1) ABSTRACT

A long-established practise is steganography. In the past, government and military communications were the main uses of steganography techniques. However, a wide range of uses for these techniques are common. Yet, scholars provide and uncover a number of ways to enhance steganographic applications, while others enhance steganographic approaches and procedures.

The steganography tool for exchanging confidential communications currently employs multimedia files as a cover carrier for the secret message because there are so many possible methods to convey the secret message utilising various types of covers. With a video file acting as the cover carrier, this project will employ steganography techniques to accomplish its objectives. In order to protect information, the art of steganography involves hiding data on a material carrier. Video-based steganography is possible with a single video file.

More often than other multimedia forms, video-based steganography may be used. There have been several benefits suggested for employing a video file as a cover carrier for steganography. In this project, the data is protected from prying eyes using steganography and encryption. The primary distinction between them is that without encryption, anyone can see that both parties are privately speaking with one another. It is possible to hide a message using steganography.

2) INTRODUCTION

Steganography is a word that means "covered or hidden writing" and is derived from Greek. Thousands of years have passed since the invention of steganography. It uses a clandestine transmission technique called data concealing. In digital images, audio, and video, steganography is a method for concealing sensitive information from prying eyes. The power of steganography lies in its ability to subtly conceal the presence of sensitive data within a public carrier file.

Steganography differs from cryptography in this regard because cryptography encrypts the secret information while leaving it susceptible to being decoded by unauthorised parties. Numerous scenarios, including industrial and military ones, utilise steganography. Lossless steganography techniques are employed to successfully and securely convey data between sender and receiver. With steganography, secret messages in digital image files are often covered up.

Steganographic methods have recently piqued the interest of computer programmers who want to use them on audio and video files. Steganographic systems are currently utilising multimedia artefacts like photographs, audio, and videos as cover media due to the prominence of sending digital photos over email and other forms of Internet communication. The picture file formats are JPEG, GIF, and BMP; the audio and video file types are WAV, MP3, MPEG, MP4, and AVI.

3) LITERATURE REVIEW

The challenge, according to A. Sarkar, U. Madhow, S. Chandrasekaran, and B. S. Manjunath [1], is to develop a steganographic technique that can hide a sizable amount of data without lowering the quality of the host signal. The pixel-value differencing (PVD) steganographic approach and its two modified variants, upgraded pixel-value differencing (EPVD), and tri-way pixel-value differencing, were examined in this work for their intangibility, commitment, and impact on compression effectiveness (TPVD). The results of the testing demonstrate that the EPVD plots are superior to the others in terms of their ability to carry out plans.

B. S. Manjunath, K. Solanki, N. Jacobsen, and S. Chandrasekaran are few of the authors. The hidden information can always be recovered, even after being subjected to attacks like compression, minor video resizing, and other modifications. Below are the first three conclusions. In order to minimise detectable mutilation while hiding a lot of information, covering up plans must apply video-adaptive criteria in addition to factual criteria based on data speculation. If local factors are taken into consideration while deciding where to hide data, the encoder and decoder may differ. This synchronisation issue is resolved by the use of efficient yet simple deletions and mistakes correcting methods, which also provide vigour against a range of assaults. Techniques based on scalar quantization are efficient even when information theory is hidden.

E. Muller, M. Schlauweg, and D. Profrock [3] The techniques can be divided into three groups: punctured channel coding, energetic programming, and concatenated coding. As can be seen, the last example does not take de-synchronization in moment era watermarking schemes into consideration when there are much more selected insertion areas than have flag tests. a modern method that performs better than every previous method up to this point in terms of insertion/deletion error correction in modern watermarking schemes.

B. Liu, M. Wu, and H. Yu Utilizing multilayer inserting system that enable adjustable information extraction amount according on actual clamour circumstance. The issues of masking different bits are then taken into consideration as we examine various multiplexing and balance solutions. Finally, the nonstationary nature of visual signals hampers information stowing and produces a significantly unequal distribution of implanting capacity.A versatile system that can alternate between rearrangement and a constant implanting rate as well as control bits and a variable implanting rate.

4) SYSTEM ANALYSIS

4.1. EXISTING SYSTEM

Nowadays, text- and image-based steganography is used to hide data. The most straightforward approach to change, even unintentionally, is text-based steganography, which hides the secure message within the plain text. Text-based steganography cannot be quantified since doing so would compromise the secure message's confidentiality. Secure messages have been concealed in the literature by enlarging images by more than 50%. Its capability was hoped to be increased using image-based steganography. There are alternative techniques to help strengthen the security of collaborative papers because there is a cap on how much information can be buried in an image, making the usage of the image solutions difficult. It has been discovered that videobased steganography can overcome the capacity problem. Video-based steganography also has the lowest likelihood of drawing attention because the frames are shown swiftly, making it harder for the human visual system.

DRAWBACKS

- It doesn't offer data security. While the data is being transmitted, the sensitive information is exposed.
- Data about specific individuals is not private.
- By taking into account the pixel values of images, hidden information can be found using image-steganography.

4.2. PROPOSED SYSTEM

Using redundant cover data, including photographs, audios, videos, documents, and so on, is a common practise for keeping information hidden. In a variety of application sectors, this technique has recently gained importance. Digital video, music, and image files, for example, are increasingly being incorporated with invisible markers, such as watermarks or secret signatures, that assist prevent unauthorised duplication. In order to hide their existence, hidden messages are performed by being placed inside of a cover file. This method uses video-based steganography to conceal data. The first step in adding data to a video file is choosing the desired video. Next, the input file is chosen for additional processing. Afterwards the data is encrypted and the Forbidden Zone Data Hiding allows data to be concealed. the video's technical approach. You can extract the data from a video file by selecting it and then inputting the key.

ADVANTAGES:

- User cannot find the original data.
- It is not easily cracked.
- To increase the Security.
- To increase the size of stored data.
- We can hide more than one bit

5) SYSTEM SPECIFICATION

5.1. SOFTWARE REQUIREMENTS:

- SYSTEM : Pentium IV
- HARD DISK : 80 GB
- MONITOR : 15 VGA colour
- MOUSE : Logitech.
- RAM : 512 MB
- KEYBOARD : 110 keys enhanced.

5.2. HARDWARE REQUIREMENTS:

- Operating system :- Windows XP Professional
- Front End :- Microsoft Visual Studio .Net 2008
- Back End :- Sql server 2005

6) PROJECT DESCRIPTION

6.1. PROBLEM DEFINITION:

To hide the data using Forbidden Zone Data Hiding and Careful Surrounding by Using Encoding and Decoding by Digital Watermarking. ENCODDING: It provide encryption key
DECODDING: It provides decryption key
Digital watermarking: Protect the original data's copyright

6.2. INTRODUCTION PROPOSED SYSTEM

The two primary methods for obscuring information in video sequences are data-level hiding and bit stream-level concealing. Here, we present a novel block-based selective embedding type data-hiding paradigm based on Forbidden Zone Data Hiding (FZDH) By implementing straightforward constraints to the frame markers, we strengthen the resistance against frame drop, repeat, and insert attacks. The two primary methods for obscuring information in video sequences are data-level hiding and bit stream-level concealing. Here, we present a novel blockbased selective embedding type data-hiding paradigm based on Forbidden Zone Data Hiding (FZDH) By implementing straightforward constraints to the frame markers, we strengthen the resistance against frame drop, repeat, and insert attacks. Data is hidden via video segments.

ADVANTAGES

- User cannot find the original data.
- It is not easily cracked.
- To increase the Security.
- To increase the size of stored data.
- We can hide more than one bit

6.3. MODULES

- ✞ Select video file
- ✞ Input Modules
- ✞ Security Key
- ✞ Encoding Module
- ✞ Decoding Module

6.3.1. Module:1:-SELECT VIDEO FILE

In order to hide the data in this module, authorised users must choose an input video file. The files that have hidden messages must be in the mpeg format. The output video file's name and location are also chosen. The option is selected by launching a new dialogue box, and the selected path is displayed in a text box.

6.3.2. Module:2-INPUT MODULE

The suggested system must be able to cope with any sort of data; for example, if a user wants to hide any data, it must be compatible with all popular text file types. The input module's design is based on this justification. Any format must be usable by the user to conceal the secret data.

6.3.3. Module 3:-SECURITY KEY

In this module, the security key file is either selected or produced. The video file can be protected with this, as can the embedded data. The selected files are then checked. We view any files we may have selected, and the path is verified.

6.3.4. Module 4:-ENCODING MODULE

The video file is embedded with data using the Forbidden Zone Data Hiding Method. The material will be embedded before the output video file is played, so the listener won't be able to detect the difference between the input and output video files. The user of this module may upload data or type it in using the browse button. The user can select the secret message when they click the browse button, which causes the open file dialogue box to appear. The user can select the video file by clicking the cover file button, which triggers the appearance of a new open file dialogue box. The user picks the cover file and clicks the Hide button to conceal the hidden data or message in the cover file.

6.3.5. Module 5:-DECODING MODULE

An encryption component and the Key file must both be specified in this module, which is the opposite of an encryption module. The user should choose the encrypted cover file and then click the extract button so that the hidden message will either be displayed in the application's designated text field or extracted to the location they specify.

7) SYSTEM IMPLEMENTATION

This module, which is the reverse of an encryption module, needs to specify the Key file as well as the encryption component. Once the encrypted cover file has been selected, the user should click the extract button so that the concealed message will either be displayed in the application's allocated text field or extracted to the location they specify. The objective of the implementation process is to develop and manufacture (or produce) a system element that conforms with the design requirements of the element. Suitable technology and industry standards were used in the construction of the element. This procedure links the system definition process and the integration process.

The proposed system was developed with.NET Visual Studio. The existing system features a very user-friendly tool with a menu-based and graphical user interface, but it required a timeconsuming transmission process. This contrasts with the earlier technology, which transmitted data slowly. After developing and testing, the project must be installed on the necessary system. The system must be created with the executable file loaded into it. The code is checked out in the installed system once more. Implementation entails loading the written code into the computer as an executable file.

8) RESULTS AND DISCUSSION

A video that is text-based and must be saved before being added to another video file. We can add text with a couple of clicks. Font, colour, style, and other elements can all be changed. Put the text tool on the screen after uploading the video to get started. Choose a handwritten-looking font, add a title, or use some simple text. Take the words out and make a video. When the text is integrated in the video, you must once more remove it. When a text-based file is extracted, the original text file's content is once more visible Comments and tracked file modifications are made possible by this. In the second phase, errors are corrected and performance against various popular video processing attacks is assessed. Use is made of a standard 10-minute TV broadcast. We recommend coming to conclusions quickly even if RA decoding requires a lot of work but still produces precise results. The test movie is 720x576 pixels in size and is in MPEG2 9Mb/s format. For two distinct levels of embedded distortion, the results are displayed in a table. The findings show that the number of retries needed is more than the elimination rate. This discovery is supported by the observation that both compression and block selection-based erasure lead to decoding errors. There must be additional iterations for error-free decoding. Steganography in video is a secure method of secret communication. Even after a security breach, difficulties still need to be taken into account, as was already said, even though the majority of intruders do not view or listen to video with much temptation or mistrust. The random least significant bit algorithm is the fundamental and primary building block of this steganography technology. A straightforward comparison reveals that the RLSB approach is superior to the LSB algorithm. Moreover, the LSB outperforms DWT-based and DCT-based approaches in terms of performance. Keys have a crucial role in embedding messages. It is more harder to disbelieve the secret with larger keys. Hence, it is secure to combine steganography using the RLSB approach. As a result, it may be argued that video steganography utilising a random, lowest-order algorithm is a practical and efficient communication technique in the current, unreliable cyberspace.

9) CONCLUSION AND FUTURE ENHANCEMENT

9.1) CONCLUSION

The programme works well and satisfies user needs, so that much is true. The programme is rigorously tested, and any bugs are effectively debugged. The programme is being used by several systems at once. There are several simultaneous login tries tested. This system is userfriendly, so anyone may use it with ease. The required documentation is presented. The end user can rapidly comprehend the practical application of the entire system by reading the documentation. The system has undergone testing and implementation, and its performance has been good. The full amount of output is generated. The project was thus effectively finished. The application can still be enhanced to function in a more enticing and useful manner than it does at the moment. The speed of transactions has increased.

9.2) FUTURE ENHANCEMENT

The random LSB approach offers security, but the choice of cover media bits can be enhanced by concentrating on particular regions of the image, such as the edges. This method is efficient since it enables you to detect edges, mask them, and then apply the RLSB algorithm. Robert, Laplace, Prewitt, Sobel, and Canny can all be used to find edges.Text in plain text is the cover's cryptic message. To enable the algorithm to hide extensions like mp3, rar, and flv, improve it.