Dual Protection for Data using Steganographic Techniques with Embedded Framework

T. R. Kowshika, K. Geetha

Abstract*: As the world is getting digitalized, the rush for need of secured data communication is overtop. Provoked by the vulnerability of human visual system to understand the progressive changes in the scenes, a new steganography method is proposed. The paper represents a double protection methodology for secured transmission of data. The original data is hidden inside a cover image using LSB substitution algorithm. The image obtained is inserted inside a frame of the video producing a stego-video. Stego-video attained is less vulnerable to attacks. After decryption phase, the original text is obtained which is error-free and the output image obtained is similar as the cover image. The quality of stego-video is high and there is no need for additional bandwidth for transmission. The hardware implement is required in order to calculate the corresponding analytical results. The proposed algorithm is examined and realized for various encryption standards using Raspberry Pi3 embedded hardware. The results obtained focuses on the attributes of the proposed model. On comparing with other conventional algorithms, the proposed scheme exhibits high performance in both encryption and decryption process with increase in efficiency of secured data communication.

Index Terms: Data Hiding, Data Security, Steganography.

I. INTRODUCTION

The evolution of technology across generators is booming day by day. High speed communication of data tends to be the hot core concern in this vast development. Digital communication have made process of living easy. It has turned to be a mandatory part of everyone live hood. Earlier the mode of communication was the biggest challenge but now the security behind every single communication or transmission is a question mark. In the case of cryptography, the original data to be transmitted is encrypted using different patterns. Thereby, the quality and efficiency of content is diminished at the end of decryption. So another preferred method is data hiding in which the content of the text is hidden inside a text or any multimedia file like audio, video. Various data hiding techniques are available such as watermarking, steganography. Steganography is method of concealing information of any form into a cover medium. To preserve data through the channels during transmission security methods are to be incorporated. The important information is hidden inside a multimedia file and the technique should be at high security levels. Digital watermarking and steganography differ from one another and have their individual specifications, functionalities and merits. Watermarking provides secured transmission along with copyrights protection. In steganography, the message is embedded into cover image and cover image can be chosen according to the user technical suitability. Image watermarking is an approach of bit insertion into an image file. The process is mainly concerned about data protection and copyrights. Watermarking is of two types visible and invisible. Invisible watermarking has high level of imperceptibility as compared to other conventional techniques like encryption. Robust watermarking is consummated in such a way that the bits are scattered and rearrange throughout the cover image and changes are made invisible. In LSB watermarking, bit value is placed at the least bit value of pixel of the image It is robust, imperceptible, authenticated and have high tolerance over various attacks. Use of multimedia files for steganography makes use of the weakness of human visual system (HVS) which is less sensitive to the pattern changes. In the process of embedding information into a video with high security, firstly video framing should be done. Video is a collection of set of frames, the frames played in sequence forms a video. It involves collection of individual frames with frame rates . On corresponding to the frame rate the video is split into collection of images. In video steganography, the file which to be hidden is placed in between frames using various embedding techniques. One suitable method is least significant bit substitution in which the image or data to be embedded is placed inside any one of the frame. A frame is considered and its corresponding least significant bit pixel is replaced with the image pixel that is to be hidden.

The main goal of the proposed work is to observe the security levels and analyze the performance metrics like peak signal to noise ratio, mean square error, entropy, computational time and efficiency of the system. This is adopted with the hardware implementation using Raspberry Pi. Raspbian OS along with Open CV-python which is the Python API is also used. Further this paper is organized as follows. Section 2, briefs us about the related. In section 3, the design and implementation of various algorithms used is illustrated. In section 4, performance metrics and efficiency of the system is analyzed and tabulated. Section 5, states us with and future work.

II. RELATED WORK

Considering today's scenario, data hiding is highly robust than traditional encryption methods. As encryption requires conversion of original data content during transmission which at the end of reception produces very low quality data and it is vulnerable to security attacks. So data hiding is meant to be used for secured transmission.

In [1] Mritha Ramalingam proposes a new method of video steganography using scene change detection technique. The main objective is to reduce the distortion level of video and maintain high security for the embedded data.

Revised Version Manuscript Received on Jun 20, 2019.

T.R.Kowshika, Embedded Systems, SASTRA Deemed to be university, Thanjavur, India.

K.Geetha, CSE Department, SASTRA University, Thanjavur, India.

Discrete wavelet transform (DWT) and discrete cosine transform (DCT) coefficient are the methods used to enhance the quality of the video. DCT is used for detecting the scene change which enhances the security of the message and DWT fuses and normalizes the payload of the video. The experimental results shows superior performance in security and quality of the files used.

A video steganography method suggested by Mahdi Hashemzadeh [2] uses motion clues of feature points technique of data hiding. The intention of this approach is to show high performance over embedding capacity and imperceptibility of hidden data. The path follows detection of high dynamic area of video scene which are later used for hiding data and eventually selecting the right amount of data to be hidden in that particular area. Statistical indicators extricated from the feature point behaviors are used predict the embedding capacity of each pixel. The metrics shows sustainable improvement in performance over other existing methods and the perpetual invisibility rate is very high.

Xinpeng Zhang [3] introduces a novel approach in which the image is encrypted using suitable encryption key and the LSB of the image is compressed is create sparse space so hiding data. During decryption phase, the original image is retrieved using encryption key and by analyzing the spatial correlation of the image inserted on the sparse space. This method solves the problem of miscarrying of image and data quality during recovery stage.

Rupali Bhardwaj [5] analysis the process and the efficiency of image steganography based on complement message and Inverted LSB substitution. In this first the secret message is complimented using pixel generated randomly through pseudo random number. The complimented message is inserted inside cover image using Inverted LSB method which shows a high PSNR, low MSE at the decryption phase along with high visual quality. But pseudo random number generator has low performance so should alternative method.

III. PROPOSED METHOD

In this segment ,we propose a double protection method of data-hiding inside multimedia file. The inputs of the process are the secured message, cover image and cover video and the output is the stego-video. The data-hiding process is carried out inside two different medium one is inside a image and another inside video so it is known to be double protection. The proposed method is processed through three main steps: (1) Data watermarking inside a image using LSB substitution (2) Video framing (3)Video Steganography. The scheme of data hiding and data extraction along with its setup is define in the following chapters.

A. Data hiding process

The proposed data-hiding with double protection methodology is illustrated as a block diagram in Fig1.In this method the original data, cover image and cover video is used as inputs to create a steganographic video into which the text that is to be securely transmitted is placed. The follow of this process involves the usage of three different media such as data, image and video.

Firstly, the data to be transmitted is taken and the characters of the text files is considered individually. Each character is transformed into its corresponding ASCII values that are grouped as a array of binary bits. A standard image is to be selected into which the binary bits are to be embedded. This process is carried out using LSB watermarking and we get a watermarked image. Second, a preferred video is seized and framing is done i.e. the video is split as frames in a required ratio. Among the frames a desired frame is taken into which the watermarked image is hidden using LSB replacement. As a result we obtain a stego-video inside which the data is hidden securely.

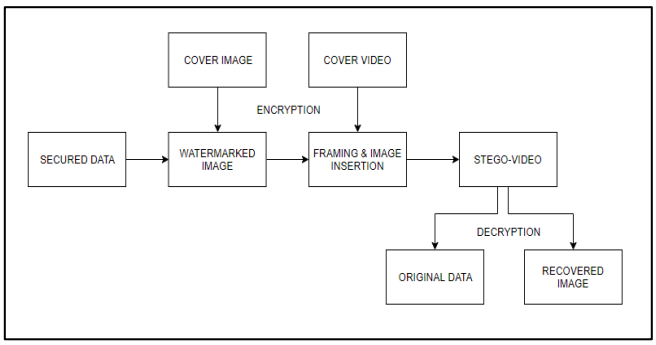

Fig 1. Block diagram of the proposed algorithm

B. Watermarking using LSB substitution

Watermarking is embedding a context of data inside another file, it can be audio, video or another text file. Here we use an image to embed the data. A standard image is taken and the LSB bits of some of the bytes of the image is changed corresponding to the message bits. The ASCII value of the data is converted to binary bits. These binary bits are inserted into the least significant bits of the standard image to form a watermarked image holding the data bits.

For example , let us consider a -bit image that are represented as bytes. A 2-grid pixel of 8-bit image is represented as:

[11000011 00101010]
[01010111 11100010]
[11010101 00010101]
[00101011 10101011]

Consider the first alphabet of the text is c, then the ASCII value of c is converted into corresponding bit as 01100011. This is inserted into the least significant bit of the standard cover image.

[1100001**0** 0010101**1**]
[0101011**1** 1110001**0**]
[1101010**0** 0001010**0**]
[0010101**1** 1010101**1**]

Since only the least significant bit value is change, it will not produce a major difference in the color of the pixel and remains the same as before. The data is hidden inside the cover image in such a manner that it is not visible to the naked and not easily cracked. This is achieved by Least Significant Bit watermarking.

C. Video framing

After the process of data hiding inside an image we move on to the next step. Video framing involves breaking the continues sequence of video into images or frames. The number of frames obtained depends upon the video size and the frame rate. Frame rate is the frequency rate at which the images appear on display. The video framing of this process involves:

ALGORITHM FOR VIDEO FRAMING:

(1)Setting up the suitable frame rate
(2)Video capturing mode is initialized
(3)Frame rate is setup

(4)Frame Id is assigned for each frame
Thus the video framing process carried out and the video is broken into individual image called frames. It is to be noted that the frame rate should be selected and coded in such a way that it does not touch 0 or produce error.

D. Video Steganography

In this scheme, the watermarked image containing the data is plunged inside a frame using LSB replacement method. Rather than encryption, watermarking or data hiding is always more advisable. Because in encryption the information is transformed in a different ways and is sent, but in steganography the information is just being hidden and ensured with highly secured communication. The quality of the information is kept unaffected through the process of transmission and reception.
In the reverse process of retrieving the original data back with high accuracy and ease involves, writing the frames into a video. The method of writing frames to video follows reading the frame from the stream. This can be done be calculating the height, width and layers of the images. Build a new frame that visualizes the required image. The image from which the data to be removed. Obtaining the least significant value we perform the reverse action and get can the original data and a distortion free cover image.

IV. EXPERIMENTAL SETUP AND RESULTS

The ensured data transmission and reception is materialized using Raspberry Pi. Raspbian is the commended operating system for the raspberry pi. The hardware demand is met by Raspberry Pi 3 embedded hardware that uses python programming language. It consists of inbuilt processor along with peripherals for connecting mouse and keyboard. The Raspbian OS to be processed is computed to a SD card and enveloped into the Raspberry Pi board. The whole initiatory construction and the code framework is shown in the fig 2.

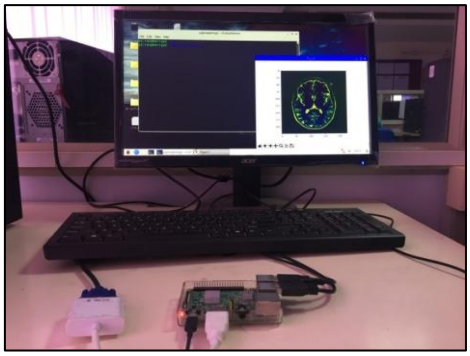

Fig 2. Experimental Setup

The parameters used to measure the performance of the system are Peak Signal to Noise Ratio(PSNR), Mean Square Error(MSE).The computational time which defines the time required for both encryption and decryption process is calculated individually. In addition it is elaborated in [10] .

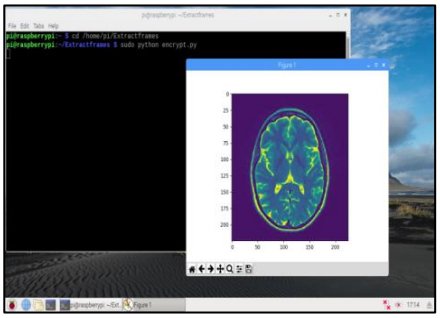

Fig 3.a. Cover Image

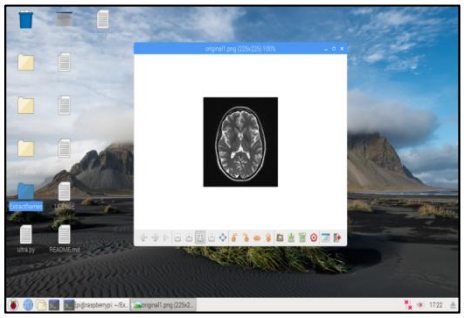

Fig 3. b. Image obtained after encryption

In fig 3.(a)Cover image is taken along with the cover video, the data is hidden inside the cover image using LSB substitution method thus the image obtained is shown in fig 3. (b). In fig 3. (c)Video framing is done and watermarked image is inserted inside a frame using least significant bit replacement. In fig 3.(d) the output image is obtained after decryption phase which is similar to the original image which is distortion less and in fig 3.(e) the original data obtained as the output of the proposed method is shown along with the performance metrics such as PSNR, MSE are calculated.

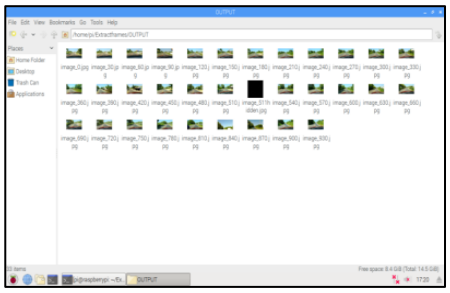

Fig 3.c. Video framing

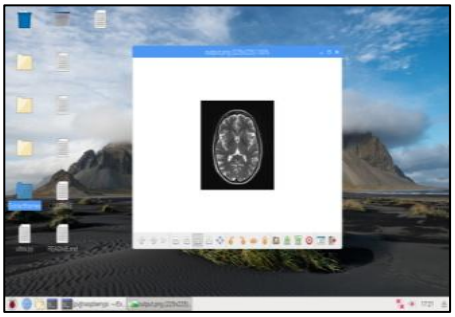

Fig.3.d. Retrieved Image

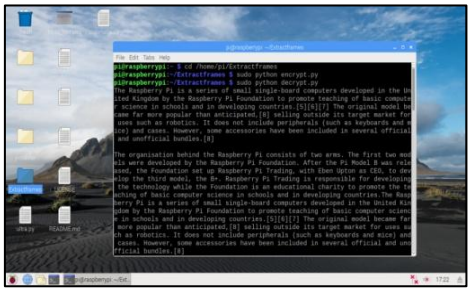

Fig.3.e. Original data

Three different criteria are taken concerning the main objectives of the proposed methodology shown in fig 4. The secured encryption and decryption process for these cases are analyzed. After the encryption phase their performance metrics are studied and tabulated. It is observed that the performance measures holds good in cases of embryo model for both encryption and decryption.

(a) (b) (c)

Fig.4. Different cover images (a) CT scan-Brain (b) Vegetables
(c) Embryo model

The efficiency of the proposed method is conceived due to the abatement of time complexity. The algorithm is more influenced and holds good results for embryo model medical image and it may even vary for other medical images as in table 1. The time taken for the decryption process is very less when compared to the encryption phase. Decryption process is carried out and the output is produced rapidly.

Table 1. Performance metrics of various test images

Test Image	Mean Square Error (MSE)	Peak Signal to Noise Ratio (PSNR) dB	CPU clock time for encryption (seconds)	CPU clock time for decryption (seconds)
CT scan - Brain	50.4	51.10	21.89	1.66
Vegetab -les	52.7	50.90	22.38	2.20
Embryo model	89.50	28.61	22.69	1.70

Reconstruction of the data and the image is very easy when correlated with other prevailing methods. It provides double protection and security with high quality data and distortion less image. The watermarked image is of same size as the output image obtained during decryption. Thus it does not require extra storage space memory and bandwidth. The power consumption for the process is very less. On visualizing the original data gained after decryption is of high quality and error free.

V. CONCLUSION

The proposed work is executed using Raspberry Pi3 embedded hardware illustrating data security with lower power consumption. Double layer protection method is introduced in which the data is hidden inside image and the image is embedded inside a video producing highly secured stego-video. It is observed that the proposed scheme holds good outcome for real time medical image i.e. embryo model, the computational time (CPU clock time) required for execution of this image is less compared to other cases. The visual appearance of the image after embedding data remains unaltered. The quality of the stego-video is same as the cover video. Additional bandwidth for transmission and storage space is not required. In future, this work can further be extended to reinforce the security of the algorithm. Therefore conclusion is made analyzing different performance metrics based on real time circumstances. This implementation may serve as a platform for the future enhancement in the field of developing a secured data transmission irrespective of the ambiguity attacks.

ACKNOWLEDGMENT

The authors are grateful to the Department of Science & Technology, New Delhi, India (SR/FST/ETI-371/2014). They also wish to acknowledge SASTRA University, Thanjavur, India for extending the infrastructural support to accomplish this work.

REFERENCES

1. MrithaRamalingam, Nor Ahidi Mat Isa, "A data hiding technique using scene-change detection for video steganography", Computers and Electrical Engineering,pp1-12,2015.
2. Mahdi Hashemzadeh, "Hiding information in videos using motion clues of feature points", Computers and Electrical Engineering, Vol 68 pp 14-25, 2018.
3. Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Transaction on Information Forensics and Security, Vol 7 No.2, pp 826-833.
4. Yunxia Liu, Shuyang Liu, Yonghao Wang and Hongguo Zhao, Si Liu (2019) Video Steganography", Neurocomputing, 335, 238-250.
5. Rupali Bhradwaj, Vaishali Sharama, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution ", Procedia Computer Science 93, 832-838., 2016.
6. Poonam, Shafali M. Arora, (2018) A DWT-SVD based robust Digital Watermarking for Digital Images, Procedia Computer Science, 251, 1441-1448.
7. Dawen Xu, Rangding Wang (2016) Separable and error-free reversible data hiding in encrypted image, Signal Processing, 123, 9-21.
8. Rakesh Mehta, Jaume Amores (2018) Improving detection speed in video by exploiting frame correlation, Pattern Recognition Letters, 112, 303-309.
9. Ayhan Yilmaz, A. Aydin Alatan, (2008) Error detection and concealment for video transmission using information hiding, 23, 298-312.
10. Wien Hong, Tung-Shou Chen and Han-Yan Wu (2012) An improved Reversible Data Hiding in Encrypted Images Using Side Match, Signal processing,,19, 199-202,
11. Soumitra Roy, Arup Kumar Pal, (2012) A blind DCT based color watermarking algorithm for embedding multiple watermarks, Signal processing, 19, 199-202.
12. GuruPrasad .K.Basavaraju, "Introduction to Raspberry Pi with Raspbian OS" in
13. https://www.codeproject.com/Articles/839230/Introduction-to-Raspberry-Pi-with-Raspbian-OS.

14. Image fusion using approximation and detail, http://shodhganga.inflibnet.ac.in/bitstream/10603/20682/13/13_chapter%204.pdf

AUTHORS PROFILE

T.R.Kowshika is currently pursuing Masters of Technology at SASTRA University, Thanjavur, India. Her research interests are in the areas of Image Processing, Embedded Systems, Internet of Things.

Dr.K.Geetha received the PhD degree in NIT, Trichy. She is a Senior Assistant Professor from Sastra university. Her research interests are in Multicore Computing, Computer Architecture, High Performance Computing, Web Caching, Network Security.