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)

Vol. 5, Issue 4, April 2016

Dual Steganography: A New Hiding Technique for Digital Communication

Jigar Makwana[1], S.G Chudasama[2]

PG Student, Dept. of E&C, S.S. Engineering College, Bhavnagar, Gujarat, India[1]

Assistant Professor, Dept. of E&C, S.S Engineering College, Bhavnagar, Gujarat, India[2]

ABSTRACT: In comparison with analog communication, digital communication provides several advantages like better quality, ease of editing, high fidelity, compression, etc. But with rapid growth of World Wide Web and advance computer network, there are some issues related to content security, privacy, and media authentication. In modern age in which data is conveyed through digital medium, the protection of data is top priority concern for any organization. Digital steganography is an advance technique in which secret data can't be detected easily. Steganography envelopes and information to such degree that it is invisible to a spectator. 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. A preliminary result shows the high imperceptibility of the proposed method as well as the hiding capacity of presented method.

KEYWORDS: Dual steganography, Image steganography, LSB, Video steganography, DWT.

I.INTRODUCTION

Ancient people used various techniques to send secret messages during war times. Sending of massages safely and securely has been top priority for any organization that deals with confidential data. Information hiding techniques are necessary for military, intelligence agencies, internet banking, privacy, etc. so it is on-going research area in present time [1]. Increased use of internet, information become available on-internet, a person who possessesan internet can easily get data from internet for information that they want. As more and more techniques for hiding information are developed and improved, more and more different information detecting techniques are also developed. That has produced a strong need to create new techniques for protecting confidential information from hackers. There are numbers of data hiding techniques available for different purpose and applications like steganography, cryptography, and watermarking [1]

Steganography means covered writing. Cryptography means scrambling of data such that it becomes meaningless to eavesdroppers [3]. Watermarking means embedding of watermark signal into data to generate watermark object [7]. So that it is mostly used in copyright protection and authentication of media. In steganography method confidential data is embedded in such way that the existence of secret data is invisible. Steganography approaches are mainly organized into spatial domain and frequency domain based approaches [1]. Spatial domain techniques operate on pixel wise and embeds messages directly in Least Significant Bits (LSB) of data [10]. In frequency domain, host files are first converted to frequency domain e.g. by using FFT, DCT or DWT and then the messages are embedded in some or all of the transformed coefficients. Steganography methods can also be classified base on cover medium as text, image, video, audio and protocol steganography.

The cover file/medium referred as cover object, after embedding data into it, it is referred as stego-object. A stego-key is used for embedding process so that only authorized person can access the hidden message. Steganography gives an ultimate guarantee of confidentiality that no other hiding technique can ensure. The primary concern of steganography is to maximize embedding rate and minimizing the detectability of resulting stego-object against steganalysis. To detect the hidden data in stego object is called steganlysis. Dual steganography can provide potential solution for that security concern.

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)

Vol. 5, Issue 4, April 2016

Dual steganography that is, first embed secret information into one cover medium and then again embed the resulting stego-object generated from first embedding process into other object. In this paper dual steganography is performed by first embedding data into image cover file using LSB(spatial domain technique) and then resulted stego-image is embedded into video using DWT(frequency domain technique)[4].The advantage of using video as cover object in last embedding process is to add security against several hacker attacks due to relative complexity of video structure compared to image structure.

II.LITERATURE REVIE

There are numbers of steganography techniques available that use digital image/video as carrier. In [7] various steganography methods and classification of image steganography approaches based on type of host object, domain type and file format has been introduce and concluded that the uncompressed file format(bmp,gif)based on lossless compression provides high data capacity and more convenient for data hiding algorithm. N.provos and P.honeyman [9] define the main objectives for any steganography algorithm such as capacity, undetectibility and robustness. Most LSB based techniques were proposed in an attempt to enhance its tamper resistance. For example, [5] presented an algorithm for hiding video using LSB. The BPCS algorithm proposed in [8] to compensate the weakness of lsb substitution methods. BPCS embeds data in bit plane complex region where the cover object are divided into informative and noise region. J.k mandal and P.dutta [11] present hash based lsb for video steganography using hash function. In [6] method presented is based on pixel-wise administration of video files to hide the data.

[2] Presents a comprehensive review of video steganography techniques and comparisons between those techniques. Furthermore popular image and video quality metrics also discussed. in [10] presents primary goal of steganography techniques is to maximize embedding rate and minimize the detectability of resulting stego-file against steganalysis

III.PROPOSED ALGORITHM

In this paper dual steganography of text for secure communication has been proposed. Here in dual steganography, image steganography is used within video steganography.

A. Data insertion stage

The process of embedding data in host file is shown in figure (1). 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 10 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.

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)

Vol. 5, Issue 4, April 2016

- 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.

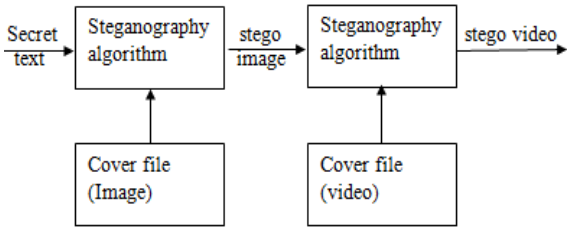

Fig.1 Embedding process.

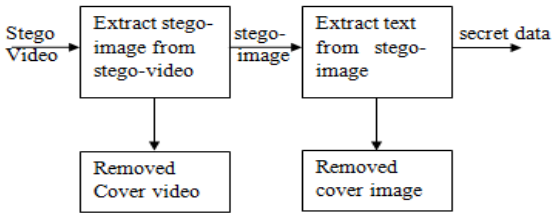

Fig.2 Extraction process

B. Data extraction stage.

The process of extraction is shown in figure (2). In section the process of retrieving the embedded message (stego-image) from stego-videos first and the 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.PERFORMANCE EVALUATION

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.

$$\text{MSE}=\frac{1}{HW}\sum_{x=1}^{H}\sum_{y=1}^{W}\big(S(x,y)-T(x,y)\big)^2$$

Where and are the pixel values at row i and column j of the host image and generated stego-image respectively.

$$PSNR = 10log_{10}(255/MSE)\ dB.$$

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)

Vol. 5, Issue 4, April 2016

V. 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.

1. Result regarding image steganography: for BMP files Size of data file 200KB.

File name	Original size	H x W	MSE	PSNR(dB)
T21.bmp	1.02MB	600x600	$3.795e^{-9}$	84.2079
T22.bmp	937KB	800x600	$8.714e^{-10}$	90.597
T23.bmp	1.37MB	800x600	$4.711e^{-10}$	93.268
T24.bmp	1.37MB	800x600	$8.26e^{-10}$	88.9716
T25.bmp	881KB	621x484	$2.025e^{-9}$	86.224
T26.bmp	337KB	800x600	$1.404e^{-9}$	88.5257

TABLE 1.PSNR and MSE values (BMP files)

2. Result regarding image steganography: For same cover file but different data types.Cover file(T28.bmp file) size 83.3kb and dimension 600x800.

File name	Original size	MSE	PSNR(dB)
TT1.docx	226KB	$1.130e^{-9}$	89.467
T32.txt	14KB	$1.636e^{-9}$	87.861
TT3.pdf	166KB	$1.293e^{-9}$	88.8832
TT4.m	9KB	$1.648e^{-9}$	87.829
TT5.jpg	48KB	$1.552e^{-9}$	88.08

TABLE 2.PSNR and MSE values

3. Result regarding image steganography: for jpeg files. Size of data file 56KB.

File name	Original size	H x W	MSE	PSNR (dB)
T1	143KB	1536x1024	2.50x10-4	92.522
T2	109KB	800x600	2.06x10-4	87.75
T3	819KB	3000x2000	6.18x10-5	98.657

TABLE 3.PSNR and MSE values (JPEG)

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)

Vol. 5, Issue 4, April 2016

- After text is embedded within image, generated stego-image will be embedded within video using DWT method.
  Video steganography: Video size=1.48MB
  HxW=288x352 FPS=25fps

File to hide	MSE	PSNR(dB)
T21.bmp	0.0189	65.36
T22.bmp	0.0228	64.55
T23.bmp	0.0229	64.53
T1.jpg	0.0198	65.164
T2.jpg	0.0249	64.168
T3.jpg	0.0219	64.72

TABLE 4.VIDEO STEGANOGRAPHY

VI.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.

In all experiments, the average PSNR is greater than 84dB for image steganography and 64 for video steganography. 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] Sumeet Kaur, Savina Bansal, and R. K. Bansal., "Steganography and Classification of Image Steganography Techniques". International Conference on Computing for Sustainable Global Development.978-93-80544-12-0/14 2014 IEEE 2014
[2] Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa. "Video steganography: a comprehensive review" DOI 10.1007/s11042-014-1952-z Springer Science New York 2014
[3] Wang Tianfu, K. Ramesh Babu., "Design of a Hybrid Cryptographic Algorithm". International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283
[4] Ramadhan J. Mstafa, Khaled M. Elleithy., "A high payload video steganography algorithm in DWT domain based on BCH codes(15,11)", 978-1-4799-6776-6/15 2015 IEEE
[5] Vishnu S babu and Prof. Helen K J. "A Study on Combined Cryptography and Steganography:" International Journal of Research Studies in Computer Science and Engineering Volume 2, Issue 5, May 2015, PP 45-49 ISSN 2349-4840 (Print) & ISSN 2349-4859(online).
[6] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb "A secure covert communication model based on video steganography" 11331. 978-1-4244-2677-5 IEEE 2008
[7] Priyanka Singh, Suneeta Agarwal, and Akanksha Pandey "A Hybrid DWT-SVD Based Robust Watermarking Scheme for Color Images and its Comparative Performance in YIQ and YUV Color Spaces" 2013 3rd IEEE International Advance Computing Conference (IACC) 978-1-4673-4529-3 IEEE 2012
[8] Smita P. Bansod Vanita M. Mane Leena R. Ragha., "Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity". 978-1-4577-2078-9 IEEE 2011.
[9] N. Provos and P. Honeyman, "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003
[10] M. Kharrazi, H.T. Sencar and N. Memon, "Cover Selection for Steganographic Embedding", IEEE International Conference on Image processing, 8-11 oct 2006, Atlanta USA, pp. 117-120.
[11] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta.,"hash based least significant bit technique for video steganography(HLSB)". Nternational Journal of Security, Privacy and Trust Management (IJSPTM) Vol. 1, No 2, April 2012 DO: 10.5121/ijsptm.2012.2201.