International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 4 July-August 2017 p-ISSN: 2394-8280

A HIGHLY SECURED DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGNOGRAPHY

Megha S. Kurhe , Dr.Prof.Gunjal B.L
Department of Computer Engineering AVCOE, Sangmner,India
kurheegha92@gmail.com,hellobaisa@gmail.com

ABSTRACT—
With the recent surge and rapid growth in digital data usage and transfer in many real life applications, there is a question of new and effective ways to check their security. More secrecy can be achieved by using the steganography mechanism. In this proposed system, steganographic techniques for embedding text data in image, image data in image , text data in video , image data in video , video data in video is developed. The basic approach behind this system is to provide a good, well-organized method for hiding the data and pass to the target system using secured media in safer manner. Our method is secure in the way that even if the thief finds details and decode the embedded message from the stego medium (image/audio/video), one would not be able to recover the hidden message without the encoded key. Proposed system used efficient techniques such as LSB (Least Significant Bit) , RDH (Reversible Data Hiding) when image , text and video data are hided in selected cover media. Techniques used for such variety range of data hiding are all efficient and secured one. Proposed system analyzed and applies these techniques in such a way so that final stego image or stego video should not degrade in quality which is the main concern. Hence DCT (Discrete Cosine Transform) technique is used for image compression and also helps to retain the image quality. In this way proposed system triggers the steganography process by assuring the security and final image and video quality. Also proposed system uses cloud to share secured data which is one step ahead idea and contribution as far as secret data sharing is concern.

INDEX TERMS—Steganography , Secret Sharing , LSB , RDH , DCT , cloud

I. INTRODUCTION

Steganography [1] , [2] , [3] is the technique and science of writing secret messages in such a way that no one apart from the intended recipient knows of the presences of the details message; this is in contrast to cryptography, where the existence of the message file is clear, but the term is obscured. Steganography means ”covered writing” and is the art of hiding the very existence of a message. In today’s digital media world, invisible ink and paper have been replaced by much more versatile and practical covers file for hiding messages digital documents, images, video, and audio files. As long as an digital electronic document contains perceptually irrelevant, it can be used as a ”cover” for hiding secret messages. The pos- sible cover carriers are good looking carriers (images, audio, video, text) which will hold the secret information. A message is the information to be hidden and it may be plaintext, cipher text, images, or anything that can be embedded into a bit stream data. Together the cover carrier and the embedded message file create a stego-carrier. Hiding information may require a key which is additional hidden information, such as a key or password, required for embedding the information. For example, when secret information is hidden within a cover image file, the resulting product is a stego-image file. Recently this sharing process is enhanced and various platforms such as server, clouds are used. Cloud is smart, efficient and secured platform to share data. Though it is secured and good for communication it is curious too. Hence data present on the cloud may be touched by the cloud providers. Hence there must be provision for secured sharing on cloud also [4] which is contribution for proposed system. Proposed system work for text data hiding, image data hiding and video data hiding. Various techniques and algorithms are studied and used for secure sharing factor of proposed system. LSB (Least Significant Bits) [5] technique is studied and used on image to enhance the security of the communication. In the LSB approach the basic idea is to replace Least Significant Bits of the cover image with the bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one, as it is difficult to differentiate between the cover object and stego object if few LSB bits of the cover object are replaced. LSB majorly used for text data hiding, in image and video. LSB technique keeps the stego-image and stego- video quality. Though this technique is efficient some pixels

are modified. This modification is not allowed while data is outsourced to cloud to preserve but sometimes which not be the case. Sometimes cloud may add some information as data management part which helps them to identify the owners of the data. Since data is modified it may compromise with quality which is not expected. Hence there must be technique that helps to get original media file after extracting clubbed data. In RDH (Reversible Data Hiding) [6] technique, original media file can be maintained after extraction of embed data. Hence proposed system approach is helpful as far as secure data sharing is concern. In the business world, audio data hiding, video data hiding and text data hiding can be used as a secret chemical formula or plans for a new invention. Audio data hiding can also be used in Corporate world. Terrorists can also use audio data hiding to keep their communications secreand to co-ordinate attacks. Data hiding in video and audio is of interest for the protection of copyrighted digital media and to the government for information system security and for covert communication. It can also be used in forensic application for inserting hidden data in to audio files for the authentication of spoken words and other sounds and in the music business for the monitoring of the songs over broadcast radio. Image hiding is to secure in the way that even if the attacker detects (i.e., statistical attacks) and extracts the embedded message from the stego-image, he/she would not be able to recover the secret message without the encoded key. So, the key areas for the use of steganography are Confidential Communication and Secret Data Storing, Protection of Data Alteration, Access Control System for Digital Content Distribution, E-Commerce, Media, Database Systems, Digital watermarking etc.

II. REVIEW OF LITERATURE

Literature survey is carried out for sections such as image steganography and video steganography. In image steganogra- phy text data is hide in image also image data is hide in another image. Various techniques are there that performs this secret sharing. Hence in this case image is the cover object and used to hide data like text and image. In the image Steganography, data hiding method can be classified into different categories. These are spatial domain, frequency domain, and adaptive domain. LSB (Least Significant Bit) [1] [2] [3] [5] method is one of the important method amongst them. It is one of the most common and easiest methods for message hiding. In this method, message is hidden in the least significant bits of image pixels .Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image. In case of 24-bit images three bits of pixel can be used for LSB substitution as each pixel has separate components for red, green and blue. Masking and filtering [1] [2] [3] method is also important method. Basically, this method is used for 24-bit and grey scale images. It is similar to placing watermarks on the image. Steganography only hides the information where as watermarks becomes part or attribute of the image. This method is more robust than LSB in terms of some image processing like - compression, crop- ping which makes it suitable in lossy JPEG images. Masking images involves changing the luminance of the masked area. It is more robust than LSB but original image changes in it. Parity checker method [7] is also important method. In this method, concept of even and odd parity is used. 0' is inserted at pixel value when it contains odd parity i.e. no. of 1's in the binary value of pixel must be odd similarly, 1' is inserted at pixel value if it contains even parity i.e. no. of 1's in the binary value of the pixel must be even. If the corresponding parity does not exist at pixel location for 0 or 1 then it is made by adding or subtracting 1from the pixel value. For retrieval of message, if odd parity is present, then 0' is the message bit and if even parity is present, then 1' is the message bit. For retrieval of message parity checker is used. With parity checker 0' is return if there exist an odd parity otherwise it returns 1'. This strategy is used every time when message isinserted. In Gray Level Modification (GLM) [8] technique, gray level values of the image pixels are modified. In Pixel value Differencing (PVD) technique [9] method, Wu Tsai selected two consecutive pixels for embedding the message. By checking the difference between two consecutive pixels,payload of Wu and Tsai method is determined and it serves as basis to find out whether the two pixels belongs to an edge area or smooth area. If the difference is large, it means pixels belong to an edge area and more secret data can be embedded at this location. On the other hand, if difference is small, it means pixels belong to smooth area and less secret data can be embedded at this place. If the original difference value is unequal to the secret message, then the two consecutive pixels are directly adjusted so that the difference value can stand for the secret data. The hiding effect that appears in the stego-image when Wu and Tsai's scheme is used to hide the secret data can be significantly decreased by the proposed optimal embedding algorithm. Amongst these techniques LSB is most powerful technique but it is not so robust and hided data can be cracked with few attacks and with minimum efforts. Hence Reversible Data Hiding (RDH) [6] [10] technique is explored and analyzed to hide imaged data in image and video data in video. This technique is found

to be robust as far as data outsourcing to cloud is concern. It is interesting to implement RDH in encrypted image by which cloud server by which the cloud server can reversibly embed data into the image but cannot get any knowledge about the image contents. Same technique is found useful for video hiding. In that technique video is divided into frames and cover video is also divided into frames. These frames are nothing but images and used to hide behind cover video frames.

III. PROBLEM DEFINITION

Major concern of the end user while sharing or outsourcing data like text message, image or video to cloud the data is security. Cloud is secure but curious and hence data can be in trouble. Hence there must be techniques involved in steganography that helps to hide data behind another data format.
Proposed system should work for text message hiding, image hiding and video hiding. Basic technique involves following modules
A] Data Embedding
In data embedding technique data , stego-key (using which data is hide and unhide) and cover image or video (behind which data is hidden) is required. Using algorithms this data embedding is carried out. After embedding process stego- image or stego-video is generated. Stego-key is shared with another user to unhide the data which is hidden in stego files. B] Data Extraction
In this data extraction process shared stego-key is necessary to extract hidden data from stego files. While applying these steganographic algorithms there are chances where image quality or video quality of original data can be hampered.Which is the main concern of the system. Hence to avoid that efficient algorithms like LSB , RDH are used. Following is the system architecture diagram.

IV. SYSTEM ARCHITECTURE

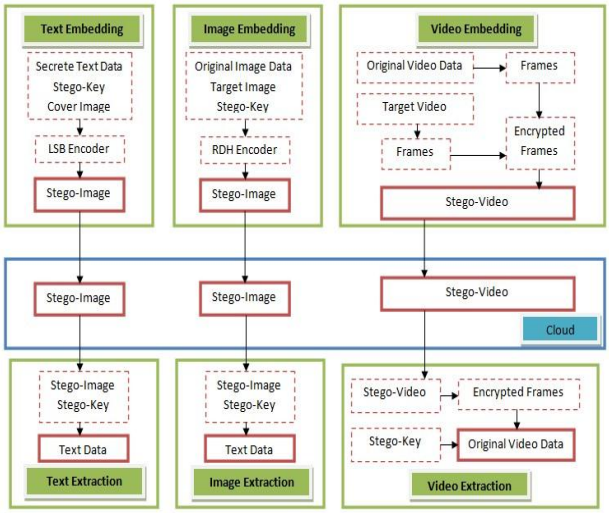

Fig. 1. System Architecture

As per the system architecture diagram, proposed system will help the user when they share text , images or videos with the cloud. Following are details of the embedding and extraction sections
A] Text Embedding:
This section comes in focus when user wants to share text data other user via cloud. Secret text data is selected. Also cover image is selected to hide text. LSB algorithm is used to hide text with help of Stego-key.
B] Image Embedding:
This section comes in focus when user wants to share image data other user via cloud. Secret image data is selected. Also cover image is selected to hide image. RDH algorithm is used to hide text with help of Stego-key. Before applying this algorithm secret image size and cover image size is checked whether equal or not.

C] Video Embedding :

This section comes in focus when user wants to share video data other user via cloud. Secret video data is selected. Also cover video is selected to hide video. In this both secret video and cover video should be of equal size. Initially secret video in converted into frames. These frames are noting but sequence of images. Also cover video is converted into frames. Using RDH algorithm secret video frames are hided in cover video frames and from this encrypted video frames stego-video is generated and shared on cloud.

D] Text Extraction:

In this , end user is having stego-key. He downloads the stego- image and by applying stego-key and reverse process, secret text data is extracted.

E] Image Extraction :

In this , end user is having stego-key. He downloads the stego- image and by applying stego-key and reverse process, secret image data is extracted.

F] Video Extraction :

In this , end user is having stego-key. He downloads the stego- video. Frames are generated from stego-video. These frames are encrypted. Using stego-key these frames are decrypted and original video frames are generated. By using these frames video is constructed and secret video is extracted.

A] LSB Algorithm

1. Algorithm to embed text message: Input: Cover image and text message Procedure:
Start
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
End
Output: Stego Image
2. Algorithm to retrieve text message: Input: Stego image
Procedure:
Start
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character
End
Output: Text Message

B] RDH Algorithm : For Image

Following are the algorithmic steps for Transformation process i.e. embedding images and videos
Input : Secret image data Im, Private Key K
Output: The Stego image S(I).
Steps :
Step 1 : Get a cover image T_i having the same size as secret image Im
Step 2 : Divide both Ti and Im into several distinct 4 *4 blocks. Where it is Assumed that Ti and Im consists of N blocks. Calculate the mean and Standard Deviation for each block.
Step 3 : Block classification with %η quantile of Standard Deviation's and generate Class Index Table (CIT) for Ti and Im respectively. Pair up blocks of Im with blocks of Ti according the Class Index Tables (CIT)
Step 4 : For each block pair (Bi , Ti) ($1 < i < N$), compute the mean difference λui . Add λui to each pixel of Bi and then block rotation is done into the optimal direction θi (θi
{0 , 90,180,270}), which yields a transformed block Ti . Step 5 : In the target image Ti, replace each block Ti with the corresponding transformed block T' i for $1 < i < N$ and generate the transformed image Im'i.
Step 6 : Collect λuis and θis for all block pairs, and compress them together with the CIT of I. Encrypt the compressed sequence andthe parameter by a standard encryption scheme such as AES with the key K.

Step 7 : Take the encrypted sequence as accessorial informa- tion (AI), and embed AI into the transformed image Im' with an RDH method and output the encrypted image S(I).

Same process is carried out for video embedding. In video em- bedding equi-sized secret video and cover video are selected and they are converted into frames i.e. sequence of images. Same transformation is applied to them recursively and secret video frames are hided in cover video frames and encrypted frames are generated. From these generated frames encrypted video is formed.

Following are the algorithmic steps for Anti-Transformation process i.e. extraction of images and videos

Input : The encrypted image S(I) and the key K.

Output: The secret image Im.

Steps :

Step 1 : Extract AI and restore the transformed image Im'
from S(I) with the RDH scheme .

Step 2 : Decrypt AI by AES scheme with the key K, and then decompress the sequence to obtain CIT of I, λui , θi ($1 < i < N$) and η.

Step 3 : Divide Im' into non-overlapping N blocks with size of
4 * 4. Calculate the SDs of blocks, and then form the Class Index Table (CIT) of Im' according to the % η quantile of SD's.

Step 4 : As per Class Index Table (CIT) of Im' and Im, rearrange the blocks of Im'

Step 5 : For each block T' i of Im' for $1 < i < N$, rotate T' i in the anti-direction of θi , and then subtract λui from each pixel of T'i , and finally output the original image Im.

Same process is carried out for video extraction. In video extraction stego-video is downloaded converted into frames i.e. encrypted sequence of images. Anti-transformation is applied to them recursively and secret video frames are extracted. From these generated frames secret video is formed.

VI. EXPERIMENTAL SETUP

As this is client server application setup needs Apache Tomcat on cloud. Also image dataset and video dataset is require. Using these datasets equal sized secret images and cover images are decided. Also equal length secret videos and cover videos are decided. This sharing experiment is carried out for such number of images and videos.

VII. CONCLUSION

Proposed a system supports the image, text and video (as a carrier file) to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. Based on literature survey it is found that LSB technique is efficient for text hiding. For image and video hiding RDH technique is efficient. These methods are secure in the way that even if the attacker detects and extracts the embedded message from the stego-image, one would not be able to recover the secret message without the encoded key. Steganography can be used for hidden communication. Finally, it is shown that steganography that uses a key has a better security than non- key steganography. This is so because without the knowledge of the valid key, it is difficult for a third party or malicious people to recover the embedded message.

ACKNOWLEDGMENT

A very firstly I gladly thanks to my project guide Dr.Prof. B.L.Gunjal, for her valuable guidance for implementation of proposed system. I will forever remain a thankful for their excellent as well as polite guidance for preparation of this report. Also I would sincerely like to thank to HOD of computer department Mrs.R.L.Paikrao and other staff for their helpful coordination and support in project work.

REFERENCES

[1] Adel Almohammad "Steganography-Based Secret and Reliable Commu- nications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August, 2010.

[2] Neil F Johnson, Sushil Jajodia, "Exploring Stenography: Seeing the Unseen", IEEE Computer, Feb 1998, pp 26-34.

[3] Rajkumar Yadav ”Analysis of Incremental Growth in Image Steganogra- phy Techniques for Various Parameters” Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870, NOV-DEC 2011.

[4] K. Hwang, D. Li, ”Trusted cloud computing with secure resources and data coloring,” IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept.- Oct. 2010.

[5] Saleh Saraireh , ”A Secure Data Communication System Using Cryptography and Steganography” , International Journal of Computer Networks Communications (IJCNC) Vol.5, No.3, May 2013

[6] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, ”Reversible watermarking algorithm using sorting and prediction,” IEEE Trans. On Circuits and Systems for Video Technology, vol.19, no.7, pp. 989-999,Jul. 2009

[7] Rajkumar , Rahul Rishi , Sudhir Batra ” A New Steganography Method for Gray Level Images using Parity Checker” International Journal of Computer Applications (0975 8887) Volume 11 No.11, December 2010.

[8] Ahmad T. Al-Taani and Abdullah M. AL-Issa ”A Novel Steganographic Method for Gray- Level Images” International Journal of Computer and Information Engineering 3:1 2009.

[9] Chung-Ming Wang , Nan-I Wu , Chwei-Shyong Tsai , Min- Shiang Hwang, ”A high quality steganographic method with pixel- value differencing and modulus function” J. Syst. Software (2007), doi:10.1016/j.jss.2007.01.049.

[10] Weiming Zhang, Hui Wang, Dongdong Hou, Nenghai Yu , ”Reversible Data Hiding in Encrypted Images by Reversible Image Transformation” , IEEE