Current Trends in Technology and Sciences
ISSN: 2279-0535. Volume: 3, Issue: 6 (Oct.- Nov. 2014)

Secure Communication with the help of Encryption in Video Steganography

Chandra Prakash Shukla[1], Awadhesh Kumar Singh[2],
1Asst Professor (CSE Dept), Satyam Engineering College Ghaziabad, India, 30cp90@gmail.com
2Asst Professor (CSE Dept), Satyam Engineering College Ghaziabad, India, awadheshcse@gmail.com

Abstract - In many organizations like FBI and RAW, Banks share confidential and important data on any network. Some unauthorized persons always try to use these facts to harm someone. In either case, message sender or receiver has to pay the price. To protect from these undesirable acts, we proposed a new system with use of Steganography and cryptography to make sure high security of the message. One hides the existence of the message and the other distorts the message itself. Here we use one of the most efficient and a secure algorithm is RSA Algorithm for encryption. Video Steganography is a popular technique of hiding message into video file. We first encrypt our message and decoy with an efficient algorithm and then hide at random frames in video.

Key words - Steganography, Encryption, Cipher, Public Key.

I. INTRODUCTION

Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word steganos which literally means "covered" and graphia which means "writing", i.e. covered writing. The most common use of steganography is to hide a file inside another file [1]. Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography[3] could be more eligible than other multimedia files, because of its size and memory requirements[3].

Here, we use RSA algorithm for message encryption. RSA algorithm is a very secure technique for cryptography. There is a chance to detection of original message after couples of attacks. Therefore, we proposed a new system with combination of steganography and cryptography.

The paper is organized as follows:

Section II describes the proposed approach of this paper.

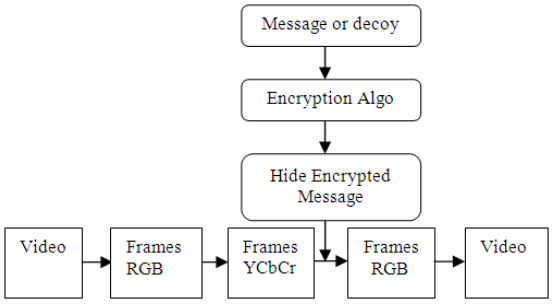
Section III describes encryption with RSA algorithm.

Section IV describes the popular Steganography technique Video Steganography.

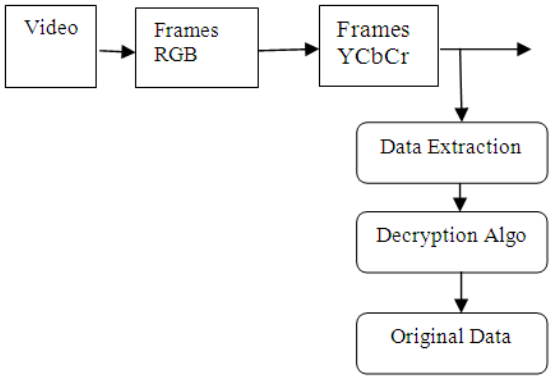
Section V describes the Experimental results of my above discussed approach.

II. PROPOSED APPROACH

The block diagrams of video encoder and decoder used to hide and extract the data are given in Figure 1.



(a) Block diagram of data hiding in video



(b) Block diagram of data extraction from video

Figure 1 Block diagram of data hiding and extracting in video

The method to embed and extract the hidden message is described as follows.

First, we convert original message into cipher text with RSA algorithm.

Second, we convert cipher text into binary numbers.

- Encoder

1) Select the frames from video

a) Converting frames from video for hiding message and decoy randomly.

b) RGB frames will be converting into YCbCr format then choose Y (luminance) for message hiding.

c) We hide message in frequency of Y part of YCbCr.

d) We hide decoye in frequency of Y part of YCbCr.

2) Apply Embedding Algorithm[1]

If C is the value of the bit to be hide and Va is embedded point in the frames.
When C is 0, the Va is modified as:

$$\begin{cases} Va & \text{if } Va\%2 = 0 \\ Va+1 & \text{if } Va\%2 = 1 \end{cases}$$

When C is 1, the Va modified as:

$$\begin{cases} Va & \text{if } Va\%2 = 1 \\ Va+1 & \text{if } Va\%2 = 0 \end{cases}$$

Apply the embedding algorithm we produce an efficient result.

- Decoder

1) Select the right frames for message extraction.

a) Select the frames from video in which message hidden already.

2) Extract the embedding bit by embedding mark.

$$\begin{cases} C=1 & \text{if } Va\ \%2 = 1 \\ C=0 & \text{if } Va\%2 = 0 \end{cases}$$

Where, Va is the embedded point and C is the embedded bits.

Key exchange Approach:

Here we are going to discuss one time share password. We send to receiver's side the value of public key 'e', and multiple of 2 prime number 'Pk' because of encryption, value of index frame and size of bits embedded in index frame.
Here receiver can generate the value of index frame with the help of generator.
We do following operations on message_size and encryption 'e'. Then we send message_size and generator. Here we can choose generator anything randomly.

Operation	Generator
Divide, Floor	1
Divide, Ceil	2
Multiply	3
Add	4
Subtraction	5
Mode	6
Power	7

III. EXPERIMENTAL RESULTS

We are using AVI (Audio Video Interleaved) format video for hiding message and converting AVI video into PNG (Portable Network Graphics) format image frames. We are using PNG format because it is lossless data compression we can get real data after compression.

Video Properties	**Baseline Values**
Bits Per Pixel	24
Frame Rate	15
Video Format	RGB24

TABLE I. Configuration Parameters of the Video

Figure 2 the 17th frame of video rofl.to30secondvideo before hide 96 bit message

Figure 3 the 17th frame of video rofl.to30secondvideo after hide 96 bit message

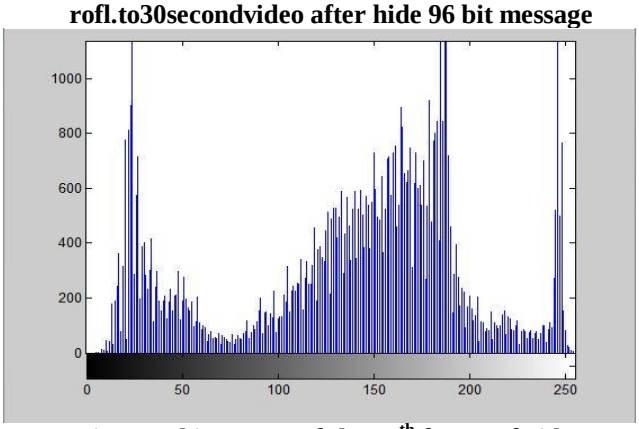


Figure 4 histogram of the 17th frame of video rofl.to30secondvideo before hide 96 bit message

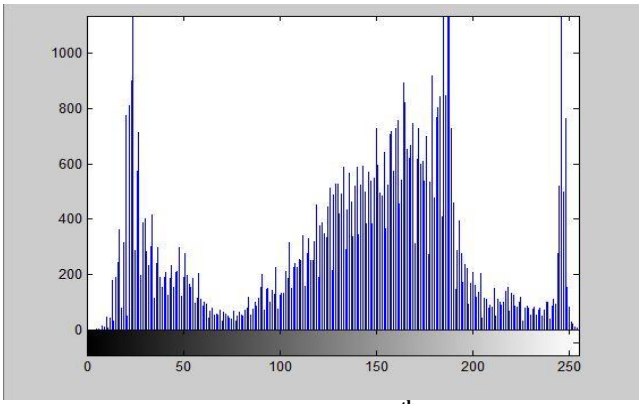


Figure 5 histogram of the 17th frame of video rofl.to30secondvideo after hide 96 bit message

Here, we can see the difference between both histograms it means our message is successfully embedded into frames.

PSNR value of above frames before message hide and after message hide is 78.3457.

IV. Future Work

An algorithm, which can decide the random positions in the frames to hide message bits, could be developed. This will further enhance this method of Video Steganography.

V. Conclusion

We can conclude that the proposed system is more effective for secret communication over the network channel. In this paper we presented a way of hiding the secret data inside the cover medium such as video. The proposed system for data hiding uses RSA for encryption and decryption which generating public key, which results in more secure technique for data hiding. We are using random selection of frames and hide decoy with message also.

References

[1] Yu Li, He-xin Chen, Yan Zhao, "A New Method of Data Hiding Based on H.264 Encoded Video Sequences", 978-1-4244-5900-1/10/$26.00 ©2010 IEEE.

[2] R. Balaji, G. Naveen, "Secure Data Transmission Using Video Steganography", International Journal of Computational Engineering Research (ijceronline.com) VOLUME 2. July-August 2012.

[3] A. Swathi, Dr. S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, September 2012.

[4] V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari, "Data hiding in audio signal, video signal, text and jpeg images", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[5] Tsutomu Matsumoto, Junji Shikata, "Authenticated Encryption and Steganography in Unconditional Security Setting", 0-7803-9491-7/05/$20.00 ©2005 IEEE.

[6] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010.

[7] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998

[8] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013.

[9] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science 1. Elsevier.

[10] Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984).

[11] a b c d e f g AJ Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-85237.

[12] Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk , Borko Furht, "New approaches to encryption and steganography for digital videos", © Springer-Verlag 2007.

[13] Neil F. Jonhson and Stefan C. Katzenbeisser, "A survey of steganographic techniques", *Artech house*.

[14] Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

[15] Yam bern Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh, "A Short Survey on Image Steganography and Steganalysis Techniques", IEEE-International Conference 978-1-4577-0748-3/12/$26.00 © 2012 IEEE.

[16] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images", World Academy of Science, Engineering and Technology 50 2009.

[17] Vinod Pankajakshan, Prabin Kumar Bora, "Detection of Motion-Incoherent Components in Video Streams", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 1, MARCH 2009.