International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

EDGE Based Video Steganography with RSA Algorithm

G R Manjula[1], Sushma R B [2], Sahana H[3]
[1,2,3]Department of CSE, JNNCE, Shivamogga, Karnataka, India

***Abstract*— In the present scenario, various data security and data hiding algorithms are used to provide security over network application. Cryptography and steganography are the two major techniques used for secure communication. Cryptography is a technique that enables to store sensitive information and transmit it across the internet so that the information cannot be read by anyone except the intend recipient. Steganography is a technique of hiding information within the multimedia like text, image, audio, video etc. Nowadays, Video steganography is one of the important technique to hide huge amount of information within digital media like text, image, audio and video. In this paper, there is a hybrid approach of cryptography and steganography for video steganography to achieve high capacity data and high quality of stego video on the basis of performance metrics like MSE and PSNR. The proposed methodology is a combination of different techniques such as RSA encryption and decryption, Edge detection, 4LSB substitution method and 2LSB technique, in which secret image and secret message is hidden inside a cover video in all layers of RGB color frames. The experimental results is implemented on MATLAB software and resulting values show that our proposed methodology has high imperceptibility and high security communication.**

***Keywords*—Video Steganography; RSA encryption and decryption; Sobel Edge Detector; 4LSB; 2LSB; PSNR; MSE.**

I. Introduction

Nowadays, Information security is extremely challenging issue that affects many sectors including computers and communication through internet. Because in today's contemporary world, interchanging of personal information from one peer to another peer is obstacle; that is how to preserve our secret data from cyber hackers in the internet. The various applications like chats, e-mails etc can be sent and received through various kinds of multimedia data like text, images, video regularly over the internet. Many attacks were discovered on cyber security to provide confidentiality for the users. But these attacks failed due to security algorithms and affected authentication, confidentiality, identification, availability and integrity of user data.

Cryptography and Steganography are two ways that provide identification, authentication, integrity confidentiality and availability of user data as well as maintain the secrecy and privacy of data provided by the user.

In Cryptography, transmitter scrambles the information using an encryption key and receiver will extract the original information from scrambled message using the correct unscrambling key. In other case, the message is not mixed in Steganography, rather the information is covered up in a transporter typically called as cover medium.

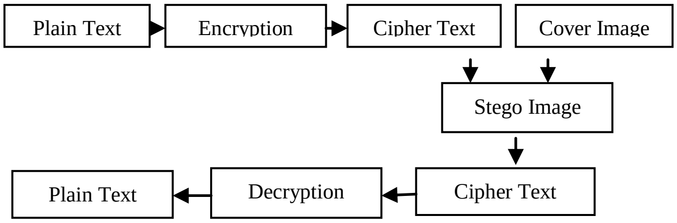

Fig.1: Combination of Steganography and Cryptography

In Fig 1, the message is encrypted using Cryptography and then encrypted message is hidden in cover medium called Steganography. The resulted stego-image is transmitted without revealing the secret message. If hackers want to detect the secret message from stego-object then attacker need to defeat steganographic technique. But it is not possible, because attacker should know the cryptographic decoding key to decipher the encrypted data. The study techniques for deciphering cipher information and detecting hidden information are called cryptanalysis and steganalysis.

Than audio and image more data can be hidden in one or more frames of the carrier video. Recently, Video steganography is one of the growing technique and this paper deals more about video steganography. Video steganography is a technique that is used to conceal the secret information behind the carrier video and sent through transmission medium. The important aspect of video steganography, structure is complex compare to other types of digital media and video size is huge that is suitable for cover medium. Large amount of hidden information can hide in video files inside their bit streams. So, nowadays video steganography is more preferable than other digital media.

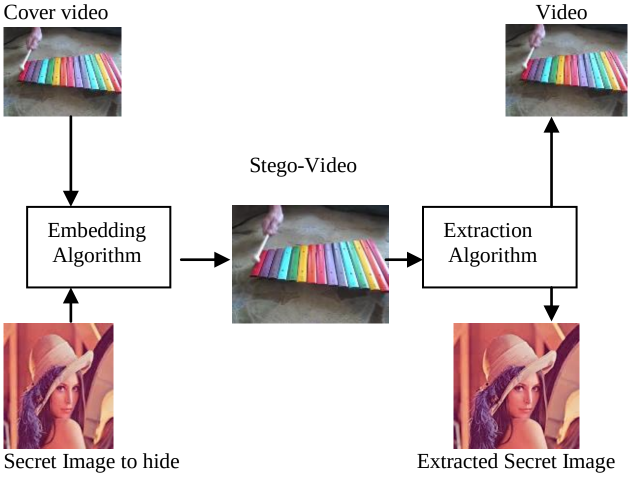

Fig.2: Video Steganography Mechanism

Fig 2 explains about mechanism of video steganography. The cover video(xylopone.mp4) and secret image (lena.jpg) is analyzed. The secret image is embedded in cover video using embedding algorithm and generate stego-video. Then using extraction algorithm the user can extract the secret image from stego-video. Advantage of using the cover video is development in security is developed against the hackers by its complex structure and has high embedding capacity.

The further paper gives the details of Proposed methodology in section I, algorithms of embedding and extraction process are described in section II and experimental results and performance calculations are explained in section III. In section IV conclusion & future work are explained.

II. PROPOSED METHODOLOGY

In our proposed work an approach of edge detection is done for secret text and secret image behind a different video file. The different techniques are used in our proposed methodology that will give better results and helps to increase capacity and provide security for the data over the network.

A. Phases of Proposed Work

The following phase explains about proposed methodology:

a) Pre-Processing: In our research work, we are selecting .mp4 file as a cover video. The cover video file is divided into number of frames. These fragmented frames act as a carrier medium to hide secret Image and secret text.

b) Random Frame Selection: In this phase, frames are selected randomly so that it is difficult to analyze for the attacker whether the secret image and text is present inside cover video frames. Here, we are selecting 10 random frames from extracted frames of video.

c) Edge Detection: In our work, we are embedding secret text and secret image behind edge pixels and non edge pixels. As the edges are very sharp and finite in nature their pixel values changes frequently and have discontinuity effect [1]. In edge detection process the edge regions are highlighted from the given secret image. To detect the edge pixels in random selected frames, we are using sobel edge detector. The Sobel edge operator performs a 2-D spatial gradient measurement on an image. It is used to find the approximately absolute gradient magnitude at each point I of an input secret image. The Sobel edge detector uses a pair of 3 x 3 convolution masks, one estimating gradient in the x-direction and the other estimating gradient in y-direction [15]. The Sobel edge detector is sensitive to noise in images, and highlights them as edges. Hence, Sobel edge detector is recommended in huge data communication found in data transfer.

d) RSA (Rivest-Shamir-Adleman Algorithm): The RSA algorithm is a asymmetric block cipher and makes our secret message more secure [9]. Asymmetric means two different keys are used to encrypt and decrypt the messages. Only one round of encryption process is possible. Large integers like 1,024 bits in size are used. The secret information is converted into unreadable format and impossible for the attackers to identify the message. In this paper instead of using symmetric key based encryption, RSA encryption algorithm is used. The RSA algorithm increases its security from attackers. To encrypt and decrypt the secret text, transmitter and receiver use their own public and private keys. It is based on factorial number for encryption. It is difficult for hackers to find out the factoring problem and decrypt the secret message, so RSA encryption is used that provide security to our algorithm and hide the encrypted secret text behind video frames.

Following algorithm is used in RSA,

1. Choose p and q
2. Compute $n = p * q$
3. Compute $\varphi(n) = (p - 1) * (q - 1)$
4. Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime.
5. Compute a value for d such that $(d * e) \% \varphi(n) = 1$.
6. Public key is (e, n)
7. Private key is (d, n)
8. For encryption C=me(mod n) and decryption m =cd (mod n)

In Fig 3, the plain text is encrypted to cipher text using public keys and then decrypted from cipher text to plain text using private key and finally generate secret message.

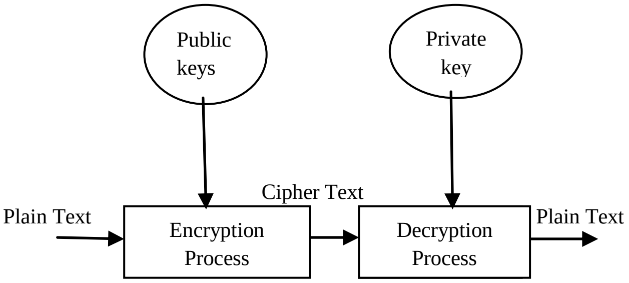

Fig.3 : RSA Algorithm (Asymmetric Key Cryptography)

In symmetric key based algorithms such as XOR encryption, AES, DES etc. the secret message can be easily breakable by hackers since they are using third party to share the secret key between sender and receiver, so they are not secure.

e) Embedding Process: In our work, we are hiding both secret information and secret image between edge pixels and non-edge pixels. The secret data (.txt) is hidden between edge pixels using 4LSB substitution method. The secret image (.jpg) is hidden between non-edge pixels using 2LSB technique (Smooth areas).

f) Extraction Process: The hidden data is decoded from stego video using our algorithm and final output is generated. The final output displays the secret information and secret image.

g) Comparison: In our work, the proposed methodology is compared on the basis of quality metrics such as PSNR, MSE and achieve high imperceptibility performance and large hiding capacity and security of data for video steganography process.

III. ALGORITHMS

A. Embedding Algorithm (Sender Side)

The fig 4 explains about how edge pixels are recognized using 4LSB method and non-edge pixels using 2LSB method. The sender selects video file and hide secret image and text inside random frames using following algorithm:

- Select carrier video (.mp4 file) from current folder and divide into number of frames.
- Enter the number between 1 to 10 to select the frames from extracted video frames.
- Select secret image (.jpg) and enter public key to perform encryption using RSA algorithm.
- Enter secret message (.txt). The entered message is converted to ASCII code.
- Enter the public key to get message encrypted using RSA algorithm.
- Both, encrypted image and encrypted text is embedded behind carrier video.
- To detect the edges of selected frames Sobel edge operator is used.
- In Non-edge pixels, 2 bits of secret image are hidden in red and green channel using 2LSB technique and 4 bits of secret text is hidden in blue channel using 4LSB technique in edge pixel.
- The quality metrics for all selected frames is computed using Mean Square Error (MSE) and Peak Signal To Noise Ratio(PSNR).
- Finally generated Stego Video file is received where encrypted image and text is inside and can communicate over the network such as chats, e-mail etc.

B. Extraction Algorithm (Receiver Side)

At receiver side, secret image and text is extracted from stego video file. The following algorithm is explained for extraction process:

- Select stego video and extract secret image and secret text from frames.
- To decrypt the secret image from non-edge pixels enter the private key using RSA decryption algorithm and obtain the original secret image.
- To decrypt the secret text from edge pixels enter the private key using RSA decryption algorithm and obtain the original secret text.
- Exit.

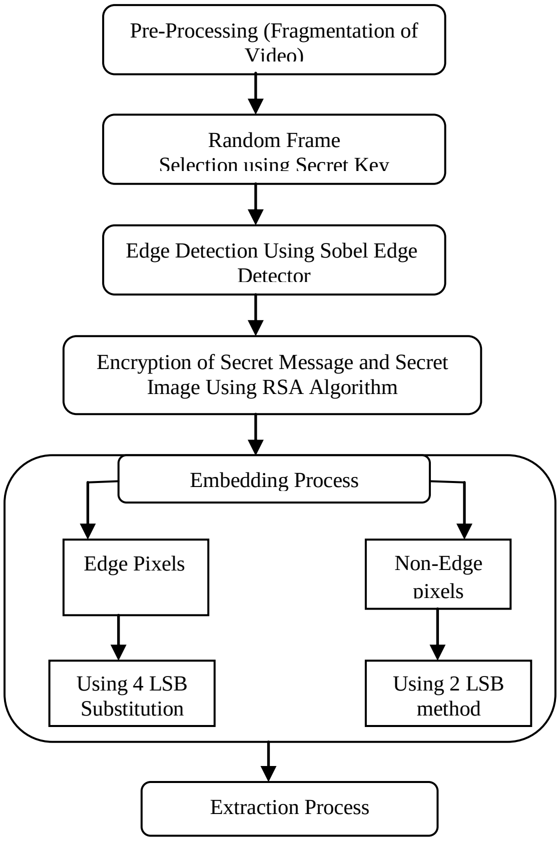
Pre-Processing (Fragmentation of Video)
Random Frame Selection using Secret Key
Edge Detection Using Sobel Edge Detector
Encryption of Secret Message and Secret Image Using RSA Algorithm
Embedding Process
Edge Pixels
Non-Edge pixels
Using 4 LSB Substitution
Using 2 LSB method
Extraction Process

Fig .4 : Flow Chart of Proposed Methodology

IV. EXPERIMENTAL RESULTS & PERFORMANCE CALCULATIONS

The MATLAB Software version15 is used to implement the proposed methodology and achieve the experimental values for that algorithm. Fig. 5 shows four different video formats that are used in our proposed work. They are: Akiyo360.mp4, Container.mp4, Carphone.mp4 and Foreman.mp4.

Fig. 5: Various Cover Videos (Akiyo360.mp4, Container.mp4)

In Fig.6 five various secret images are hidden in cover video. They are: Lena, Pepper, Tiger, Building and Flower respectively in .jpg format all 128 X 128 in dimension.

Fig. 6: Secret Images- Lena, Pepper, Tiger, Building and Flower respectively in .jpg format

The proposed methodology is implemented using five different secret images and four various cover videos of Akiyo360.mp4, Container.mp4. The size of the secret image is 128 x 128 in dimension.

Fig. 7: Cover Video

Fig. 8: Secret Image

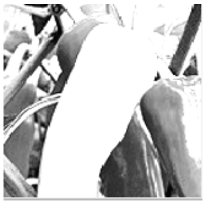

Fig. 9: Encrypted Secret Image

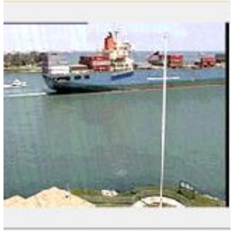

Fig. 10: Stego Video

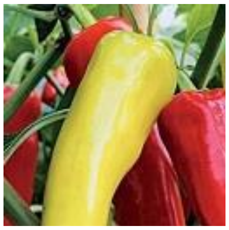

Fig. 11: Decrypted Secret Image

In Fig.7, the video file 'Container.mp4' is used as a cover video. The 10 random frames are selected to hide the secret image. The secret image pepper.jpg in hidden in cover video as shown in fig 8. Using RSA encryption algorithm the secret image is encrypted as shown in fig 9.After hiding the encrypted secret image next we need to embed inside carrier video using embedding algorithm. A non-edge pixel is identified in encrypted secret image using 2 LSB technique. The 2 bits are hidden in red channel and green channel and obtain stego video as shown in fig 10. Then obtain the decrypted secret image as in fig 11.The edge pixel is identified in secret message using 4LSB method. The 4 bits are hidden in blue channel and obtain the stego object. By hiding 4 bits in each pixel of frame the capacity of hidden data will increase in a video frame, edge of frame and corresponding stego frame.

A simple example is demonstrated how the secret message is encrypted and decrypted.

```
Enter Secret Message: 'How are you'
ASCII Code of the entered Message:
   72   111   119   32   97  114  101   32  121  111  117
Enter public key to perform Encryption: 11
Encrypted - Secret Message
enc_msg =
 144   222   238   64   194   228   202   64   242   222
234
Enter private key to perform Decryption: 2291
Decrypted - Secret Message: How are you
```

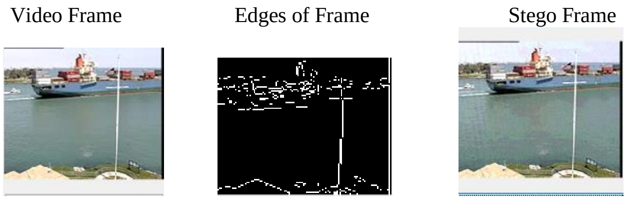

Fig. 12 : Selected Video Frame, Edge of Frame and Stego Frame

The quality of stego video is same as that of cover video and cannot identify by human visual system. The hacker is unable to understand the extracted secret image and secret text from cover video and creates full confusion to the hackers as the image bits are scrambled using RSA algorithm. This algorithm is robust against the hackers.

In fig 12 the edges of the frame is identified from cover video and obtain the stego video. Due to random frame selection the security is high on the basis of secret key. One extra layer protection is presented by using RSA algorithm. If the user knows the correct secret key then those user can decrypt the secret message.

If user tries to access repeatedly then stego file will get damaged due to unauthorized access for video steganography process. To calculate the performance metrics such as PSNR and MSE between stego object and its cover video is calculated. Two video frames are used to hide five different images, MSE for all RGB channel is measured and PSNR for all RGB channel is measured. Table 1 and Table 2 gives the experimental results of PSNR and MSE of all RGB channel.

$$MSE(m) = \frac{1}{N}\sum_{i,j}(Y_{out}(i,j,m) - Y_{in}(i,j,m))^2$$

$$PSNR(m) = 10\log_{10}\left(\frac{(2^{B-1})^2}{MSE(m)}\right)$$

Table -1
Experiment Result of PSNR

Video Sequences(.mp4)	**Secret Images (128 x 128)**	**PSNR R**	**PSNR G**	**PSNR B**
Container	Lena	58.088	46.412	59.081
Container	Pepper	58.385	46.432	61.245
Container	Tiger	58.396	46.651	58.263
Container	Building	58.383	46.443	51.821
Container	Flower	58.197	46.488	67.970
Akiyo	Lena	64.174	50.9224	56.7773
Akiyo	Pepper	64.399	50.700	63.102
Akiyo	Tiger	64.602	51.112	65.045
Akiyo	Building	64.739	50.622	63.696
Akiyo	Flower	64.557	51.180	61.662

Table -2
Experiment Result of MSE

Video Sequences(.mp4)	Secret Images (128 x 128)	MSE R	MSE G	MSE B
Container	Lena	0.101	1.485	0.080
Container	Pepper	0.094	1.478	0.048
Container	Tiger	0.094	1.405	0.097
Container	Building	0.094	1.474	0.427
Container	Flower	0.098	1.459	0.010
Akiyo	Lena	0.024	0.525	0.136
Akiyo	Pepper	0.023	0.553	0.031
Akiyo	Tiger	0.022	0.503	0.020
Akiyo	Building	0.021	0.563	0.027
Akiyo	Flower	0.022	0.495	0.044

V. CONCLUSION & FUTURE WORK

Video steganography is an information hiding tool and there are lots of applications in research field. The proposed methodology is a combination of edge detection, 4LSB substitution, RSA algorithm and 2LSB technique. We achieve high quality and security because of high PSNR and low MSE values. The embedding capacity is also high as we are using video frames. The huge amount of information can be hidden behind the cover video using these methodologies.

In future work, various formats of video can be used such as .avi, .mov, .Flv. Different image formats can be used. In different languages the secret message can be hidden such as Hindi, Punjabi etc. We can also hide the video inside cover video file and transmit across the world.

REFERENCES

[1] Ramandeep Kaur, Pooja, Varsha" A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques". IEEE WiSPNET 2016 conference.

[2] Shraddha Jagad, DaxaVekariya." A Proposed Approach to Hide Image on Video Using DCT and ID3 Algorithm of Data Mining" in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 11, November 2015.

[3] Nishi Khan, Kanchan S. Gorde. "Video Steganography by Using Statistical Key Frame Extraction Method and LSB Technique" in International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 10, October 2015.

[4] Anmol D Kulkarni, Esti bansal, Rasika R Jadhav, Hole Rajashree B, Laxmi Madhuri. " Improved Data Security Using Two Stage Steganography"in International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 4, April 2016 .

[5] Hemant Gupta, Setu Chaturvedi, " Video Steganography through LSB Based Hybrid Approach" in IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[6] Atallah M. Al-Shatnawi, " A New Method in Image Steganography with Improved Image Quality" in Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915.

[7] Ramandeep Kaur, Pooja, Varsha " The Non-Tangible Masking of Confidential Information using Video Steganography" in International Journal of Computer Applications (0975 – 8887) Volume 119 – No.17, June 2015.

[8] Nishi Khan, Kanchan S. Gorde, "Data Security by Video Steganography and Cryptography Techniques" in International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569) Vol. 11, Issue. 5, Sep-2015.

[9] Rajdeep Bhanot and Rahul Hans., " A Review and Comparative Analysis of Various Encryption Algorithms" in International Journal of Security and Its Applications Vol. 9,No.4 (2015), pp. 289-306.

[10] Ajit Danti,G R Manjula, Priya K," An Innovative Approach For Video Steganography Using Statistical Features In Round- Lsb" in International Journal of Engineering Applied Sciences and Technology, 2016 Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 194-199.

[11] Bharti Chandel, Dr.Shaily Jain, " Video Steganography: A Survey" in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17.

[12] Ashwini B. Akkawar, Prof. komal B. Bijwe, " Hybrid Approach for Embedding Text or Image in Cover Images"in International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 5, Issue 5, May 2016.

[13] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi, " A Technique for Data Hiding using Audio and Video Steganography" in International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 2, February 2016 ISSN: 2277 128X.

[14] Syeda Musfia Nasreen , Gaurav Jalewal, Saurabh Sutradhar," A Study on Video Steganographic Techniques" in International Journal of Computational Engineering Research (IJCER) ISSN (e): 2250 – 3005 || Volume, 05 || Issue, 10 ||October – 2015||

[15] O. R. Vincent, O. Folorunso " A Descriptive Algorithm for Sobel Image Edge Detection" in Proceedings of Informing Science & IT Education Conference (InSITE) 2009.