International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Video Steganography

Jagruti Mishra[1]
Information Technology,
Bharati Vidyapeeth College of Engineering, Kharghar – 410210
Maharashtra, India

Madhavi Chavan[2]
Information Technology,
Bharati Vidyapeeth College of Engineering, Kharghar – 410210
Maharashtra, India

Riddhi Ambekar[3]
Information Technology,
Bharati Vidyapeeth College of Engineering, Kharghar –410210
Maharashtra, India

Abstract - *Steganography is that the art of hiding the very fact that communication is happening, by hiding information in other information. Many different carrier file formats are often used, but digital images are the foremost popular due to their frequency on the web. For hiding secret information in video frames, there exist an outsized sort of steganography techniques some are more complex than others and every one of them have respective strong and weak points. For example, some applications may require absolute invisibility of the key information, while others require a bigger secret message to be hidden. This project hides the message with in the image. For a safer approach, the project it allows user to settle on the bits for replacement rather than LSB replacement from the image. sender select the duvet image with the key text or document and conceal it in to the image with the bit replacement choice, it help to get the secure stego image .the stego image is shipped to the destination with the assistance of personal or public communication network .on the opposite side i.e. receiver. Receiver download the stego image and using the software retrieve the key text hidden within the stego image.*

***Key Words*: Encryption, Decryption, Data-hiding, Compression, MATLAB.**

1. INTRODUCTION

Steganography may be a Greek word which suggests concealed writing. The word steganos means covered and graphical means writing. Thus, steganography isn't only the art of hiding data but also hiding the very fact of transmission of secret data. Steganography hides the key data in another enter such how that only the recipient knows the existence of message. In ancient time, the information was protected by hiding it on the rear of wax, writing tables and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the information within the sort of text, images, video, and audio over the medium. In order to securely transmission of confidential data, the multimedia object like audio, video, images are used as a canopy sources to cover the information. Steganography usually deals with the ways of hiding the existence of the communicated data in such how that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are differing types of steganography techniques each have their strengths and weaknesses. In this paper, we review the various security and data hiding techniques that are wont to implement a steganography like LSB, ISB and MLSB etc. In today's world, the communication is that the basic necessity of each growing area. Everyone wants the secrecy and safety of their communicating data. In our lifestyle, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a particular level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is modified in an encrypted form with the assistance of encryption key which is understood to sender and receiver only. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Steganography hides the existence of data so that no one can detect its presence. For increasing confidentiality of communicating data we used video Steganography.

2. LITERATURE SURVEY

2.1 A Video Steganography in Spatial, Discrete Wavelet Transform and Integer wavelet domain (2018).

Steganography is the sculpture and science of literature text which is to be hide overdue chose one as a cover file like multimedia file as audio, image or video. Secret message hiding is best of the techniques that provide for retreat by hiding secret word into the video or image file by some elements in the cover file. The main advantage of using video in hiding the main data is to be added, safekeeping against hacker beats due to the comparative complexity of video compared to image files and audio files. An image steganography has been a

large region of research for many years but now day's increase the information hiding on the www (world wide web) and internet day by day so in this paper proposed the more data or information hide by though video steganography main purpose of that paper is increasing the capacity of hiding information on the internet or www and also used various methods and compare better result is depends on the parameter value matrix.

METHODOLOGY USED:-

1. DISCRETE WAVELET TRANSFORM (DWT)
2. Integer Wavelet Transform (IWT)
3. 3D SPHIT ENCODER

The paper has high hiding information payload. The secret message in each or every video frame is round 5.12 Mbytes and the hiding rate is 27.66. -This research describes one of the techniques of video steganography. The main objective of this technique is implemented on any type of image or video format. Jpeg, bmp and png images. [10.1109/ICICS.2018.00060]

2.2 A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes (2016).

In the past decade, the science of information hiding has gained tremendous significance due to advances in information and communication technology. The performance of any stenographic algorithm relies on the embedding efficiency, embedding payload, and robustness against attackers. Low hidden ratio, less security, and inferiority of stego videos are the main problems with many existing stenographic methods. Message and cover data might be any sort of format like text, audio, image, and video. The development of steganalysis tools weakens unsecure steganography schemes and rendering them useless. Hence, researchers need to develop secure steganography algorithms that are shielded from both attackers and steganalysis detectors.

-DISCRETE COSINE TRANSFORM (DCT) DCT is used for separation of signal into low, medium and high frequency regions. It is well known method used for image and video compression.
-HAMMING AND BCH CODES Hamming codes correct the identification of single bit error. Message is encoded by adding extra bits as a parity to become a code word of 7-bit length. Bose, Chaudhry and Hocquenghem invented the BCH codes. BCH can correct more than one bit. It is used for detecting and correcting errors in block of data.
-The proposed algorithm has a high embedding payload. Experimental results showed that the proposed algorithm is robust against several attacks.
-In addition, the security of our method is improved, by ciphering and encoding processes prior to the embedding process.
[10.1109/SARNOF.2016.7846757]

2.3 Texture Based Video Steganography Technique Using Block-Wise Encryption (2017).

The video data hiding methods utilize uncompressed video data. Proposes a high-volume transform domain data hiding in MPEG-2 videos. They apply QIM (Quantization Index Modulation) to low frequency DCT (discrete cosine transformation) coefficients and adapt the quantization parameter based on MPEG-2 parameters. Furthermore, they vary the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes de-synchronization. The proposed algorithm can be applied in the following steps: -
•Pre-processing Phase
•Feature extracted -GLCM algorithm (for textual feature analysis)
•Apply PCA algorithm (feature selection and block wise encryption)
•Encryption of first image
-Venkata Krishna et al. proposed in this paper a new image encryption mechanism that includes the AES and visual cryptography methods.
-The main motive here is to protect the image for which an encoding mapping is proposed.
-This method helps in converting the key into shared with respect to the Visual Secret Sharing mechanism. By making modifications in the key shares the confidentiality is tested here. [10.1109/SITIS.2017.28]

3. PROBLEM STATEMENT

The usage of Internet in the world is increasing very highly. Present day transactions are considered to be "untrusted" in terms of security, i.e. they are relatively easy to be hacked. We also have to consider the transfer of large amount of data through the network which will give errors at the time of transferring and only the single level of security is present in the

existing systems. Now days, hacking activities are growing day-by-day and they easily hack important information and security mechanisms is not sufficient to stop it. Though security status increased at a higher level but the major drawback of new status of security is costly. For that we need better solutions with good security level and lower cost. There are many techniques to overcome this problem like Image steganography, cryptography, and audio steganography. But many limitations have aroused in Image, audio and text steganography related to security, encryption, decryption and the space provided by these techniques. To overcome all these problems, the technique which gained a special importance is "Video steganography". It has gained a considerable amount of attention due to its possible applications in multimedia fund information security.

4. FUTURE SCOPE

The scope of the project is to limit unauthorized access and supply better security during message transmission. To meet the wants, I exploit the straightforward and basic approach of steganography.

• During this project, the proposed approach finds the acceptable algorithm for embedding the info in a picture using steganography which provides the higher security pattern for sending messages through a network.

• For practically implementing the function of the discussed algorithms, Matlab framework is employed.

5. OBJECTIVES

In my project I primarily targeting the info security issues while sending the info over the network using stenographic techniques.

The main objectives of the project are:

• Requirement of this steganography system is that the hider message carried by Stego-media shouldn't be sensible to citizenry.

• The opposite goal of steganography is to avoid drawing suspicion to the existence of a hidden message.
• This approach of data hiding technique has recently become important during a number of Application areas.

6. SYSTEM ARCHITECTURE

6.1 System Architecture

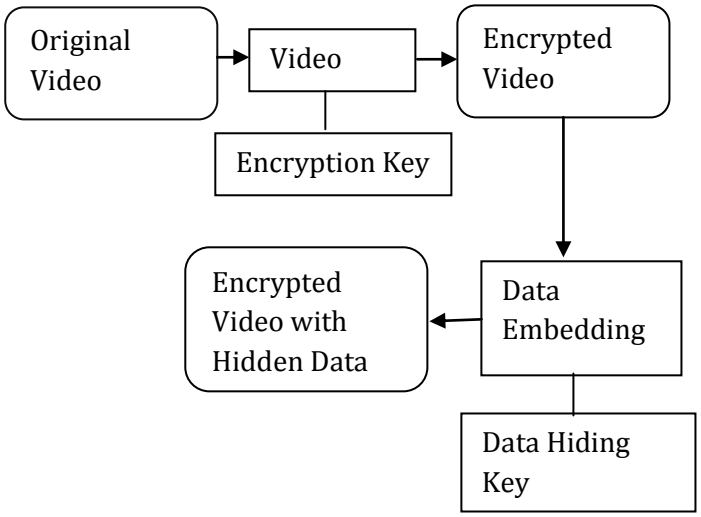


Fig1. System Architecture

6.2 Block Diagram

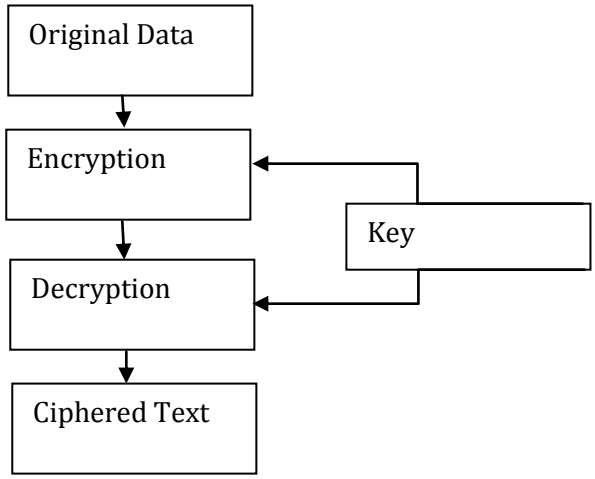


Fig2. Block Diagram

6.3 Flow Diagram

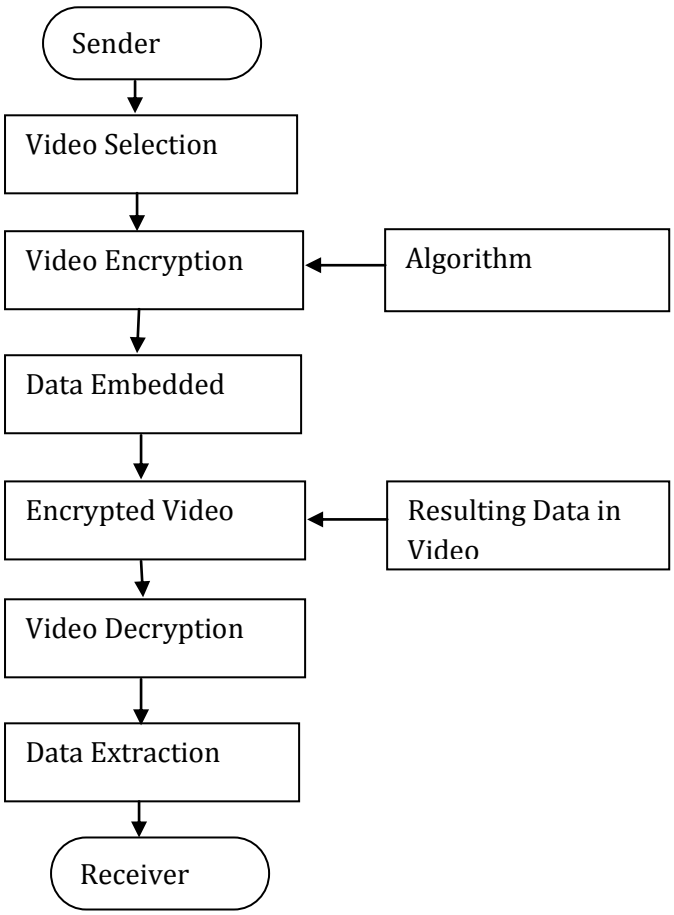


Fig3. Flow Diagram

7. Result

- **Comparison of Test Cases**

Algorithms	PSNR Values	Size	Encoding Time	Decoding Time
LSB	45.02db	32768 bytes	0.06909 sec	0.01991 sec
DCT	40.15db	512 bytes	6.32192 sec	0.82727 sec
ZK	22.79db	270 bytes	0.83634 sec	0.50305 sec
WDCT	44.10db	128 bytes	5.36287 sec	0.46884 sec
Fusion	32.52db	8192 bytes	1.88729 sec	0.58793 sec
Egypt	57.86db	18 bytes	2.90338 sec	0.65923 sec
RDH	47.56db	230400 bytes	0.05762 sec	0.00545 sec

On comparison of various Algorithms Test Cases (LSB, DCT, ZK, W-DCT, Fusion, Egypt, RDH). It is clearly shown that RDH algorithm is the best suited Algorithm for video Steganography. The PSNR value is the highest as compare to other six Algorithms. Size of Bytes is greater among all Algorithms. Encoding time and Decoding time is the lowest of all.

8. ALGORITHMS

8.1 LSB Algorithm

LSB stands for Least Significant bit. The idea behind LSB embedding is that if we modify the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

8.2 DCT Algorithm

In a DCT algorithm, a picture (or frame a picture sequence) is split into square blocks which are processed independently from one another, then the DCT of those blocks is taken, and therefore the resulting DCT coefficients are quantized.

8.3 ZK Algorithm

The acronym ZK-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of knowledge" and refers to a logo construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and with none interaction between the prover and verifier.

8.4 WDCT Algorithm

The DCT-based JPEG standard is that the most ordinarily used lossy compression algorithm for still continuous-tone images due to its high effectiveness and low computational complexity. However, the visually disturbing blocking artifacts generate when image is compressed at low bit rates. With the frequency warping, the warped discrete cosine transform (WDCT) makes the signal energy distribution more suitable for image coding.

8.5 Fusion Algorithm

The secret message shouldn't be damaged on the method of the duvet media. In order to make sure the invisibility of secret message, complex texture objects should be chosen for embedding information. Firstly, complex texture regions are selected supported a sort of objects detection algorithm. Secondly, three different stenographic methods were wont to hide secret message into the chosen block region.

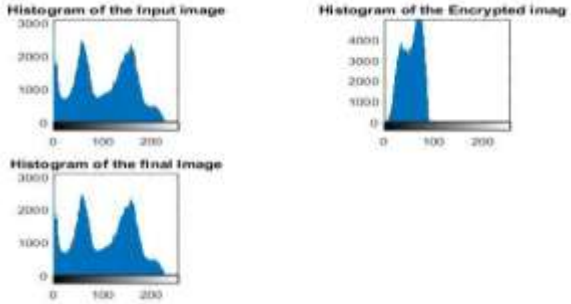
8.6 EGYPT Algorithm

The image steganography systems use either the spatial domain or the frequency domain to cover the key information. The proposed technique uses spatial domain technique to cover secret information within the frequency domain. The cover image is transformed using integer wavelet transform to get four sub bands: LL, LH, HL, and HH. Then, the PVD approach is employed to cover the key information within the wavelet coefficients of all the four sub bands. For improving the security of the hidden information, the proposed method first modifies the difference between two wavelet coefficients of a pair then uses the modified difference to cover the information.

8.7 RDH Algorithm

REVERSIBLE DATA HIDING (RDH) has been intensively studied within the community of signal processing. Also referred as invertible or lossless data hiding. RDH is to embed a bit of data into a number signal to get the marked one, from which the first signal is often exactly recovered after extracting the embedded data. The hiding data and the marked image quality are important metrics while evaluating the performance of a RDH algorithm.

9. Histogram Result



Advantages: -

- The main advantages of this technique is Security; that it provides security to your messages without knowing to 3rd party.
- Number of bits are replaced consistent with user or sender; therefore, third party can't guess password.
- Normal network user can't guess image.
- In steganography anyone can't hop on suspect by looking images.
- It is Reliable.
- Easy to use.
- Easy Maintenance.
- System are secured by password authentication.

Disadvantages: -

- Images can have attacks like diluting, nosing, contrast changes then on.
- Number bits of pixel should get replaced by equal bits of message.
- If someone is eavesdropping then there's probability of message get unfold.
- If quite two people having same Steganography software then hidden message can acquire.

10. Conclusion

Objective of any data hiding algorithm is to hide the data in such way that it should become difficult to retrieve the hidden data for unintended user. Code Word substitution is used to hide data in host video. Using this scheme file size of the host video is preserved alongside the confidentiality. This algorithm can achieve a better performance compared with the other algorithms. So, the proposed framework features a potential to supply excellent RDH algorithms.

11. References

[1.] A Video Steganography in Spatial, Discrete Wavelet Transform and Integer Wavelet Domain. https://ieeexplore.ieee.org/document/8479581

[2.] Texture Based Video Steganography Technique Using Block-Wise Encryption. https://ieeexplore.ieee.org/document/8334733

[3.] A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes.
https://ieeexplore.ieee.org/document/7494111

[4.] A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes.
https://ieeexplore.ieee.org/document/7846757