IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN APPROACH FOR DUAL SECURITY FOR DATA TRANSMISSION USING IMAGE-VIDEO SECRET WRITING TECHNIQUE

[1]ROUSHA, [2]SHAIFA SHALA [3]SHILPA

[1]Student, [2]Student, [3]Assistant Professor

[1,2,3] Department of Computer Science and Engineering

[1,2,3] Alva's Institute of Engineering and Technology, Moodbidri, India

Abstract: Secret writing is any means of written communication where by a spy conceals the actual written text, whether it is encoded or not. Though different carrier file formats can be used, but digital images are more popular because of their frequency on the internet. For the hiding of secret information in images, there exists various techniques of secret writing in which some are complex than others but all of them have strong and weak points. Here this paper intends the requirements of a good secret writing algorithms and gives the brief information about the secret writing techniques which are more suitable for the specific applications.

***Index Terms* – Secret writing, Encryption, Decryption, LSB, Text, Stego picture, Stego video.**

I. INTRODUCTION

Secret writing conceals the restricted information in another file so that solitary the beneficiary knows the presence of message. In old time, the information was secured by concealing it on the rear of wax, composing tables, stomach of bunnies or on the scalp of the slaves. In any case, the present the vast majority of individuals communicate the information as text, pictures, video, and sound over the medium. To securely transmission of confidential information, the sight and sound item like sound, video, pictures are utilized as a cover source to shroud the information.

Secret writing is defined as the investigation of imperceptible correspondence. It generally manages the methods of concealing the presence of the conveyed information so that it remains confidential. It keeps up with mystery between two conveying parties. In picture secret composition, mystery is accomplished by inserting information into cover picture and creating a stego-picture and further installing a stego-picture into cover video and producing a stego-video.

There are different kinds of mystery composing procedures each have their qualities and shortcomings. In this paper, we will carry out the twofold security by concealing the content inside a picture and further, this picture will be covered up inside a video

II. PROBLEM STATEMENT

To communicate something specific subtly to the objective, Secret composing strategy is utilized, data can be stowed away in transporters like pictures, sound documents, text records, recordings and information transmissions. In this venture, we proposed another structure of a picture video secret composing procedure, where first we are attempting to shroud an advanced book of a mysterious message inside a picture and this picture is covered up under a video.

The current framework has a few disadvantages, for example, the mysterious message might be lost or hacked by the outsider. Since in the current framework, Image and video secret composing is executed independently which gives the single level protection or security to the information.

III. LITERATURE SURVEY

There are quantities of steganography procedures accessible that utilization computerized picture/video as transporter. In [7] different steganography strategies and grouping of picture steganography approaches dependent on sort of host object, area type and record design has been present and presumed that the uncompressed document format(bmp.gif) based on lossless pressure gives high information limit and more helpful for information concealing calculation. N.provos and Honeyman [9] characterize the fundamental destinations for any steganography calculation like limit, undetectability and vigor. Most LSB based procedures were proposed trying to upgrade its altered opposition.

A Madhusudhan, Kota and Haripal Reddy et al [1] proposed a condition of workmanship mix work of two conspicuous information security draws near, in particular cryptography and steganography. Both of the techniques give security for restricted data yet independently one can't guarantee for preeminent security of data. Consequently, to give more noteworthy security to the information at the period of correspondence over unbound channel a novel advancement strategy for data security is required.

Ankit Chadha et al (2013) zeroed in on further developing the information encryption in a wide range of sight and sound information arrangement to make covered up message imperceptible. To give greater security to the data at the hour of correspondence over unstable channel a novel development method for information security is required

Jigar Makwana, S.G Chudasama et al (2016) have introduced a best in class mix work of two mainstream data security draws near, in particular cryptography and steganography. Anyway, both of methods give security to discharge data at the hour of correspondence over unstable channel a novel development procedure for information security is required.

Budda Lavanya et al (2013) have portrayed a steganography-based technique for installing printed data in a sound document. In the current steganography strategy, at first the sound record is examined and afterward a fitting piece of each substitute example is changed to embed the printed data. Interestingly, in the proposed procedure, the restricted information is first hided into the picture which is then installed into the sound. In experiments, to imagine in what degree the objective has been accomplished, the content-based information has been effectively implanted to the sound record for additional examination.

Harvinder Singh et al (2013) have portrayed a news steganography that conceals the mysterious message dependent on the quest for the indistinguishable pieces between the mysterious messages and picture pixel esteems. The proposed strategy is contrasted and the LSB benchmarking technique. The consequences of the proposed and LSB concealing strategies are talked about and broke down dependent on the proportion between the quantity of the indistinguishable and the non-indistinguishable pieces between the pixel shading esteems and the mysterious message esteems. A methodology is taken to produce a cross-stage which can viably shroud a message inside a computerized picture.[8] As an image is the blend of a couple of pixels and each pixel has three concealing numbers which consequently achieves a reality that an image involves a large number of numbers, the change a few concealing numbers makes the picture look an extraordinary arrangement favors the main picture.

IV. EXISTING SYSTEM

The existing system consists of the image and video secret writing implemented separately. In image secret writing, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to know which pixels he or she must select to extract the message.

Video Secret Writing is a technique to hide any kind of files into a cover Video file. The use of the video-based secret writing can be more secure than other multimedia files because of its size and complexity.

Drawbacks of existing system:

The existing system has several drawbacks such as the secret message may be lost or hacked by the third party. Because in the existing system, Image and video secret writing is implemented separately which gives the single level privacy or security to the data

V. PROPOSED SYSTEM

The main proposed system has the concept of dual secret writing for secure communication. In dual secret writing, Image secret writing technique is utilized inside a Video secret writing. Here we are giving a double security for the data to be sent to a receiver.

VI. METHODOLOGY.

6.1. DEVELOPMENT ENVIRONMENT:

Google Colab

6.2. IMPLEMENTATION:

The way toward installing information in host record is appeared in below figure. The secret data has been embedded inside spread image with the help of 4-bit LSB (Least significant bit) algorithm along with the stego-key. The key utilized is limit of 10-bit length Key is embedded in the spread image during the LSB inserting process. This should be known at the receiver side amid the capture procedure for recovering the secret record.

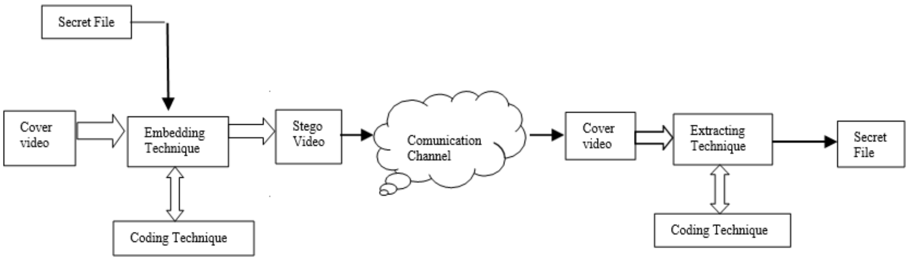

Image Secret Writing:

• Cover picture is isolated into RGB Planes.

• Secret information taken is then changed over into paired structure.

• Those qualities are isolated into upper and lower snack which are inserted in two separate planes of the cover picture.

• Upper snack is installed in green plane and lower snack in red plane utilizing 4 cycle LSB Method.

• Stego Key is installed inside the blue plane.

• After which, every one of the three planes are consolidated to create stego-picture.

Video Secret Writing:

• Input the cover video transfer.

• Convert the video arrangement into various edges.

• Split each edge into the YUV shading space.

• Apply the two-dimensional DWT twice independently to every Y outline segments.

• Embed the message(stego-picture) into the center recurrence coefficients (LH,HL) of every one of the Y parts.

• Rebuild the stego outlines from the YUV stego parts.

• Output the stego recordings, which are reproduced from all implanted edges

VII RESULTS:

The sample output showing below is the encrypted image inside which text is hidden.

Figure 7.1

The following is the video inside which the encrypted image is hidden which provide the double security

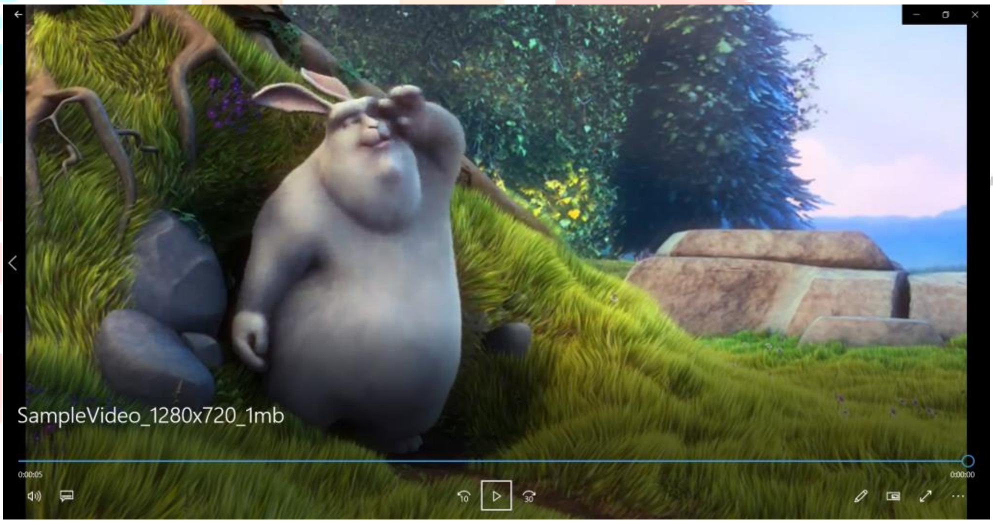

Figure 7.2

Figure 7.1 and 7.2 shows the sample outputs

VIII. CONCLUSION:

In this paper, it is seen that through LSB Substitution Steganographic strategy, the outcomes got in information covering up are quite noteworthy as it uses the straightforward reality that any picture could be separated to singular piece planes each comprising of different levels of data. It is to be noticed that as talked about before, this strategy is just effective for bitmap pictures as these include lossless pressure procedures. In any case, this cycle can likewise be reached out to be utilized for shading pictures where, bit plane cutting is to be done independently for the best four-bit planes for every one of R, G, B of the message picture. Examine that however steganography was once undetected, with the different strategies presently utilized, it's difficult simple to identify the presence yet in addition recovering them is simpler. For example, without utilizing a product or complex devices for discovery, straightforward techniques to notice if a picture file has been controlled are: 1. Size of the picture: A Steganographic picture has a gigantic stockpiling size when contrasted with a customary picture of similar measurements. For example, in the event that the first picture stockpiling size would be not many KBs, the Steganographic picture could be a few MBs in size. This again differs with the goal and kind of picture utilized. 2. Commotion in picture: A Steganographic picture has clamor when contrasted with a customary picture. This is the motivation behind why at first little clamor is added to the cover picture, so the Steganographic picture doesn't show up extremely boisterous when contrasted with the first cover picture..

REFERENCES

[1] A Madhusudhan, Kota, Haripal Reddy , "Dual Steganography For Hiding Technique In Video",International Journal of Research in Advent Technology,Vol.7,No.4S,April 2019.

[2] Mennatallah M. Sadek & Amal S. Khalifa & Mostafa G. M. Mostafa. "Video steganography: a comprehensive review" DOI 10.1007/s11042- 0141952-z Springer Science New York 2014.

[3] 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).

[4] 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.

[5] 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.

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

[7] Harvinder Singh, Anuj kumar et al(2013), 'Analysis and Implementation of Algorithm to Hide Secret Message', International Journal of Advanced Research in Computer Science and Software Engineering

[8]Hussein Al-Bahadili (2013),' A Secure Block Permutation Image Steganography Algorithm',International Journal on Cryptography and Information Security (IJCIS), Vol.3

[9] N. Provos and P. Honeyman, "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003