ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

Security and Privacy for Digital Communication Using Dual Steganography

Syeda Thasnim Fathima[1], D.Vijayalakshmi[2], kiran[3]

M. Tech Student, Bangalore Institute of Technology, Karnataka, India[1]

Assistant Professor, Bangalore Institute of Technology, Karnataka, India[2]

Assistant Professor, Dept. of ECE, GMIT, Mandya, Karnataka, India[3]

ABSTRACT: Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. In this proposed paper the focus is on increasing data security using dual steganography. In dual steganography secret message is first embedded into cover medium and then resulted stego-object will be again embedded into other cover medium. Mentioned paper also provides a computable evaluation of dual steganography in terms the reduction in the mean square error (MSE) and hence increase in peak signal to noise ratio (PSNR) measure between original host files and generated stenographic files.

KEYWORDS: Steganography, image, MSE, Cover medium, Video

I. INTRODUCTION

The word steganography comes from the Greek “Steganos”, which mean covered or secret and – “graphy” mean writing or drawing. Therefore, steganography mean, literally, covered writing. It is the art and science of hiding information such its presence cannot be detected and a communication is happening. A secrete information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. This technique plays a prominent role in future applications.
The basic model of steganography consists of Carrier, Message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message.
Basically, the model for steganography is shown on following figure:

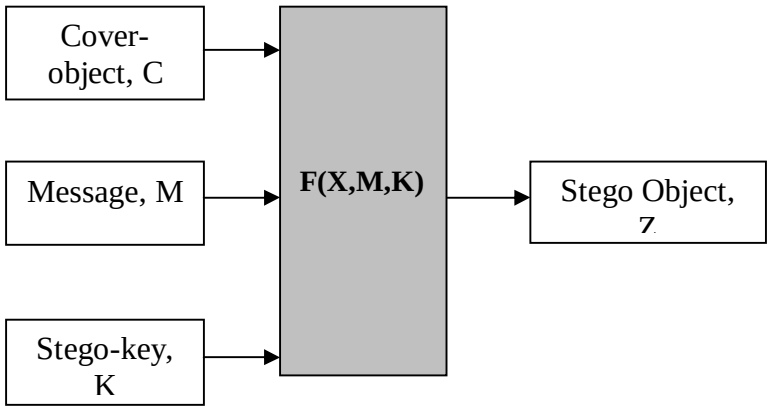

Fig.1 Basic model of Steganography

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

Message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the Stego-object. The Embedding Process can be further done again in order to main the respective security and privacy. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

II. LITERATURE SURVEY

J. Fridrich, [1] Symmetric ciphers based on two-dimensional chaotic maps: This paper provides the methodology of how to use the 2 dimensional chaotic maps on a square matrix to create a symmetric block encryption schemes. A chaotic map is first generalized by introducing parameters and then discretized to a square lattice of points which represent pixels or some other data items. Although the discretized map is a permutation and thus cannot be chaotic, it shares certain properties with its continuous counterpart as long as the number of iterations remains small.

G. Chen, Y. Mao, C.K. Chui, [2] A symmetric image encryption scheme based on 3D chaotic cat map: This paper employs a 3D cat map to shuffle the image pixels in order to provide the resistance against the statistical and differential attacks.

N. Provos, P. Honeyman, [3] Hide and seek an introduction to steganography: This paper is based on maximizing the embedding capability of an image while keeping high security.

O.Khalind, B.Aziz, [4] Single mismatch 2LSB embedding steganography: This paper includes the 2LSB steganography that makes fewer changes to the cover image with a lower probability of detection. a new method of 2LSB embedding steganography in still images. The proposed method considers a single mismatch in each 2LSB embedding between the 2LSB of the pixel value and the 2-bits of the secret message, while the 2LSB replacement overwrites the 2LSB of the image's pixel value with 2-bits of the secret message.

T.Xiang,K.W.Wong,X.liao, [5] selective image encryption using spatiotemporal chaotic system : This paper will gives the explanation about importance of 4 MSB's for image visualization, and encryption of 4 MSB's to get the good balance between security and efficiency.

M.Podesser, H.P. Schmidt, A. Uhl, [6] Selective bit plane encryption for secure transmission of image data in mobile environments: This paper will provide us a information about why we will not use the smart phones for complicated encryption operations.

III. PROPOSED METHODOLOGY

Dual steganography of text for secure text and image communication has been proposed. Here in dual steganography, image steganography is used within video steganography

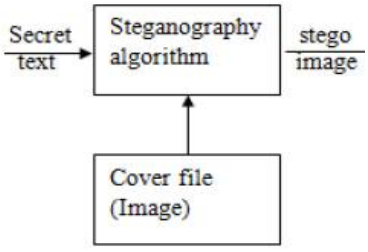

Fig. 2 Embedding Process

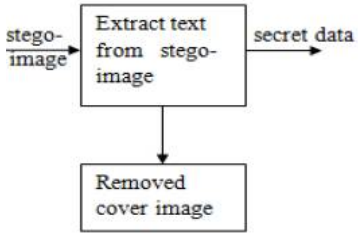

Fig. 3 Extraction Process

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

EMBEDDING PROCESS

The process of embedding data in host file is shown in figure (2). The secret data has been embedded inside cover image with the help of 4-bit LSB (least significant bit) algorithm along with the stego-key. The key used is maximum of 64 bit length. Key is embedded in the cover image during the LSB embedding process. This should be known at the receiver side during the apprehend process for retrieving the secret file.
The algorithm works as follows:

Image steganography:
• Cover image is separated into RGB planes.
• Secret data taken is then converted into binary form.
• Those values are separated into upper and lower nibbles which are embedded in two separate planes of the cover image.
• Upper nibbles are embedded in green plane and lower nibbles in red plane using 4bit LSB method.
• Stego key is embedded inside the blue plane.
• After which, all the three planes are combined to generate stego-image.

Video steganography:
• Input the cover video stream.
• Convert the video sequence into a number of frames.
• Split each frame into the YUV color space.
• Apply the two dimensional DWT twice separately to each Y frame component.
• Embed the message (stego-image) into the middle frequency coefficients (LH, HL) of each of the Y components.
• Apply the inverse two dimensional DWT on the frame components.
• Rebuild the stego frames from the YUV stego components.
• Output the stego videos, which are reconstructed from all embedded frames.

EXTRACTION PROCESS

The process of extraction is shown in figure (3). In section the process of retrieving secret massage (text) from stego-image is introduced.
The algorithm works as follows:
• Input the cover video stream
• Convert the video sequence into a number of frames.
• Split each frame into the YUV color space.
• Apply the two dimensional DWT twice separately to each Y frame component.
• Extract the message (stego-image) from the middle frequency coefficients (LH, HL) of each of the Y components.
• Perform inverse DWT method.
• The extract secret massage from stego-image

IV. RESULT AND DISCUSSION

The proposed algorithm was performed using MATLAB. For all the experiments presented herein, we used the numbers of LSB bits to be replaced was fixed at four. Several experiments were conducted to test the robustness and imperceptibility of the algorithm. Imperceptibility is the perceived quality of the host image that should not be distorted by the presence of the secret massage the perceptual imperceptibility of the embedded measure in terms of Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) and Root Mean Square error (RMS) between the cover and stego-images may be calculated. Lesser the MSE higher the PSNR values and imperceptibility.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

1. Mean Square Error

Mean squared error (MSE) is defined as an average of the square of the difference between actual image and encrypted image. The MSE is given by the equation,

$$MSE = \frac{1}{MxN} \sum_{i=1}^{n} \sum_{j=1}^{n} (x(i,j) \quad y(i,j))^2$$

Where x (i, j) represents the original image and y (i, j) represents the encrypted image and i and j are the pixel position of M x N image.

MSE is zero when x (i, j) =y (i, j).

2. Peak Signal to Noise Ratio (PSNR)

The peak signal to noise ratio is evaluated in decibels and is inversely proportional to MSE. It is given by the equation:

$$PSNR = 10 \log_{10}(\frac{255}{MSE})$$

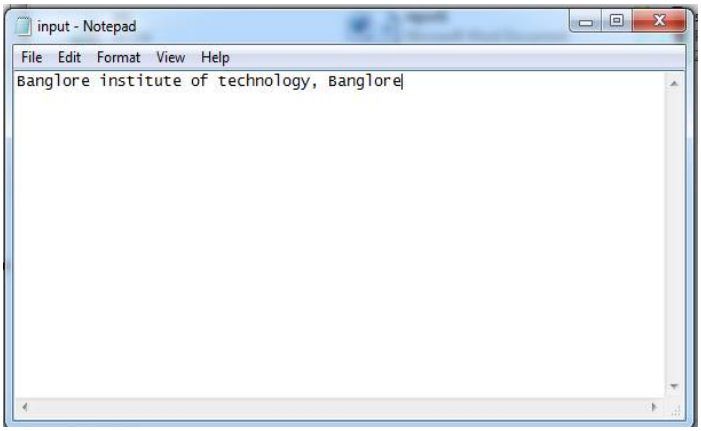

Fig. 4 Input Text Data

Fig. 5 Cover RGB Image

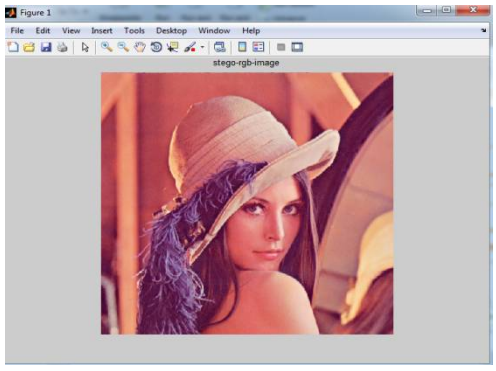

Fig. 6 Stego RGB image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

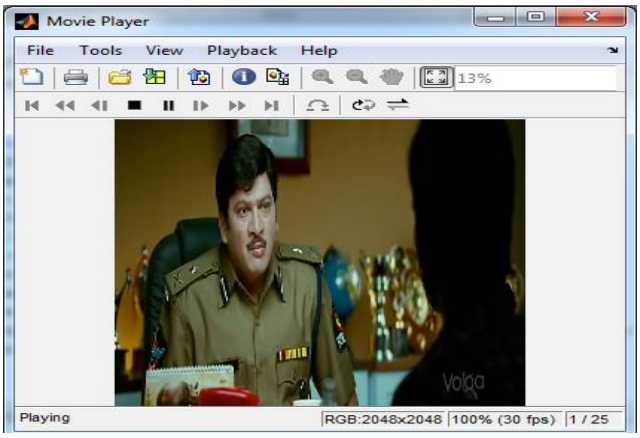

Fig. 7 Input RGB Video

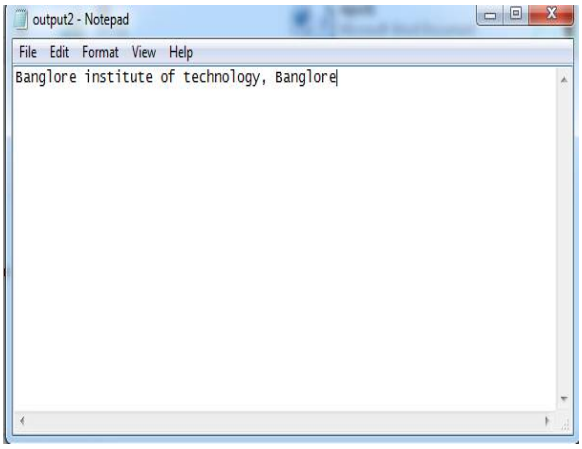

Fig. 8 Password Key for Extraction Process

Fig. 9 Input Image

Fig. 10 RGB Cover Image

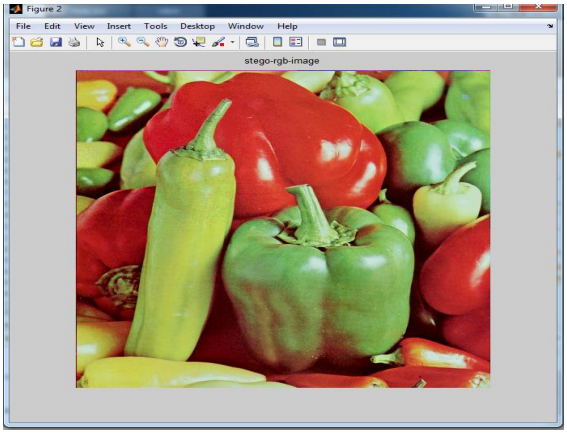

Fig. 11 Stego RGB Image

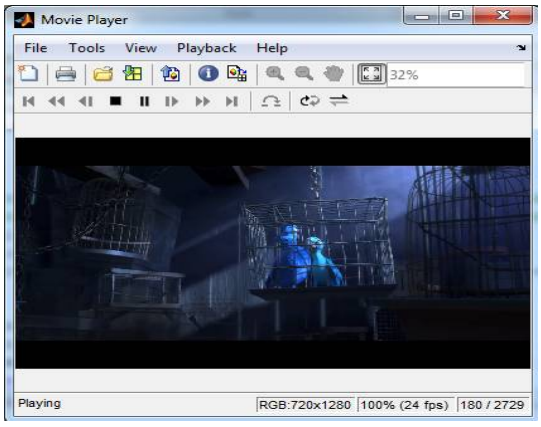

Fig. 12 Input RBG Cover Video

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

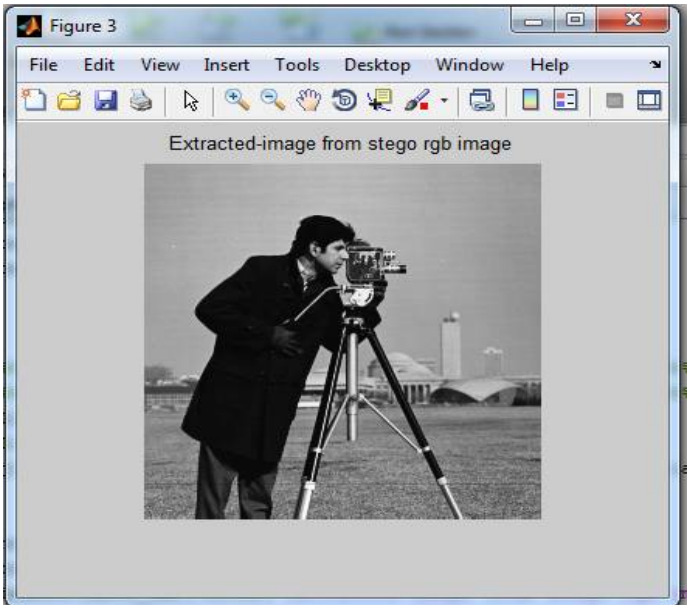

Fig. 13 Extracted input image

Input	Size	MSE	PSNR(dB)
Text file	49B	0.0494	61.1925
image	37.3KB	6.5523	39.9812

TABLE 1 MSE and PSNR values

V. CONCLUSION

This paper presents a state of the art combination work of two popular information security approaches, namely cryptography and steganography. However both of techniques provide security for secrete information but separately one can't guarantee for absolute security of data. Therefore to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed**.** Therefore experimental results show that the proposed model is effective. It maintains the quality of the video and no variation between the cover data and stego-data that can be detected by the human vision system. Future work can be done in way to combining the concepts of hybrid cryptography and audio steganography, to provide more security to the secrete message

REFERENCES

[1] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Stegano-graphy," IEEE computer society,2003.
[3] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution" Hong Kong Received 17 May 2002.
[4] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett 36 (25) (2000) 20692070.
[5] Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

[6] Y.-C. Liang et al., "Sensing-Throughput Trade-off for Cognitive Radio Networks," IEEE Trans. Wireless Communication, vol. 7, pp. 1326–37 ,April 2008

[7] T.Morkel, J.H.P.Elofi, M.S. Olivier, "An overview of image steganography" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.

[8] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.

[9] Javaid A.Shakih, Shabir A.Parah, Abdul M. Hafiz and G. M. Bhat, "Data Hiding in Scrambled Images: a new double layer security data hiding technique" Computers and Electrical Engineering, 2012.

[10] Phad Vitthal S , Bhosal Rajkumar S., Panhalkar Archana R., "A Novel Security for mystery Data Using Cryptography & Steganography" IJCNIS, 2012.

[11] Kanzariya Nitin K, Nimavat Ashish V., " Comparison of Various pictures Steganography Techniques" IJCSMR, 2013.

[12] Rohit G Bal and Dr. P.Ezhilarasu, "An Efficient Safe and Secured Video Steganography Using Shadow Derivation", IJIRCCE march 2014.

[13] Anwar H.Ibrahim and Waleed M.Ibrahim, "Text Hidden In Picture Using Steganography: Algorithms and Implication For Phase Embedding and Extraction Time", IJITCS February 2013.