Secure Reversible Data Hiding video Transformation using cloud storage

Amrutha OC
Department of Computer Science And Engineering Malabar Institute of Technology , Anjarakandy Kannur , Kerala – India

Rabina P
Department of Computer Science And Engineering Malabar Institute of Technology , Anjarakandy Kannur , Kerala – India

Abstract

Cloud is one of the most promising technology nowadays. The data's which are stored in the cloud are need to be protected .The of management of data and privacy of the data must be protected at the same time. By considering these demands reversible data hiding in encrypted images attracts more and more researcher's attention. Here proposes a work for data hiding based on the reversible data hiding. In reversible data hiding the input image is transformed in to the target image and the input image will look like the target image. After the encryption hiding is performed. Here proposes a scheme for video hiding in a target image. For hiding process the video frames are generated. These frames are hided to the target image, then the video will contain the target image. A mutual authentication is performed for authenticating the user and cloud. The target image which is chosen is greater than the frame size. The target image is send along with the video to the CSP. A user can receive the video from CSP. This work improves the security.

Index Terms- *Cloud computing, Reversible image transformation, LSB Data hiding*

1. Introduction

Cloud is one of the most emerging and widely used technology nowadays. The cloud offers some services, they are software as a service (Saas), Platform as a service (PaaS), Infrastructure as a service (IaaS) . A cloud user can send their data to the cloud in-order to store their data and save the storage space. The cloud offers reduced cost, flexibility, manageability, reliability. The privacy of the data must be protected and the data's must be managed. Nowadays cloud becomes more popular services for storage for multimedia files which need large storage space [1]. To protect the outsourced images some data are embedded to the images in order to verity the ownership. The reversible data hiding method is used to extract the original image by removing

the embedded message. The RDH method is used because the cloud has no permission to make any changes in the data privacy. RDH-EI by using reversible image transformation (RIT). RIT transfers the content of the original image I into the semantic of another image J of the same size. Here proposes a reverse image transformation in videos in which a video can be embedded in to a target image. In this system video frames are generated using video framing technique and each frame is encrypted and performs hiding operation using a target image. Here the target image chosen is greater than the frame in size. After the hiding it is joined and sends to the cloud along with target image. After the data embedding watermarking of the target image is performed. At the receiver side the receiver receives the video from the CSP. A mutual authentication mechanism is used for authentication purpose. Data hiding algorithm and encryption algorithms are used.

.

2. Related work

The reversible data hiding using RIT [1] deals data hiding method in images. Here the original image is converted to another target image of same size by performing encryption and hiding process. The CSP embed some data in to the converted images and store it as a watermarked image. When a receiver downloads the image the receiver get the target image. By using decryption the receiver can get the original image.
An id based user authentication [2] scheme provides authentication, authorization of cloud users. The ID-based user authentication scheme is designed by one-way hash functions and exclusive-or (XOR) operations so it has low computation costs. And it can be easily applied to the multi-server environments in cloud computing. It does not need the verification table on the server side, and the verification time and the storage space can be greatly reduced. It is very suitable for the user authentication in cloud computing environments**.** This scheme is divided into two phases registration phase and mutual authentication phases. In the registration phase, the user register to the CSP.
Digital image watermarking technique [3] deals with copyright protection and authentication of multimedia data and it makes possible to identify the author, owner, distributor or authorized recipient of a document.
In Anonymous user authentication [4] data preservation on cloud has several issues in terms of security. When a user transact with the sensitive cloud data, user privacy is also important.
Digital Image Encryption [5] deals with the AES algorithm for digital image encryption. AES encryption system is symmetric in group, and there are three types of key length 128 bits, 196 bits and 256 bits and block size 128 bits. AES can resist all known attacks and it is fast and simple in design.
RGB Image steganography on multiple video frame using LSB technique [6] proposed a steganography of an Image on a multiple frame video using Frame Decomposition Technique. LSB Algorithm is used on multiple frame video for Steganography. The same image can be extracted in the output phase. There will be only a small difference between the input and output image.
Separable reversible data hiding in encrypted image [7] proposed a novel scheme for separable reversible data hiding in encrypted images. a content owner encrypts the original image using an encryption key. To add additional data the data hider need to create sparse space by compressing the least significant bits of the encrypted image using hiding key. Using encryption key can decrypt the received data to get an image similar to the original one. By using the hiding key receiver can extract the additional data**.**
Data hiding in video using adaptive lsb[8] states a novel video hiding scheme based on LSB,. Here use Three-Dimensional Array and LSB technique for data hiding. The Three-Dimensional Array used to storage pixels' information of the cover image and the secret image.

3. Proposed work

Here proposes a method for video hiding in another image. The target image chosen is larger than the frames of the input video. The user can outsource his/her video to the cloud. For providing security to the video the frames for the video is generated and each frame is encrypted and performs hiding to another image. After the hiding process a new video is generated which contains only the target image i.e. the video contain a stream of target image. Here a single target image is chosen . For every frame in the video the target image is repeatedly chosen. An ID-based authentication mechanism is used here for authenticating the user. The newly generated video is send to the cloud. The target image is send along with the video to the cloud. The image contains the ownership details and watermarking process will be performed on the image.

3.1 System Architecture

In the proposed system secure reversible data hiding video transformation, first a user chooses a video which he/she wants to outsource to the cloud. The frames for the video are generated and each frame is encrypted and hiding process is done. LSB hiding technique is used here. A target image is chosen by the sender for hiding purpose. The target image is chosen repeatedly. After hiding a new video is generated, which contain only the target image as frames. And this video is outsourced to the cloud. A key is generated for the video encryption and the same key is used for the decryption in the receiver side. This key is send to the receiver by the sender then only the receiver can decrypt the frames and get the original video. The video contains audio and the audio also need to be encrypted. The target image is send along with the video to the cloud. The additional data are embedded to the target image like ownership details and watermarking is performed. When a user requested for the video the target image the CSP removes the watermarked target image and

provide the video stored in the cloud. Using the key shared by the sender the receiver can receive the video. And the user can decrypt the video and get the original uploaded video. The figure shows the system architecture

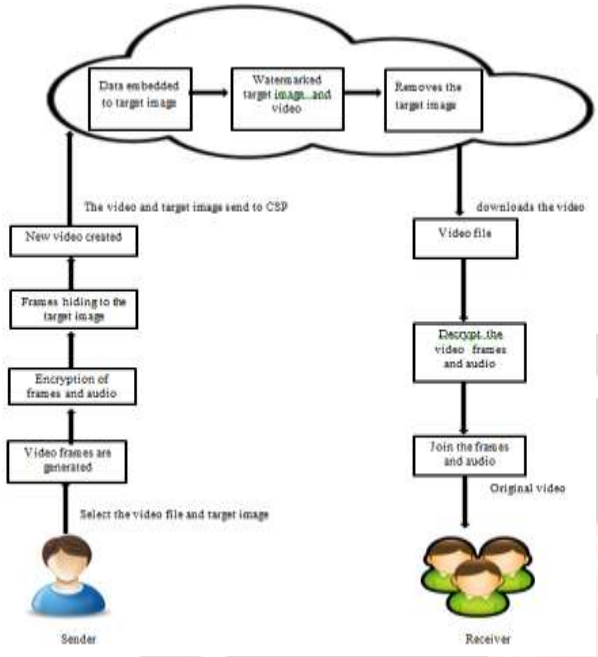

Fig1: System architecture

The framing algorithm is used for video framing. The figure 2 shows the frames of a video using framing technique.

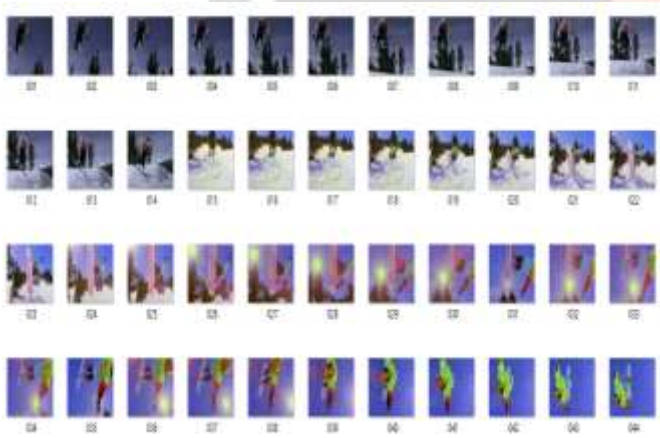

Fig 2: Video frames

3.2 METHODS USED

(1) **Video framing:** The video framing technique is used to generate video frames

1: Start.
2: Read the video file.
3: initialize i=0.
4: do until i less than total frames of video file.
5: Read the i^{th} fame from image.

6: End.

(2) **Data hiding :** The content of the data's are hided to anther image. Here LSB substitution method is used. The encrypted data's are place into the lsb of target image. It first reads the frames and the target image. Then it extracts the RGB components. Then it place into the target image LSB. The number of times the target image chosen is equal to the number of frames generated. After the lsb substitution the images are joined and forms a new video which can be viewed as a sequence of target image. This video is outsourced to the cloud.

(3) **AES algorithm:** The frames are generated by the video framing technique, and the generated frames are encrypted. The encryption is used for security purpose. A key is generated and this key is used for decrypting the frames. This key is shared to other users. Audio is also encrypted here for security. The newly created video and encrypted audio send to the cloud where the users who have the privilege to access the video can download the video.

(4) **ID Based authentication:** ID-based user authentication scheme. Scheme is designed by one-way ha functions and exclusive-or(XOR) operations. There are two phases mutual authentication and registration phase. In the mutual authentication phase the user and server checks time stamps if the time stamp is valid then it allows user to login

(A) The Registration Phase

Step1: The user sends ID_u and ID_s to the ID provider (IDP).

Step2: IDP computes $P_i=h(ID_u \oplus X)$ and $S_i=h(P_i)$. Then, ID_P sends P_i and S_i to the user and the server respectively

(B) The Mutual Authentication Phase

Step1: The user chooses a random number Ni to compute $C_i=h(h(ID_u \oplus X)||IDs||TS) \oplus Ni$ and $A=h(Ni)$. Then, the user sends {Ci, A, IDu, TS} to the server. Server computes $Ni'=Ci \oplus h(h(IDu \oplus X)||IDs||TS)$ and $A'=h(N_i')$. If $A'=A$, then the server allows the users login. Otherwise, the server denies the user.

Step2: The server checks the timestamp TS. If TS is not valid, then the server denies the user

Step3: If TS is valid, then server computes $N_i'=C_i \oplus h(h(IDu \oplus X)||ID_s||TS)$ and $A'=h(N_i')$. If A'=A, then the server allows the user's login. Otherwise, the server denies the user

Step4: The server chooses a random number Ns to computes $Bi=h(h(IDu \oplus X)||IDs||TS) \oplus Ns$ and $B=h(Ns)$. Then, the server sends $\{B_i, B, TS''\}$ to the user.

Step5: The user checks if the timestamp TS is valid or not. If TS is valid, then the user computes $N_s'=B_i \oplus h(h(ID_u \oplus X)||ID_s||TS'')$ and $B'=h(N_s')$. Finally, the user checks if B=B'. If they are equal, then the user ensures that the server is legal.

ID_u	The identity of the user
ID_s	The identity of the server
$\|$	The string concatenation
$h(\cdot)$	A secure one-way hash function
$\oplus$	XOR operation
N_i	A random number chosen by the user i
N_s	A random number chosen by the server
X	The secret key of the ID provider
TS	The timestamp

Fig 3: notations used in ID based authentication

4. Conclusion

The video transformation using reversible data hiding provides a secure method for outsourcing the videos to the cloud. The frames of the videos are transformed into the target image and generate a new video. The target image is send with the video to the cloud and this target image is watermarked by the CSP. A mutual authentication is performed for authentication purpose. A receiver can receive the video from the CSP. This proposed scheme uses an ID based authentication scheme, LSB embedding and AES encryption. The user can outsource the data to the cloud in a secured manner. This work improves the security of the data and provide authentication.

References

[1] Weiming Zhang, Hui Wang, Dongdong Hou and Neng-Hai Yu. Reversible data hiding in encrypted images by reversible image transformation. 2016.

[2] Jen Ho Yang and Pei Yu Lin. An id-based user authentication scheme for cloud computing. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on, pages 98–101. IEEE, 2014.

[3] Bhupendra Ram. Digital image watermarking technique using discrete wavelet transform and discrete cosine transform. International journal of Advancements in Research & technology, 2(4):19–27, 2013.

[4] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak. Decentralized access control with anonymous authentication of data stored in clouds. IEEE transactions on parallel and distributed systems, 25(2):384–394, 2014.

[5] Zhang, Qi, and Qun Ding. "Digital Image Encryption Based on Advanced Encryption Standard (AES).Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015 Fifth International Conference on. IEEE, 2015.

[6] Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta, and Pradeep Kumar. Rgb image steganography on multiple frame video using lsb technique. In Computer and Computational Sciences (ICCCS), 2015 International Conference on, pages 226–231. IEEE, 2015.

[7] Xinpeng Zhang. Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security, 7(2):826–832,2012.

[8] Yi-Chun Liao, Chung-Han Chen, Timothy K Shih, and Nick C Tang. Data hiding in video using adaptive lsb. In Pervasive Computing (JCPC),2009 Joint Conferences on, pages 185–190. IEEE, 2009..