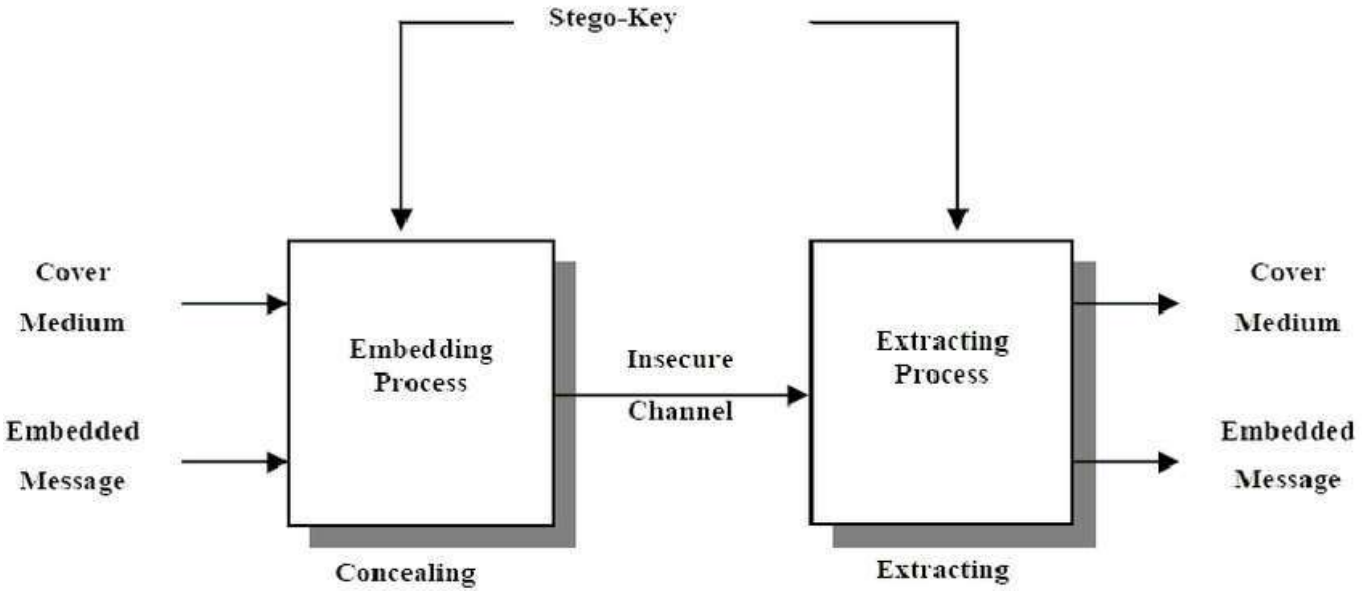
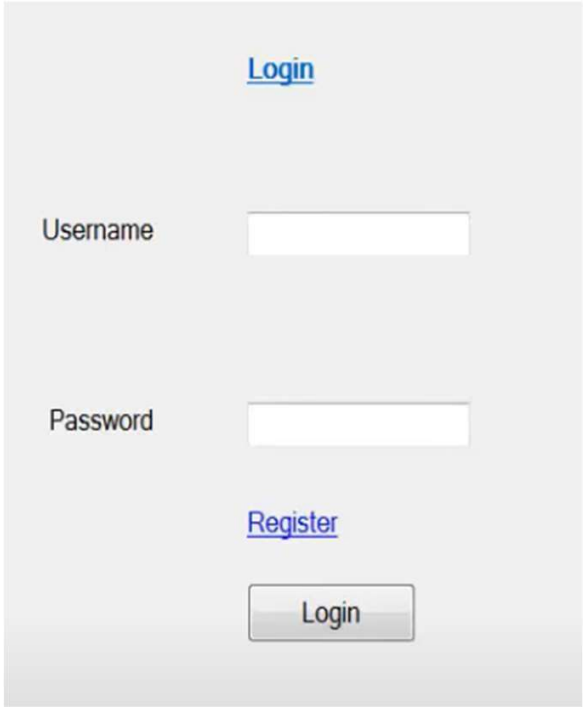
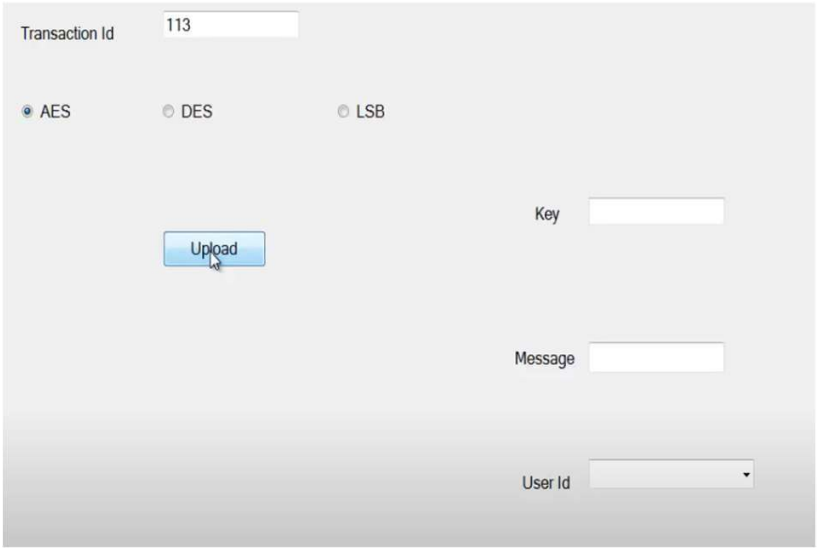


Fig. 1: The General Steganography System

Prototype For Implementation Of Image Steganography





Hardware and Software Requirements For Implementation

- **Hardware Requirement:-**
  - Dual Core Processor Based Computer
  - 1GB RAM
  - 50 GB Hard Disk Space
  - Monitor
- **Software Requirement:**
  - Windows 7 or higher
  - Visual studio 2010
  - SQL Server 2008

Advantages and Disadvantages of Steganography

Advantages:

- Fast and easy way of to send secure stuff.
- Easy process to encrypt text on image.
- Can be added on any image, so that it is like other images only.

Disadvantages:

- Password have to be shared which can be hacked and used.
- Only small length of text can be sent like hardly 2-3 lines.
- Have to manually send the image to receiver.

Applications of Steganography

1) Confidential communication and secret data storing

2) Protection of data alteration

3) Access control system for digital content distribution

4) Media Database systems

5) Digital watermarking

6) E- Commerce

Conclusion

The network security is becoming more & more important as the number of data being exchanged on the Internet increases. Steganography and steganalysis are the important topics in information hiding. Steganography is the ability and discipline of writing hidden messages in such a way that no one, apart from the sender and projected recipient, suspects the existence of the message.

Refrences

- W. Bender, D. Gruhl, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3&4) (1996) 313–336.
- Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. Second edition. Wiley India edition 2007
- C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.
- W. Diffie and M. E. Hellman, ―Exhaustive Cryptanalysis of the NBS Data Encryption Standard,¦ IEEE Computer, Vol. 10, 1977, pp. 74-84.

Thank you