International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 12, Number 2 (2016), pp. 193-196

http://www.ripublication.com

Secure Reversible Data Hiding Image Transformation Using Cloud Storage

Ms. Amrutha O.C and Ms. Rabina P

Department of Computer Science and Engineering,
Malabar institute of technology, Anjarakkandy, India.
E-mail: amrutha.oc@gmail.com, rebinap@gmail.com

Abstract

With the development of information technology the datas are stored in the cloud and it need to be protect the privacy of data and management of the data at the same time. By these demands the reversible data hiding in encrypted images (RDH-EI) attracts more and more researchers attention. Here propose a novel framework for RDH-EI based on RIT (Reverse image Transformation). Herethe content of the original image can be tansform to the content of another image. Then the transformed image, that looks like the target image, is used as the encrypted image, and send to the cloud. Therefore, the cloud server can embed data into the encrypted image by using any RDH methods for plaintext images. RDH-EI is a client free scheme and the data embedding scheme is irrelevent with both process encryption and decryption. In the proposed method video framing technique is used to make video frames and this frames are embedded with a target image and store into the cloud and also improve the quality of encrypted image. This works improve the storage capacity cloud as well as the security of data.

Keywords: Reversible Data Hiding, Reversible Image transformation, Cloud computing

INTRODUCTION

Cloud computing is a emerging technology. In cloud computing a large pool of systems are connected in private or public networks. It is used to provide dynamically scalable infrastructure for application and storage of data and files. Cloud Providers off er services are classified into three categories they are Software as a Service(SaaS), Platform as a Service(Paas), Infrastructure as a Service(Iaas). Cloud Computing provides some benefits such as Reduced Cost, Increased Storage and Flexibility.

Nowadays outsourced storage by cloud becomes a more and more popular service, especially for multimedia files, such as images or videos, which need large storage space [1]. To manage the outsourced images, the cloud server may embed some additional data into the images, such as image category and notation information, and use such data to identify the ownership or verify the integrity of images. The CSP has no right to make permanent changes during data embedding into the outsourced images. Therefore, reversible data hiding (RDH) technology is needed, by which the original image can be losslessly recovered after the embedded message is extracted. The RDH is helpful for managing the outsourced images, it cannot protect the image content. Encryption is the most popular technique for protecting privacy. RDH-EI by using reversible image transformation (RIT). RIT transfers the content of the original image I into the semantic of another image.

Existing System Reverse image Transformation is used to hide an image to another image. In this system both are of same size, the input image and the target image. Here the input image which is to be hidden in a target image an LSB based technique is used. And it is encrypted with the target image. In this RDH-EI techniques the encrypted image is send to the cloud and it embed the data and remove the data whenever the user want to download. At the user side it get the encrypted image, after decrypting the image the user can get the original image.

In the proposed system Secure Reversible Data Hiding Image Transformation using cloud storage where we can store videos in the cloud in a secured manner. The video frames are generated for the video which are uploaded by a user then a target image is choosen and each frames are encrypted and is transformed into the target image. These are all done in the user side. And this transformed frames are send to the cloud. In the cloud side each frames are embedded with some data to make the images as watermarked images. The embedded additional data are removed on the download request by a user and the user get the encrypted images, by decrypting the images we get the original frames and by joining these frames the user get the original video. An authentication mechanism also used here for authenticating the user.

SYSTEM MODEL

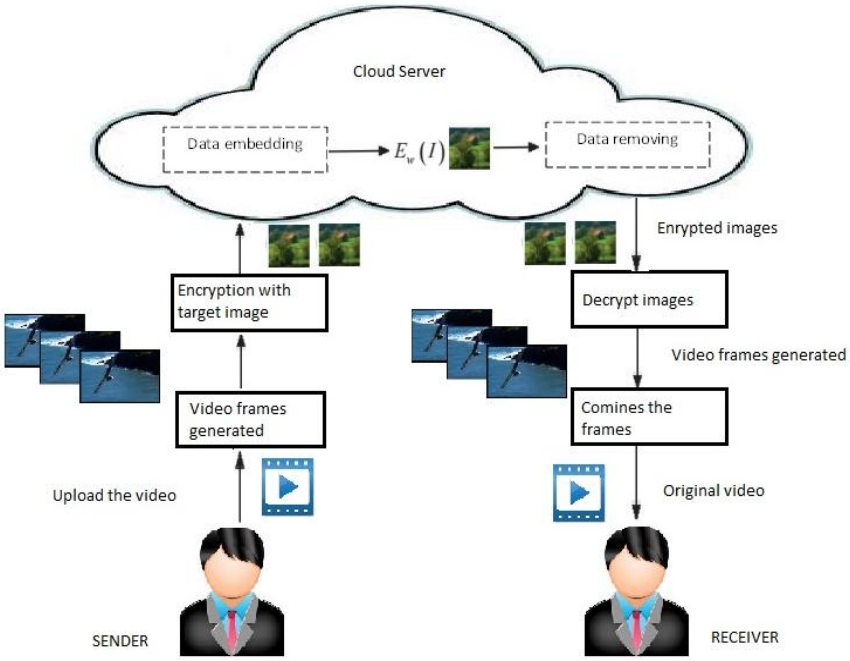
Secure Reversible Image Transformation consists of three kinds of entities, A sender, A receiver, cloud service provider. This scheme is shown in Fig.

(i) Sender : Sender uploads a video which he wants to store in the cloud.

(ii) CSP : Store the Uploaded video as watermarked images.

(iii) Receiver : Receives video from the cloud which is uploaded by another user

At each time of login an ID based authentication scheme is used for authenticating the user.



PROPOSED SYSTEM

In the proposed system Secure Reversible Data Hiding Image Transformation using cloud storage where a user wants to upload a video to the cloud. When user is uploading the video in to the cloud at the same time the user choose a target image where the video can be embedded. The target image size must be larger than the frames size When a user upload the video first frames extraction process is occurred. Aftter getting the frames each frames are embedded into the target image which is selected by the user. LSB based embedding techniques is used for embedding the data to the target image. This image is encrypted using encryption algorithm. An ID based authentication method is used for authenticating the user. In the registration phase the user register to the system by providing their details this details are stored in the csp. At the authenticating phase it verifies the users. When the encrypted images are send to the CSP it embed some data to the encrypted images and make it as watermarked images, and these watermarked images are stored in the CSP.When a download request come from a user its checks authentication and then removes the additional data which is added to make the watermarked images. At the receiver side get the encrypted frames and it perform decryption to get the original images/frames. By using join operation these frames can be joined to make the original video.This proposed system reduces the ccomputation overhead at CSP, all the processs framing, embedding,encryptions are performes at client side.

RELATED WORK

Sushmita et.al [2] proposed a privacy preserving authenticated access control scheme. According to the scheme a user can create a file and store it securely in the cloud.

This scheme consists of use of the two protocols ABE and ABS .There are three users, a creator, a reader, and writer.
P Devaki et.al [3] are proposing an algorithm to provide confidentiality to the shares of the secret image and also to authenticate the dealer. In this algorithm we are combining the concepts of threshold secret sharing and image fusion. Shabnam Sharma and Usha Mittal[4] proposed that the kerberos technique for authentication. Kerberos is the authentication technique which is used to authenticate the clients to the server in Client-Server architecture.
Xinpeng Zhang [5] proposed a novel scheme for separable reversible data hiding in encrypted image. Here the data owner encrypt the original uncommpressed image with a encryption key and the data hider compress the least significant bits of the encrypted image to create a sparse space to accomadate some additional data by using data hiding key.Jen-Ho Yang and Pei-Yu Lin [6] proposed a new ID-based user authentication scheme. One-way hash functions and exclusive-or (XOR) operations are used in this scheme. It has low computation costs. In addition, it can be easily applied to the multi-server environments in cloud computing.

CONCLUSION

This work present a new scheme for data embedding in videos. Here the video frames are generated for the uploading video and then embed the frames in to a target image using LSB technique. The system embed the data and make the watermarked image. The cloud is semi trusted so an authentication method is used. ID based authentication can be used as the authentication method. This work improves the security of the uploaded video and provides authentication to the user.

REFERENCES

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

[2] 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.

[3] P Devaki and G Raghavendra Rao. "A novel algorithm to protect the secret image through image fusion and verifying the dealer and the secret image". *In Signal and Image Processing (ICSIP), 2014 Fifth International Conference on*, pages 77–80. IEEE, 2014.

[4] Shabnam Sharma and Usha Mittal. "Comparative analysis of various authentication techniques in cloud computing".

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

[6] 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.