International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 3 (May-June 2014), PP. 84-86

REAL TIME DATA TRANSFER VIA VIDEO USING REVERSIBLE DATA HIDING TECHNIQUE

Miss Pooja Shinde, Punam Shelke,Preeti Pawar,Kajal Ranade, Prof.J.V.Shinde,
Department of computer Engineering,
Late G.N.Sapkal college of engineering,
University of Pune.

***Abstract*— The protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease transmissions time the data transmission necessary.**

Recently, more and more attention is paid to reversible data hiding (RDH) in encrypted image. It maintains original area could be perfectly restored after extraction of the hidden message. In previous method embed data by reversibly vacating area from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. A novel method by reserving area before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility, that is data extraction and image recovery are free of any error. The hidden data can be retrieved as and when required. The methods that are used in reversible data hiding techniques like Lossless embedding and encryption.

This deals with the image steganography as well as with the different security issues, general overview of cryptography approaches and about the different steganography algorithms like Least Significant Bit (LSB) algorithm , JSteg, F5 algorithms. It also compares those algorithms in means of speed, accuracy and security.

***Key words*— Reversible data hiding, image encryption, privacy protection.**

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via emails, chats, etc. The data transition is made very simple, fast and accurate using the internet.

However, one of the main problems with sending data over the internet is the „security threat‟ it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification.

This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a Method to conceal information by encrypting it to cipher texts "and transmitting it to the the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

In previous method Zhang et al. [2], [3] reserving area are selected after the Image encryption and limited data are transfer to receiver side. In the existing method there is some problem for data extraction and Image restoration [17]. Also hacker easily hack our confidential data by performing different types attacks.

In the most cases of data hiding the selected media become distorted due to data hiding and cannot be inverted back to original media [16].

However, one of the main problems with sending data over the internet is the, security threat‟ it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential Factors that need attention during the process of data transferring.

II. PREVIOUS ART

In the previous method are invented by the X. Zhang, "Reversible data hiding in encrypted images [15], Apr. 2011. in these method new idea is to apply reversible data hiding algorithm on encrypted image by remove the embedded data before the image decryption recent reversible data hiding method have been proposed with high capacity. But these methods are not applicable on encrypted images. W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match [16],"Apr.2012. Traditionally data hiding is used for secrete communication in some application. The embedded data are further encrypted to prevent the data from being analyzed other application could be for when the owner of the receiver might not wont the other person including data hider to know the content of the data before data hiding is actually perform such as military images or confidential medical image. In these method estimate

smoothness of image blocks.side match technique is employed to further reduce the error rate.

X. Zhang, "Separable reversible data hiding in encrypted image [17]," Apr 2012.

This work proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not toolarge.

III. PROPOSED METHOD

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)"

In our system first we take live video through webcam .That video contain number of frames. System reserve the area logically then we encrypt image by using AES Algorithm. After encryption we embed the data in reserve area using LSB technique. At the receiver side we decrypt the image using AES Algorithm. Receiver Extract the data and recover the original image.

A. Encrypted Image Generation
   1) IMAGE PARTITION
B. Data Hiding In Encrypted Image
C. Data Extraction and Image Recovery
D. Data Extraction and Image Restoration

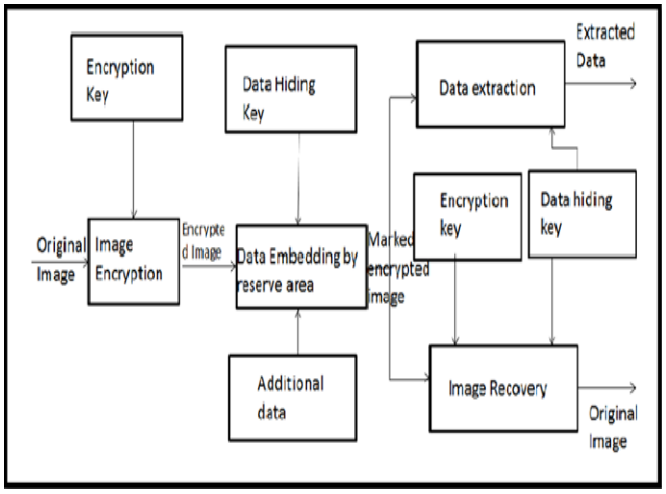

Fig:1 Framework "vacating room after encryption"

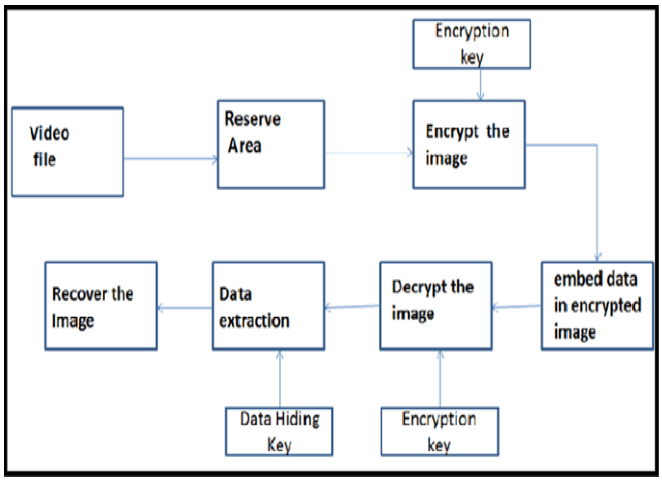

Fig 2: Block diagram for system architecture

A. Encrypted Image Generation

At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

1) IMAGE PARTITION

The operator here for reserving room before encryption is a standard RDH technique, so the goal of image partition. Assume the original image c is an 8 bit gray-scale image with its size M x N and pixels first the sender extract from the original image, along the row, several overlapping lock whose number is determine by the size of to be embedded massage, denoted by l.In detail every block consist of m rows, where m=[ ] , and the number of blocks can be computed through n=M-m+1.

B. Data Hiding In Encrypted Image

In this module, a sender encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the sender hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the sender himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

C. Data Extraction and Image Recovery

In this module, Extracting Data from Encrypted Imagestomanage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As

the whole process is entirely operated on encrypted domain, it avoids the leakage of original content

D. Data Extraction and Image Restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image.

Fig 3.(a)Original image

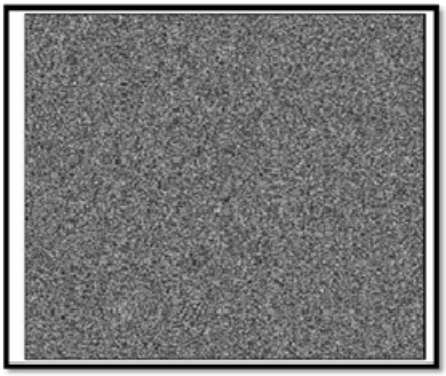

Fig :(b)encrypted image

Fig:(c) decrypted image containing message

Fig:(d) recovery image

IV. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless.

REFERENCES

[1] IEEE transactions on information forensics and security, vol. 8, no. 3, march 2013 553" Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li

[2] W. Hong, T. Chen, and H.Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[3] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[4] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process.Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4,pp. 1097–1102, Apr. 2010.