International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 2 – FEBRUARY 2018.

A Literature review on Video Content Sharing with Security using Time-domain Attribute

S.Sangeetha [#1] and P.Alaguthai [*2]

[#] *Full Time Research Scholar, Department Of Computer Science, Sakthi College Of Arts and Science for Women, Oddanchatram, India.*

[*] *Assistant Professor, Department Of Computer Science, Sakthi College Of Arts and Science for Women, Oddanchatram, India.*

***Abstract*— Internet is gaining more and more popular now a days, so there is need to provide security for everything on internet. One of the most important concepts where we need to provide higher security is in communication between sender and receiver. Due to security threats the requirement of the secure transmission of the data is also increased the reason for developing the Data Hiding is the easy access of images, documents confidential data by the hackers who always monitor the system. Data hiding is the process of secretly embedding information inside a source without changing its content and meaning there is numerous techniques which hides the data. This paper aims to implement data hiding in compressed video. Like data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis. The sender first uses the stenographic application for encrypting the secret message. For this encryption, the sender uses text document in which the data is written and the image as a carrier file in which the secret message or text document to be hidden. The sender sends the carrier file and text document to the encryption phase for data embedding, in which the text document is embedded into the image file.In encryption phase, the data is embedded into carrier file which was protected with the password now the carrier file acts as an input for the decryption phase. The image in which data is hidden i.e. the carrier file is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase. Now the carrier file acts as an input for the decryption phase. The image in which data is hidden the carrier image is sent to the receiver using a transmission medium. E.g. Web or e-mail. The receiver receives the carrier file and places the image in the decryption phase.**

Index Terms*— *Streaming media, Access Control, Time domain analysis, Encryption, Video Content Sharing.

I. Introduction

With the rapid development of communication technologies and mobile devices, video applications (e.g., video chat, video conference, movies, short sight, etc.) have become more and more popular in our daily life.

Meanwhile, the demands on video quality and user experience have also been increasing significantly in many video applications, such as Ultra-high definition (UHD) live streaming, 3D movies, instant high definition (HD) video messages and so on. The ever-increasing demands pose great challenges on video processing, coding, presentation as well as communication, especially when the resources of media devices (e.g., bandwidth, power and computation) are limited.

Cloud computing, due to its flexible,scalable and economic resources, is a natural fit for storing, processing and sharing multimedia contents.

A. Video Processing

Video processing is a method to convert a video into digital form and perform some operations on it, in order to get an enhanced video or to extract some useful information from it. It is a type of signal dispensation in which input is video, like video frame or photograph and output may be image or characteristics associated with that image. Usually video Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them.

It is among rapidly growing technologies today, with its applications in various aspects of a business. Video Processing forms core research area within engineering and computer science disciplines too.

B. Steganography Image Analyses

There are currently three effective methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification1. LSB (Least Significant Bit).

Substitution is the process of modifying the least significant bit of the pixels of the carrier image. Blocking works by breaking up an image into blocks and using Discrete Cosine Transforms (DCT).

Each block is broken into 64 DCT coefficients that approximate luminance and color the values of which are modified for hiding messages. Palette Modification replaces the unused colors within an image‘s color palette with colors that represent the hidden message. I have chosen to implement LSB Substitution in my project because of its ubiquity among carrier formats and message types.

With LSB Substitution I could easily change from Image Steganography to Video Steganography and hide a zip archive Instead of a text message. LSB Substitution lends itself to become a very powerful Steganography method with few limitations.

LSB Substitution works by iterating through the pixels of an image and extracting the ARGB values. It then separates the color channels and gets the least significant bit. Meanwhile, it also iterates through the characters of the message setting the bit to its corresponding binary value3.

II. METHODOLOGIES USED FOR INTRUSION DETECTION SYSTEM

A. *System Model*

We consider a multi-authority access control system for cloud storage, as described in Fig.1. There are five types of entities in the system: the data owners (owners), the cloud server (server), the data consumers (users), the attribute authorities (AAs) and a certificate authority (CA). The owners define the access policies and encrypt their data under the policies before hosting them in the cloud. The server stores the owners' data and provides data access service to users. Each attribute authority is a trusted entity that is responsible for setting, revoking and updating user's attributes within its Administration domain. The CA is a fully trusted entity which is responsible for issuing a global *UID* for each user and AID system.

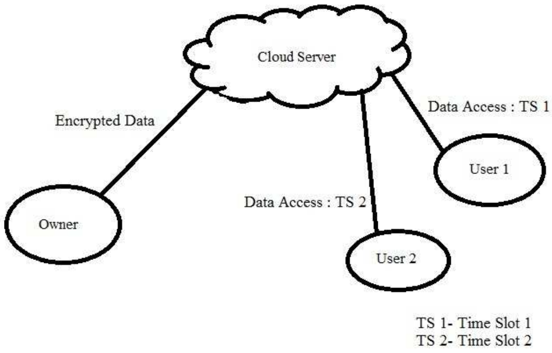


Fig 1 System Model of Multi-authority Access Control in Cloud Storage

B. *Security Model*

The security key has provided by two attribute 1.By Time 2.By passkey. In time a manual or automatic time as keyword is used so that the security over the time attribute is increased. In second a secret symmetric passkey is used to encrypt and decrypt the content.

C. *Secret Video Selection*

Here the secret video to be hidden is selected and the secret key with time is used for encryption, after that encryption details are shown below in that box. The reason why time and key used in same box is to increase the complexity for intruders (hackers) If the key or password is wrong the pop-up box of wrong passkey will not be shown, it is to confuse the intruders So that the intruder will have no knowledge of whets going on the entire process, so hacking of data is not possible.

After that selection the videos are partitioned into frames and encrypted, then later in next process the merging of that frames using LSB technique will occur. The least significant bit has the self-reversible embedding, so the correct frame.

D. *ADVANTAGES*

Merging of secret video with sample video make complications to intruders.

Time taken for decryption is less than that of encryption.

Self reversible embedding makes the extraction process easier.

III. SYSTEM ARCHITECTURE

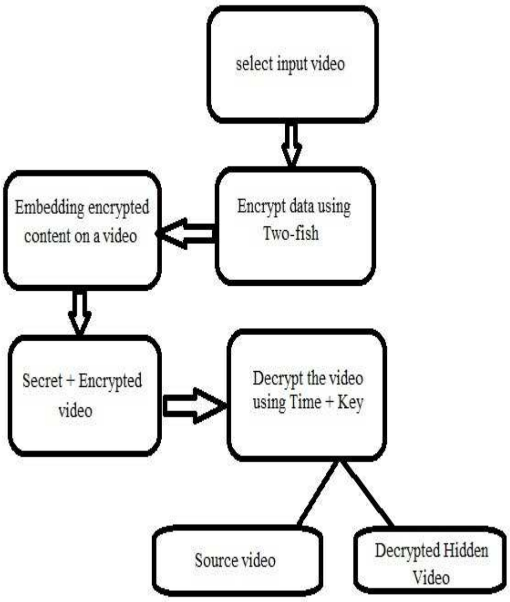

select input video
Encrypt data using Two-fish
Embedding encrypted content on a video
Secret + Encrypted video
Decrypt the video using Time + Key
Source video
Decrypted Hidden Video

Fig 2 System Architecture

A. *Secret Video Selection*

In this module,the processing of secret video takes place after the selection of video.

B. *FRAMES PARTITION*

SELF REVERSIBLE EMBEDDING - followed by video encryption.

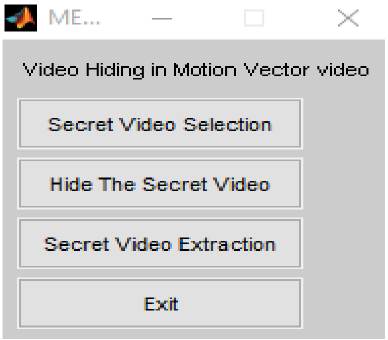


Fig 3 Video Hiding Menu

C. *FRAME PARTITION*

The selected secret video is partitioned into several frames and after that encryption of data with secret key takes place.

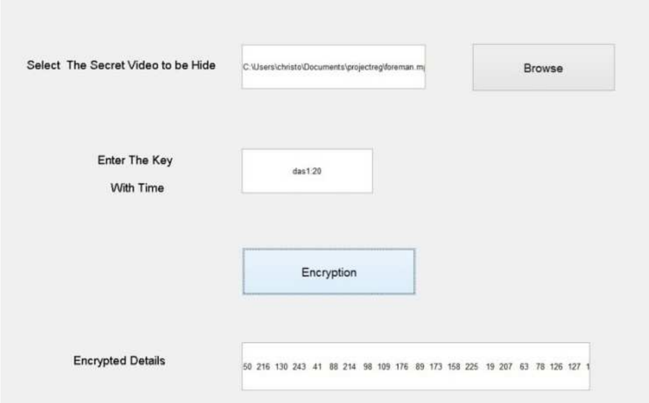
D. *SELF REVERSIBLE EMBEDDING*

The goal of self-reversible embedding is to embed the encrypted video frames into the sample video.

E. *Data Encryption*

In cryptography, Two fish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization.

Two fish is related to the earlier block cipher Blowfish. It uses 16 rounds to produce the encrypted video.



Select The Secret Video to be Hide: C:\Users\christo\Documents\projectreg\foreman.m

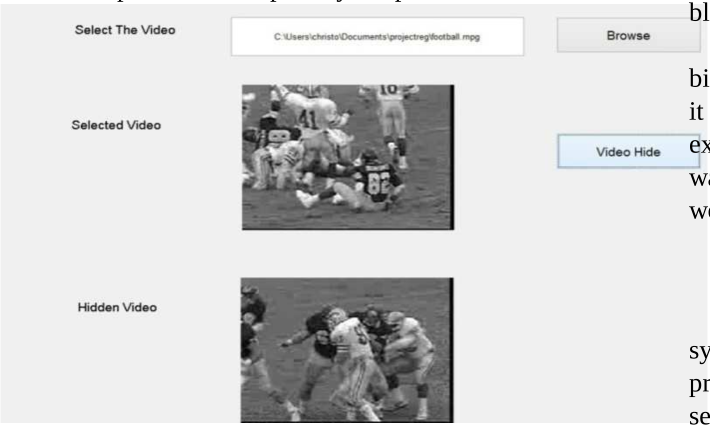
Enter The Key With Time: das1:20

Encrypted Details: 50 216 130 243 41 88 214 98 109 176 89 173 158 225 19 207 63 78 126 127 1

Fig 4 Secret Video Selection

F. Embedding Process

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

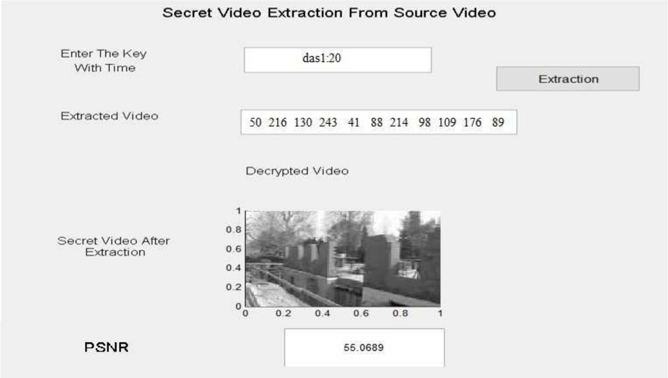


Select The Video: C:\Users\christo\Documents\projectreg\football.mpg

Fig 5 Hiding Secret video in Source Video

G. Data Extraction and Video Restoration

In this module,after providing the correct key the secret video gets extracted from sample video.



Secret Video Extraction From Source Video

Enter The Key With Time: das1:20

Extracted Video: 50 216 130 243 41 88 214 98 109 176 89

PSNR: 55.0689

Fig 6 Secret Video Extraction from Source Video

H. Peak Signal-To-Noise Ratio (PSNR)

The mean squared error (MSE) for our practical purpose allows us to compare the true‖ pixel values of our original image to our degraded image. The MSE represents the average of the squares of the "errors" between our actual image and our noisy image. The error is the amount by which the values of the original image differ from the degraded image. The proposal is that the higher the PSNR, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm.

This would occur because we wish to minimize the MSE between images with respect the maximum signal value of the image. For color images, the MSE is taken over all pixels values of each individual channel and is averaged with the number of color channels. Another option may be to simply perform the PSNR over a converted luminance or greyscale channel as the eye is generally four times more susceptible to luminance changes as opposed to changes in chrominance.

This approximation is left up to the experimenter. Data Embedding Procedure The encrypted message to be hidden is converted into its ASCII equivalent character and subsequently into binary digit. For an example if the character is an encrypted character of the message then as ASCII value for is 116 and binary value for it is 1110100.As image comprises of pixel contribution from red, green and blue components and each pixel has numbers from the color components (for 24-bit bitmap image each of red, green and blue pixel has 8 bit).

At 8 bit of the color number, if we change least significant bits, our visual system cannot detect changes in pixel and thus it is possible to replace message bits with image pixel bit. For example if we consider the pixel value 10111011, and we want to store the information in the least significant bit, at the worst situation the pixel changes to 10111010.

IV. CONCLUSION

A reversible steganographic algorithm using texture synthesis. Given an original source texture, our scheme can produce a large steganographic synthetic texture concealing secret messages. We believe our proposed scheme offers substantial benefits and provides an opportunity to extend steganographic applications. Another possible study would be to combine other steganography approaches to increase the embedding capacities.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Tech. Rep., 2009.

[2] W. Zhu, C. Luo, J. Wang, and S. Li, “Multimedia cloud computing,” IEEE Signal Processing Magazine, vol. 28, no. 3, pp. 59–69, 2011.

[3] D. D´ıaz-S´anchez, F. Almenarez, A. Mar´ın, D. Proserpio, and P. A. Cabarcos, “Media cloud: an open cloud computing middleware for content management,” IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 970–978, 2011.

[4] X. Wang, M. Chen, T. T. Kwon, L. Yang, and V. Leung, “AMES-Cloud: a framework of adaptive mobile video streaming and efficient social video sharing in the clouds,” IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 811–820, 2013.

[5] M. Hefeeda, T. ElGamal, K. Calagari, and A. Abdelsadek, “Cloudbased multimedia content protection system,” IEEE Transactions on Multimedia, vol. 17, no. 3, pp. 420–433, 2015.

[6] H. Shen, L. Zhuo, and Y. Zhao, “An efficient motion reference structure based selective encryption algorithm for h. 264 videos,” IET Information Security, vol. 8, no. 3, pp. 199–206, 2014.

[7] Z. Shahid and W. Puech, “Visual protection of hevc video by selective encryption of cabac binstrings,” IEEE Transactions on Multimedia,vol. 16, no. 1, pp. 24–36, 2014.

[8] B. Zeng, S.-K. A. Yeung, S. Zhu, and M. Gabbouj, “Perceptual encryption of h. 264 videos: Embedding sign-flips into the

integer-based transforms," IEEE Transactions on Information Forensics and Security, vol. 9, no. 2, pp. 309–320, 2014.

[9] T. St¨utz and A. Uhl, "A survey of h. 264 avc/svc encryption," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 3, pp. 325–339, 2012.

[10] PKCS1, "public key cryptography standard no. 1 version 2.2," RSA Labs, 2012.

[11] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Advances in cryptology. Springer, 1985, pp. 10–18.

[12] G. Boztok Algin and E. T. Tunali, "Scalable video encryption of h. 264 svc codec," Journal of Visual Communication and Image Representation, vol. 22, no. 4, pp. 353–364, 2011.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. Of CCS'06. New York, NY, USA: ACM, 2006, pp. 89–98.

[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. of PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.

[15] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. of EUROCRYPT'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 568–588.