Secure Algorithm for Embedding Encrypted Data with video as Carrier

[1] Himanshu Singh,[2] Dr. Pramod Sharma

[1]M.Tech Research Scholar,[2] Professor
[1,2] Department of Electronics and Communication Engineering,
Regional College for Education Research and Technology, Jaipur.

Abstract : The proposed framework gives the legitimate validation technique by giving the special idea of utilizing the scrambled pictures as secret key. Along with that the proposed framework offers the exchange of the information which is totally covered up in their separate transporters. The idea of the encoded dynamic and variable length keys or secret phrase is utilized in others with the LSB procedure in the sound and video as the transporter documents and the outcomes which are accomplished in the process are very productive and palatable.

***IndexTerms* – Steganography , Image Steganography, Video Steganography.**

I. INTRODUCTION

Steganography is the act of hiding a record, message, picture, or video inside another document, message, picture, or video. It has existed for quite a while, and these days, computerized steganography is utilized to shroud information inside pictures. We can shroud a wide range of information by utilizing diverse advanced steganographic strategies. An advanced picture is a portrayal of pixel esteems, and each pixel worth will have numbers containing data with respect to the pixel. A computerized shading picture will have red, green, and blue channels and eight pieces to speak to each channel, so every channel can take an incentive from 0-255, and this worth speaks to the force of the pixel. (R, G, B)=(0,0,0) is the portrayal of the shading dark and (255,255,255) speaks to the shading white.[1]

Accept a variety of pixels for instance and assume we need to conceal the character An in it. We should perceive how it's done:[2]

```
(R, G, B)= (11101010 11101001 11001010),(10111001,11001011,11101000),
(11001001 00100100 11101001)
```

Fig 1. Image Array

This is a pixel cluster, and we need to conceal An in it. The ASCII estimation of An is 65. On the off chance that we convert it to double, we get 01000001. So on the off chance that we use LSB change, we can change the LSB of the multitude of numbers in our cluster and get:[3]

```
(R,G, B)= (11101010 11101001 11001010),(10111000,11001010,11101000),
(11001000 00100101 11101001)
```

Fig 2. Image Array Containing Data

A video is an assortment of edges, and each edge is a picture. So in the event that we pull out all the edges from a video, we can utilize this strategy to store our information utilizing LSB steganography and join those casings back into a video with the mystery message. [4] Video steganography is a designing term characterize as concealing the mystery rub in cover mixed media record like video document, picture record. Steganography additionally recognized is the ability and learning of composing word which is need to be hole up behind picked one as a cover interactive media document like sound, video or picture The principle work of in this examination builds the limit in video information stowing away inside DWT method. Video are ideal for data stowing away on account of the measure of territory is created in the putting away of recordings. The idea raised the need of video steganography in all field like as e-paying, e-promoting , individual or public security information, and money just as the individual correspondence reports. [5]

II. LITERATURE REVIEW

Mohit Sharma ,2016 [6] In this maker have imagined the thought where they can trade the picture or text beginning with one customer then onto the following. For the circumstance they can first login as sender where we can send the message which should be text or a picture containing the covered content. By then they can in like manner login as a beneficiary which can get to the messages ship off the individual being referred to , where the instant messages are seen clearly and the pictures contained the covered content need to be decoded by the customer.

Ammad Ul Islam et. al 2016 [7] The quick imaginative headway of the data correspondence in the current day time demands the protected feeling of exchange of data. Steganography is a set up methodology for hiding data from an unapproved get to. Steganographic techniques cover secret data in different record designs, for instance, the picture, the content, the sound, and furthermore the video. Impalpability, payload cutoff, and security with respect to PSNR and life are the vital troubles to steganography. In this paper, a novel idea of the picture stegnography strategy which depends on the most basic pieces (MSB) of the picture pixels was proposed.

Imran Sarwar Bajwa and Rubata Riasat 2011[8] Image stegnography is a rising field of exploration for secure data stowing ceaselessly for data transmission over web, copyright protection, and ownership recognizing evidence. A couple of frameworks have been proposed for concealing picture stegnography. Nevertheless, the concealing pictures are generally the more excessive to send on web due to their size. In this paper, creators propose another ideal hashing based procedure for stegnography in dull scale pictures...

III. CRYPTOGRAPHY AND STEGANOGRAPHY

We have proposed a verified File sharing and the message moving framework in which the message denunciation is done just between the enrolled clients. The module of the frameworks is partitioned into the accompanying parts.

1. Registration:

- To get deeply framework, client first need to enlist themselves by giving required subtleties.

2. Login:

- After enlistment, client may login into the framework.

3. Algorithm Selection:

- Here, client will choose the calculation, for example, DES (Data Encryption Standard), AES (Advance Encryption Standard) or LSB (Least Significant Bit) for encoding information into image document.

4. Image Selection/Audio Selection

- Here, User chooses an image/audio for sending a mystery message. For some situation where the scrambled image is sent then the stage 5-6 are skipped and another progression of decoding of the image will be presented.

5. Entering Text:

- Here, User enter/inputs the text that will be covered up in the image.

6. Setting Password and Encrypting the Data:

- User sets a secret phrase and utilize the encryption method to encode the information.

7. Sharing:

- After concealing the text with the encryption method, client spares the image a then sends it to the next gathering for example Collector.

IV. IMPLEMENTATION AND RESULT ANALYSIS

The implementation is done in VS 2010 and perform is three concepts,

4.1 Encrypted Image Password

Fig 3. Encrypted Image Password

4.2 Audio as Carrier for Hidden Data

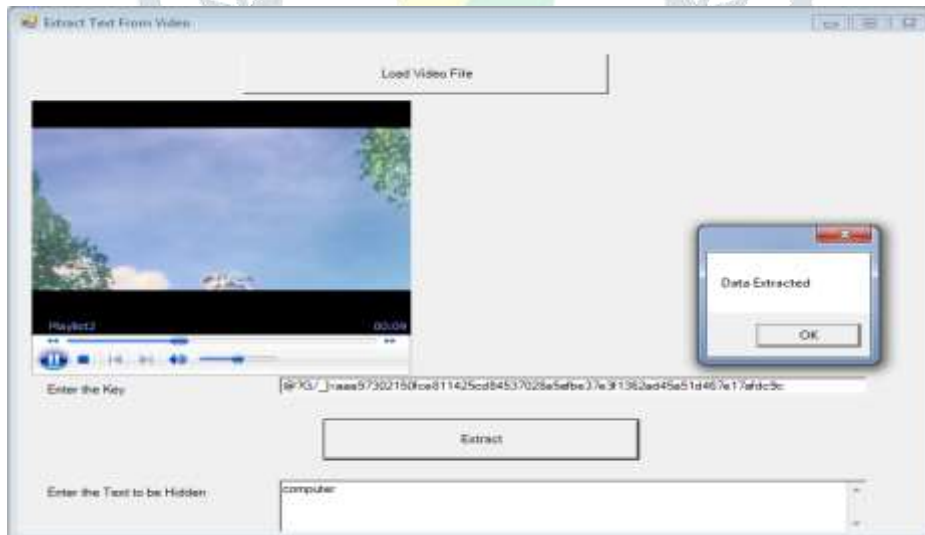

Fig 4. Audio as Carrier

4.3 Video as Carrier

Fig 5. Video as Carrier

TABLE 1. RESULT COMPARISON

Tools Used	Base Result	Proposed Work Result
The Password Meter	78%	100%
Password Checker Online	50%	100%
Rumkin.com	Entropy 37.7 bits	Entropy 306.6 bits

V. CONCLUSION

In the end, it is indicated that the proposed work will ready to achieve the better security level, and the general idea which is proposed in the framework created, gives the idea of the extraordinary method of legitimacy the clients utilizing the encoded picture as the secret phrase as it expands the unconventionality as the information base of the clients will store the scrambled pictures, in this way it will be difficult for the programmers to abuse the subtleties which are put away in the client information base. The second period of the proposed execution centers around the sound stegnography in which the client can conceal the information in the sound and the got sound will likewise be the basic sound which can utilized like the ordinary sound. Along with the variable key which is utilized for the encryption cycle will likewise builds the flightiness and furthermore further improves the security level. In the last, the proposed work center around the video stegnography utilizing the content concealing cycle, utilizing the variable length dynamic arbitrary keys and furthermore the cycle of the hash based approval at the beneficiary finish to confirm the credibility of the video and the content which is implanted in the video.

REFERENCES

1. Neha Rani and Jyoti Chaudhary, "Text Steganography Techniques: A Review", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- july 2013

2. Swati Gupta and Deepti Gupta, "Text -Steganography: Review Study & Comparative Analysis", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011

3. Chintan Dhanani and Krunal Panchal, "Steganography using web documents as a carrier: A Survey", International Journal of Engineering Development and Research (IJEDR), ISSN: 2321-9939, 2013

4. S. Low, N.Maxemchuk, J.Brassil, L. O'Gorman, 1995. "Document marking and identification using both line and word shifting", Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 95.

5. Krista Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text", CERIAS Tech Report 2004-13.

6. Mohit Sharma," Secure Message Transfer using Image Steganography", Imperial Journal of Interdisciplinary Research (IJIR) 2016.

7. Ammad Ul Islam ; Faiza Khalid ; Mohsin Shah ; Zakir Khan ; "An improved image steganography technique based on MSB using bit differencing",IEEE,2016.

8. Imran Sarwar Bajwa ; Rubata Riasat,"A new perfect hashing based approach for secure stegnograph",IEEE,2011.

9. Beenish Mehboob ; Rashid Aziz Faruqui , "A stegnography implementation",IEEE,2008

10. Shaikh Shakeela, P. Arulmozhivarman, Rohit Chudiwal, Samadrita Pal,"Double Coding Mechanism for Robust Audio Data Hiding in Videos",International Conference On Recent Trends In Electronics Information Communication Technology, 2016

11. Priyanka Sahute, Swati Waghamare, Supriya Patil,Ashwini Diwate,"Secure Messaging Using Image Stegnography",International Journal of Modern Trends in Engineering and Research.2015

12. Pooja,Sandeep Toshniwal,"A QR Code Based Highly Secure Covert Communication",IEEE,2017

13. Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan , Toqeer Mahmood, Adnan Khan, Usman Ali, Muhammad Naeem,"An Improved Image Steganography Technique based on MSB using Bit Differencing " IEEE,2016.

14. K. Rajalakshmi and K. Mahesh, "Video steganography based on embedding the video using PCF technique," 2017 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2017, pp. 1-.4.