IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HIDING HIGH SECURITY INFORMATION USING DUAL STEGANOGRAPHY

[1]G. Siva Sankar Varma, [2]R. Anila, [3]R. Gayathri, [4]N. Revathi, [5]M. K. Tejaswi

[1]Assistant Professor, [2,3,4,5]UG Student

[1]Electronics and Communication Engineering,

[1]BVRIT HYDERABAD College of Engineering for Women, Hyderabad, INDIA

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.

***Index Terms*- 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]. There are numbers of data hiding techniques available for different purpose and applications like steganography, cryptography, and watermarking. Steganography means covered writing. Cryptography means scrambling of data such that it becomes meaningless to eavesdroppers [2]. Watermarking means embedding of watermark signal into data to generate watermark object [5]. 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].

II. 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.

2.1. 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 over side during the apprehend process for retrieving the secret file.

The algorithm works as follows:

Image steganography:

In Image Steganography cover image is separated into RGB planes. Then, 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 and stego key is embedded inside the blue plane. After which, all the three planes are combined to generate stego-image.

Video steganography:

In video steganography [4] first input the cover video stream then 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 [3] on the frame components. Rebuild the stego frames from the YUV stego components. Output the stego videos, which are reconstructed from all embedded frames.

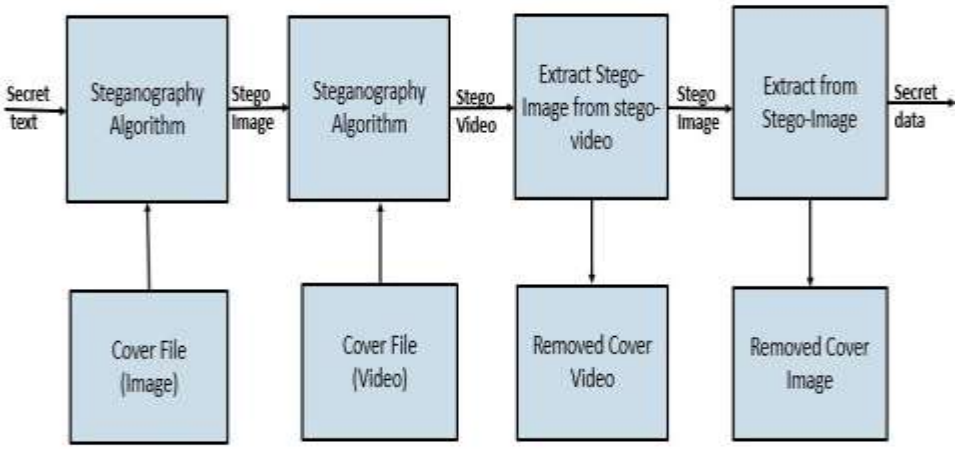

Figure 1: Block Diagram

2.2. 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. Then, 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. Thus, secret message from stego-image gets extracted.

III. RESULTS

The proposed algorithm is performed in MATLAB. The output is presented in the following figures.

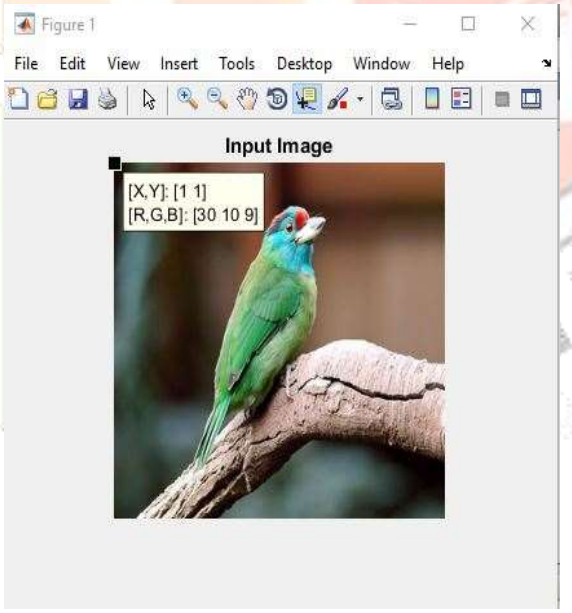

Figure 2: Input Image Without any Message

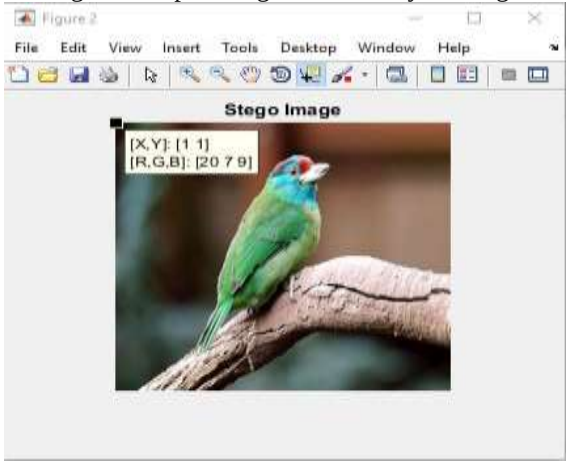

Figure 3: Stego-Image Embedded with Message

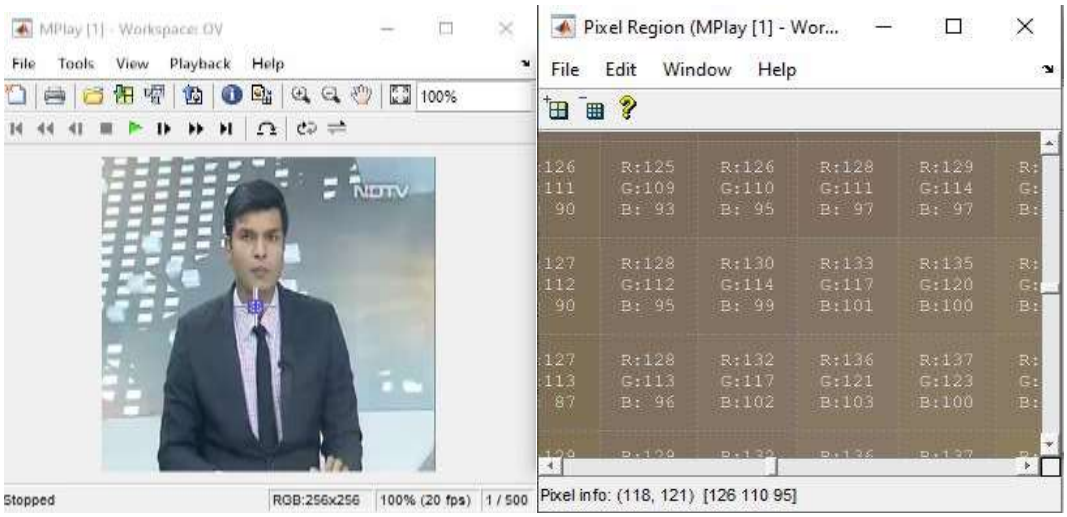

Figure 4: Input Video Without Stego-Image

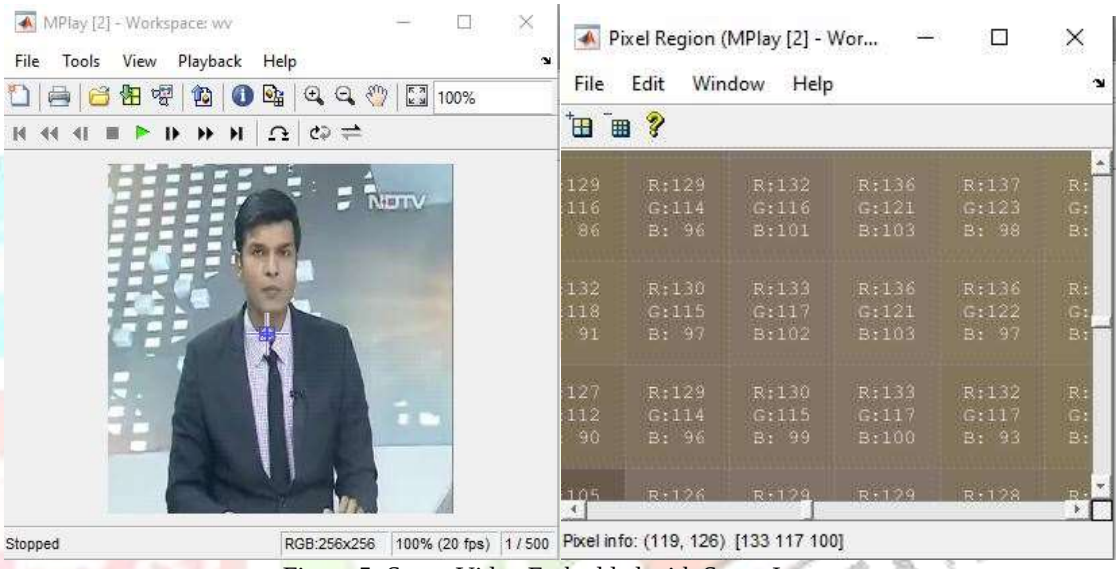

Figure 5: Stego-Video Embedded with Stego-Image

IV. 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.

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.

V. FUTURE SCOPE

In this modern era of technology with the increase in need of source and robust communication for military, intelligence agencies, internet banking etc., the information technology sector looks towards the future research in the field of dual steganography. Some future researches may include: Developing an environment which should be platform independent, focusing on other methods like audio to achieve high security, use of best algorithm to achieve high efficiency, robustness and embedding capacity for secure.

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] Wang Tianfu, K. Ramesh Babu., "Design of a Hybrid Cryptographic Algorithm". International Journal of Computer Science & Communication Networks,Vol 2(2), 277-283.

[3] Ramadhan J. Mstafa, Khaled M. Elleithy., "A high payload video steganography algorithm in DWT domain based on BCH codes(15,1 1)", 978-1 -4799-6776-6/15 2015 IEEE.

[4] 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.

[5] 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.