Personal Image Encryption For Confidential Data Transfer

A.Sundarapandian[1], A.Nitheesh kumar[2], A.Seemaan fazil[3], Dr.S.Jeyanthi[4]
[1, 2, 3] Dept of Computer Science and Engineering
[4]Associate Professor, Dept of Computer Science and Engineering
[1, 2, 3, 4] PSNA College of Engineering and Technology, Dindigul.

Abstract- *Visual Cryptography (VC) is used to break an image into two random shares which when separately viewed reveals no information about the secret image. The secret image can be obtained by super imposing the two shares. Conventional visual cryptography scheme is used to encrypt a single image into n shares. The image can be decoded by using only shares. Many visual cryptographic methods use binary images only for this process. This doesn't suit well for many applications. First, the formulation of access structures for a single secret is transformed to that for multiple secrets. A sufficient condition to be satisfied by the encryption of MSS (Multiple Secret Sharing) schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of MSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate MSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation.*

Keywords- Machine Learning, Matlab, Image Encryption, Confidential Data.

I. INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous object (cover text) to produce a stego text. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used. Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text) with bits of different and invisible information. Hidden information can be any other regular computer file or encrypted data. Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message. Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is not seen.

II. EXISTING SYSTEM

RHD-EI allows a server to embed additional message into an encrypted image uploaded by the content owner, and guarantees that the original content can be losslessly recovered after decryption on the recipient side. This method strictly relies on the properties of secret sharing. Summarizing the main techniques, secret sharing serves as the underlying primitive offering security, multiple secret preserves size complexity, and inherently additive homomorphism realizes the data embedding. The scheme overview is described as follows. P will pre-process the cover-image and generate a new cover-image, referred to as the processed image, and then send H the encrypted image by using polynomial interpolation. H will obtain a new polynomial which carries a secret message in the released LSB plane and then use addition homomorphism to generate the encrypted image with embedded message. Finally, by decryption R is able to obtain the stego-image, and then recover the cover-image and secret message.

III. PROPOSED SYSTEM

The main objective of this paper is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. The proposed system architecture for personal image encryption as shown in figure 1. The text is typed and hidden in an image. This is done using Modified LSB method. Then the XOR based VC method is used to encrypt the image and send it to the receiver. The key which is used to encrypt the shares will be mailed to the receiver. The receiver will decrypt the shares using the same key that is used for encryption. The process of personal image encryption as shown in figure 2. After that, the

hidden text will be extracted from the recovered image using the Modified LSB method.

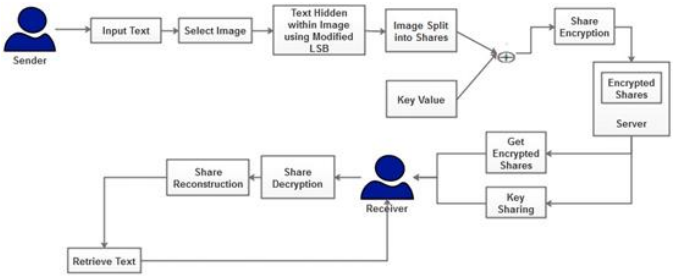

Figure.1 Proposed system architecture for personal image encryption

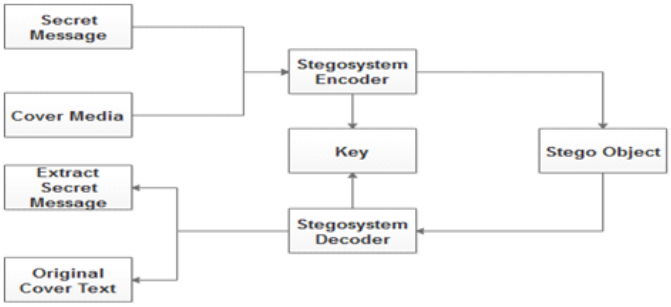

Figure.2 The process of personal image encryption

In proposed technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image as shown in figure 3.

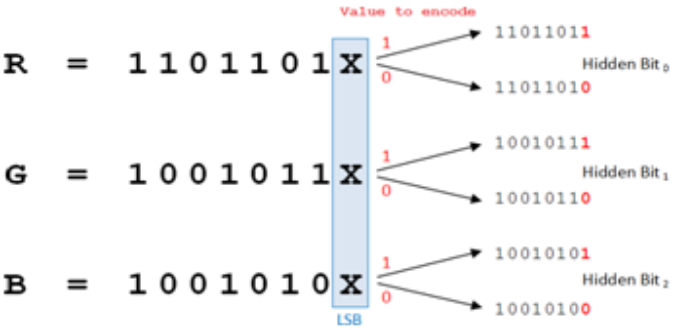

Figure. 3 LSB Steganography

LSB Encoding

First the unique image and the compressed encrypted secret message are taken. Then the encrypted secret facts need to be transformed into binary format. Binary conversion is accomplished via taking the American Standard Code of Information Interchange (ASCII) values of the person and converting them into binary layout and producing move of bits. Similarly, in cover photo, bytes representing the pixels are taken in unmarried array and byte stream is generated. Message bits are taken sequentially after which are positioned in LSB little bit of image byte. Same process is followed till all the message bits are located in photograph bytes. Image generated is called 'Stego-Image'. It is prepared for transmission through the Internet.

Algorithm for hiding mystery facts in Cover image:

Step-1: Read the cover media image and secret information which is to be embedded in to the cover image.
Step-2: Compress the secret facts.
Step-3: Convert the compressed secrets into cipher textual content by means of using secret key shared by receiver and sender.
Step-4: Convert compressed encrypted textual content message into binary shape. Step-5: Find LSBs value of each RGB pixels that present in cover image.
Step-6: Embed the bits of the secret data into bits of LSB of RGB pixels of the cover image.
Step-7: Continue the procedure till the secret information is absolutely hidden into cover document.

LSB Decoding

First, 'Stego-Image' is taken and single array of bytes are generated as it become carried out at the time of encoding. The general number of bits of encrypted secret information and the bytes representing the pixels of stego-image are taken. Counter is to begin with set to 1, which in turn offers the index range of the pixel byte where secret message bit is available in LSB. The procedure is continued till very last secret message bit is reached. After this, the bit circulation of the message shall be generated. Available bits are grouped to shape bytes such that each byte represents single ASCII character. Characters are stored in textual content record which represents the encrypted embedded message. After that the decryption and decompression are to be done.

Algorithm for unhiding secret data from Stego image:

Step-1: Read the stego image.
Step-2: Find LSBs value of each RGB pixel of the stego image.
Step-3: Find and retrieve the LSBs of every RGB pixel of the stego image.
Step-4: Continue the procedure till the message is absolutely extracted from stego image.
Step-5: Decompress the extracted secret facts.
Step-6: Using shared key, decrypt secret records to get original records.
Step-7: Reconstruct the secret statistics.

IV. MODULES

The proposed personal image encryption consists of various stages like obtain various input text, apply text hidden within image using modified LSB, image split into shares & key value done in sender side, share encryption, server (encrypted shares), get encrypted shares, key sharing is done in server side and share decryption, share reconstruction, retrieve text are done in receiver side.

V. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was hidden within QR Code then the QR will be hidden within image. The sender has to create text and generate QR for input text then select the image to hide the QR image using MPVD with LSB approach that should be sent the message secretly to the receiver. Then the secret image is splitted into “n” number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

REFERENCES

[1] Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang. "Secure reversible image data hiding over encrypted domain via key modulation." IEEE transactions on circuits and systems for video technology 26, no. 3 (2015): 441-452.

[2] Zhang, Xinpeng, Jing Long, Zichi Wang, and Hang Cheng. "Lossless and reversible data hiding in encrypted images with public-key cryptography." IEEE Transactions on Circuits and Systems for Video Technology 26, no. 9 (2015): 1622- 1631.

[3] Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc. "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction." In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190, IEEE, 2017.

[4] Yi, Shuang, and Yicong Zhou. "Binary-block embedding for reversible data hiding in encrypted images." Signal Processing 133 (2017): 40-51.

[5] Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." IEEE transactions on cybernetics 46, no. 5 (2015): 1132-1143.

[6] Xu, Shuying & Horng, Jihwei & Chang, Chin-Chen. (2021). Reversible Data Hiding Scheme Based on VQ Prediction and Adaptive Parametric Binary Tree Labeling for Encrypted Images. IEEE Access. PP. 1-1.10.1109/ACCESS.2021.3071819.

[7] Yongjun, Kong & Minqing, Zhang & Zexi, Wang & Yan, Ke & Siyuan, Huang. (2022). Reversible Data Hiding in Encrypted Domain Based on the Error-Correction Redundancy of Encryption Process. Security and Communication Networks. 2022. 10.1155/2022/6299469.

[8] Ke, Yan & Zhang, Minqing & Zhang, Xinpeng & Liu, Jia & Su, Tingting & Yang, Xiaoyuan. (2020). A Reversible Data hiding Scheme in Encrypted Domain for Secret Image Sharing based on Chinese Remainder Theorem.