ADVANCED TECHNIQUE FOR ENCRYPTED IMAGE PASSWORD AND VIDEO STEGANOGRAPHY

[1] Avinash Sharma, [2] Prashant Kumar Singh
[1] MTech. Scholar, [2] Assistant Professor
[1]Name of Department of 1st Author,
[1,2] Department of Digital Communication, Jaipur Institute of Technology Group of Institutions ,,Jaipur,Rajasthan ,India

Abstract : Security of data is the major issues in each of the organization . The concept of the Steganography , that is hiding of the data in the carrier helps a lot in the process of securely transferring the data. Together with that proper authentication of the user is also a main concern. The proposed algorithm works in the enhancing the security by applying the encrypted images as passwords and the video based Steganography for the secure data transfer.

***Index Terms* - Data Security, Steganography,Video Steganography.**

I. Introduction

Security has faithfully been a big a neighborhood of human. we have a tendency to tend to area unit encompassed by a universe of secure communication, where folks of assorted kinds area unit transmitting data like mastercard selection to an internet store than and as wily as a terrorist plot to hijackers. The ways that build secure communication practicable are not new. There has faithfully been a demand of securing the messages that unit of measurement sensitive in nature. Such messages if given to some of intruders would possibly represent a risk to country's security or organization's basic selections. Therefore, such data ought to be secured at any expense and to fill the need to cipher or hide the data. Cryptography (derived from Greek work 'kryptos' which suggests hidden and 'graphein' assuming to write) [1] is used to code the content to create it intelligible. Cryptography would possibly draw the suspicion of the entrant or third party towards the content that is in encoded. Steganography is that the attainment and exploration of composing hid messages in such however that no-one, aside from the senderand expected beneficiary, suspects the presence of the message, a kind of security whereas not data of its presence. The word Steganography is of Greek origin and suggests that "concealed writing" from the Greek words steganos (στεγανός) which suggests "covered or protected", and graphein (γράφειν) which suggests "to write" [2]. Steganography are classified supported the kind of media it utilizes to hide the data.

Text Steganography: It conceals the text behind another document. it's toughest form of steganography as a result of the repetitive live of text to hide the key message is rare in text files.
Image Steganography: this type hides text or an image inside another text. it is the foremost oftentimes used strategy as a result of the restriction of the Human Eye.
Audio Steganography: Audio Steganography is also a way used to transmit hidden data by adjusting a sound check in Associate in Nursing undetectable means that. it is the science of concealing some secret text or audio data throughout a number message [3]. The host message before applying steganography and stego message once steganography have constant attributes.
Video Steganography: Video Steganography is that the procedure of concealing some secret data inside a video. The enlargement of this data to the video is not conspicuous by the human eye as a result of the modification of a constituent color is negligible [3]..

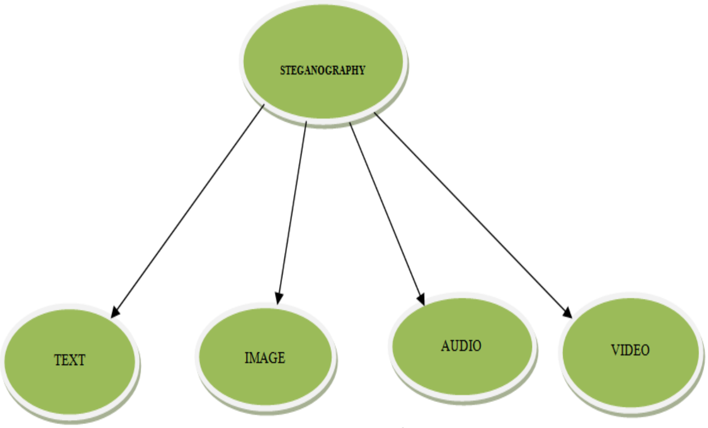


Fig 1. Steganography Types

II. Video Steganography

In video steganography, secret knowledge is embedded in cowl video. A basic model of video steganography is shown in Fig. 2. During this section, some vital techniques of video steganography area unit mentioned in short. one among the best and customary strategies is Least vital Bit (LSB) technique. during this methodology, LSB of canopy video is replaced by secret knowledge [4]. however this system of concealing the key knowledge isn't a lot of effective because the knowledge could lose when some file transformations [4] and [5]. a replacement methodology supported distinct trigonometric function rework (DCT) transformation has been introduced [5]. the most focus of this paper is to extend the capability to cover the key knowledge.

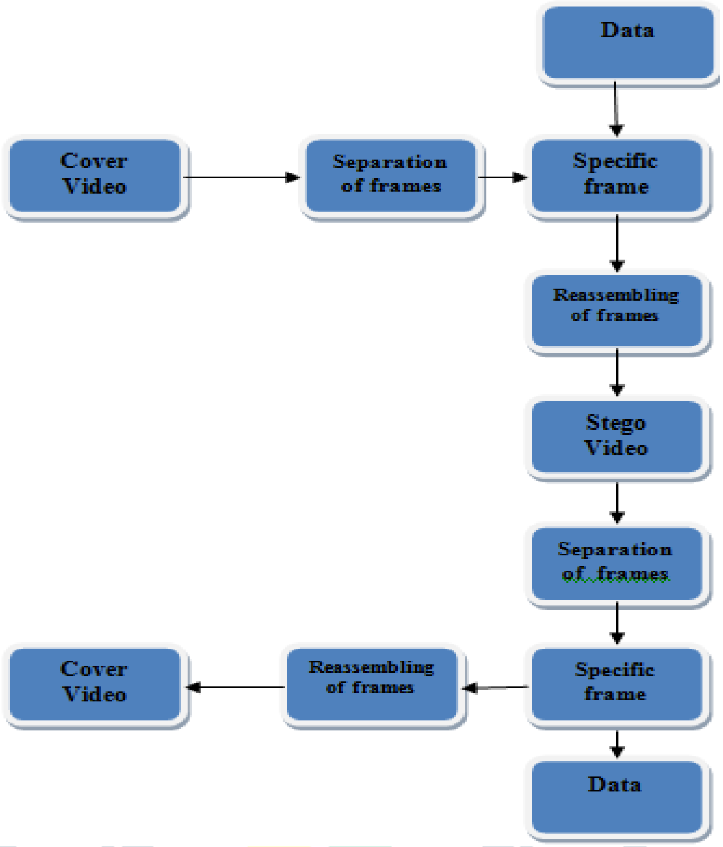


Fig 2. Video Steganographic Model

III. Related Work

Mohit Sharma [6] during this author have devised the idea wherever they will transfer the image or text from one user to a different. within the case they will 1st login as sender wherever we will send the message which might solely be text or a picture containing the hidden text.

Then they will conjointly login as a receiver which might access the messages send to him or her , wherever the text messages area unit viewed directly and therefore the pictures contained the hidden text need to be decrypted by the user.

Ammad Ul Islam [7] The speedy development of knowledge communication in era demands secure exchange of knowledge. Steganography is a longtime methodology for concealing knowledge from associate degree unauthorised access. Steganographic techniques hide secret knowledge in several file formats such as: image, text, audio, and video. physical property, payload capability, and security in terms of PSNR and hardiness area unit the key challenges to steganography. during this paper, a unique image Steganography technique supported most vital bits (MSB) of image pixels is projected. Bit No. five is employed to store the key bits supported the distinction of bit No. five and vi of canopy image. If the distinction of bit No. five and vi is completely different from secret knowledge bit then the worth of bit No. five is modified. The results state that the projected technique ensures vital enhancements in signal to noise magnitude relation. Usually, the hackers target LSB bits for secret knowledge extraction however the projected technique utilizes the mutual savings bank bits that build it safer from unauthorized access. moreover, the conferred technique isn't solely secure, however computationally economical further.

Imran Sarwar Bajwa[8] Image Steganography is associate degree rising field of analysis for secure knowledge concealing for knowledge transmission over web, copyright protection, and possession identification. a handful of techniques are projected for color image Steganography. However, the color pictures area unit additional expensive to transmit on web because of their size. during this paper, we have a tendency to propose a replacement excellent hashing primarily based approach for Steganography in grey-scale pictures. The projected approach is additional economical and effective that gives a safer means of knowledge transmission at higher speed. The conferred approach is enforced into a model tool coded in VB.NET. The conferred approach is effective in an exceedingly means that multiple file formats like bmp, gif, jpeg, and run-in are supported. a collection of sample pictures were processed with the tool {and the|and therefore the|and conjointly the} results of the initial experiments indicate the potential of the conferred approach not solely in terms of secure Steganography however also in terms of quick knowledge transmission over web.

Beenish Mehboob [9] several techniques area unit accustomed hide knowledge in varied formats in steganography. the foremost wide used mechanism on account of its simplicity is that the use of the smallest amount vital Bit. Least vital Bit or its variants area unit unremarkably accustomed hide knowledge in an exceedingly digital image. the opposite bits could also be used however it's extremely possible that image would be distorted. This paper discusses the art and science of Steganography normally and proposes a unique technique to cover knowledge in an exceedingly colourful image mistreatment least vital bit..

IV. Proposed Work

4.1 Algorithm for Embedding Text in Audio

1. Input the Audio File
2. Input the document or Text to be Hidden
3. Input the Key File Used for the cryptography Purpose (Same Key file are going to be used for cryptography purpose)

4. Within the Embedded method 1st the chunk of wave stream of the audio files area unit obtained so as to count the quantity of samples needed for embedding the info , if the samples obtained isn't comfortable then the error message is generated. Then the supply audio stream and destination audio stream area unit opened (destination audio is that the new audio file that get created when the embedding process). Then the message and key area unit embedded bit by bit with the carrier audio.
5. Finally we will get the audio with hidden knowledge

4.2 Algorithm for Extracting of Data from Audio:

1. Input the Audio File
2. Input the document which is able to store the extracted knowledge.
3. Input the Key File Used for the cryptography Purpose (Same Key file are going to be used for cryptography purpose)
4. 1st the radio wave file is extracted for the provided audio file, the message is extracted from the audio file mistreatment the key file that is provided as input then a replacement file stream is obtained so as to put in writing the extracted knowledge into the new destination file.
5. Finally this knowledge regenerate into original secrete knowledge

4.3 Algorithm for Hiding Text Video

```
Step 1: Read the Video.
Step 2: Read the Text.
Step 3: Set N:=NumberofFrames.
Step 4: Repeat for I: 1 to N
Step 5: Set Frame(i) := Extract Ith frame image
Step 6 : Save Frame(i) as Frame-(i).tiff [e.g. 1st image as Frame-(1).tiff, 2nd as Frame(2).tiff]
    [End of for Loop]
Step 7: Repeat for I: 1 to N
Step 8: Convert the Frame-(i).tiff to Binary
Step 9: Convert the text to binary
Step 10: Repeat for I:1 to M [Text Length]
Step 11: Combine Data with the Pixel of Image
[End of Loop]
Step 12: Rewrite the New Image Frame-(i)E.tiff
    [End of Out for Loop]
Step 13:  Repeat for I: 1 to N
Step 14: Combine to for the New video
    [End of for loop]
Step 15: Save the new video
Step 16: Generate SHA of Text Embedded and combine with Key..
```

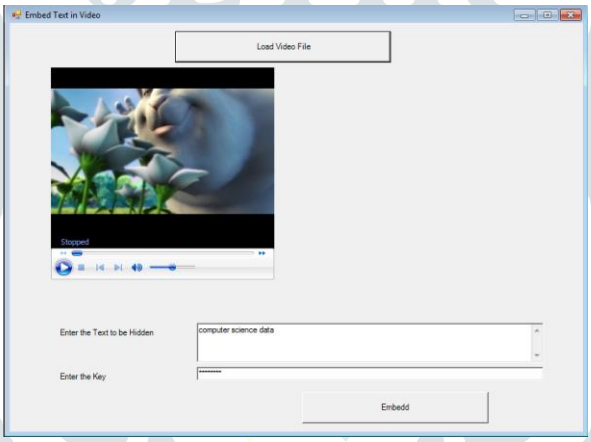
4.4 Algorithm for Extracting Text Video

```
Step 1: Read the Video,Key
Step 2:  Set N:=NumberofFrames.
Step 4: Repeat for I: 1 to N
Step 5: Set Frame(i) := Extract Ith frame image
Step 6 : Save Frame(i) as Frame-(i).tiff [e.g. 1st image as Frame-(1).tiff, 2nd as Frame(2).tiff]
    [End of for Loop]
Step 7: Repeat for I: 1 to N
Step 8: Convert the Frame-(i).tiff to Binary
Step 9: Repeat I : 1 to Size of Image.
Step 10: Extract the Pixel
Step 11: Convert the decimal value of pixel to binary
Step 12: Extract the Character Bits
Step 13: Convert to Character and combine to the resultant data
```

```
 Step 14: Combine Data with the Pixel of Image
 [End of Loop]
 Step 15: Rewrite the New Image Frame-(i)E.tif
 Step 16: Display the text extracted
     [End of Out for Loop]
 Step 17:  Repeat for I: 1 to N
 Step 18: Combine to for the new video
     [End of for loop]
 Step 19:Extract the SHA for Key part.
 Step 20: Generate SHA from text extracted.
 Step 21: If both same then:
             Save the new video.
         Else
             Generate Error
       [End of If structure]
Step 22: Stop
```

V. IMPLEMENTATION

The projected algorithmic program is dead in Visual Studio 2010 and SQL Server specific Edition 2008.To run the higher than programming the specified instrumentality are X86 processor one gigacycle or a lot of a minimum of one GB of RAM.
Presently the half takes once with clarification of execution of algorithmic program with the help of screenshots of my work I even have taken amid my viable work..

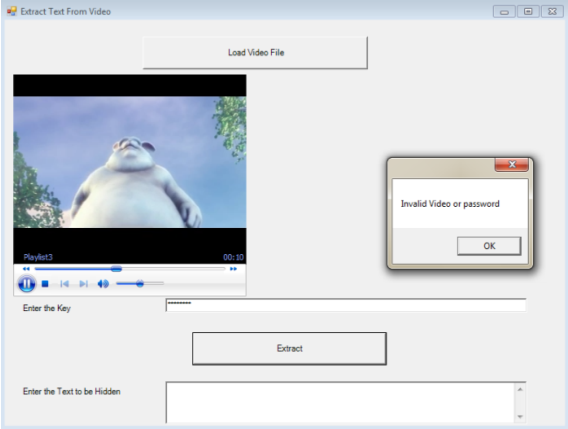


Enter the Text to be Hidden computer science data

Enter the Key ********

Fig 3 Embedding in Sample.mp4

In the fig 3 , the sample.mp is taken as the carrier and text which to be hidden "computer science data", and the password for embedding is abc123



Invalid Video or password

Enter the Key ********

Enter the Text to be Hidden

Fig 4 Extracting data from sample.mp4

The fig 4 shows that the sample.mp4 is provided as an input with the password 1234abcd and the invalid details are detected.

VI. CONCLUSION

In this knowledge is embedded with the image and sent over the network wherever its integrity is verified by the comparison of hash price of the initial knowledge or image. The audio/video steganography is additionally enforced, wherever the audio/video message will firmly carry the text. The planned work provides secure secret communication among sender and receiver, conjointly ensures the credibility of the user victimisation the encrypted image as countersign. it's helpful for copyright possession assertion functions. the info that is hidden can not be simply removed and resist common image manipulation techniques. The effectiveness and potency of the planned system may be improved and increased within the approach of capability, Security and strength.

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 Steganography implementation",IEEE,2008

[10] Mrs. Kalavathi.Alla, Dr. R. Siva Ram Prasad, “A Novel hindi Text Steganography using Letter Diacritics and its compound words”,2008.

[11] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998.

[12] S.B. Sadkhan., “Cryptography: Current status and future trends”, in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.

[13] T Mrkel,JHP Eloff and MS Olivier .”An Overview of Image Steganography,”in proceedings of the fifth annual Information Security South Africa Conference, 2005

[14] Chan, C.K., Chang, L.M., “Hiding data in image by simple LSB substitution”, Pattern Recognition, vol 37, pp.469-471, 2003.

[15] Da-Chun Wu, Wen-Hsiang Tsai, “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters 24 (2003) 1613–1626.

.