Video Frame based on Image Frames Steganography

Mrs. Sneha C R[1], Shilpa[2], Roopa Devi[3], Revathi[4], Pooja H R[5]

[1]Assistant prof, [2,3,4,5]Students

Computer Science & Engineering Dept, ATME College of Engineering, Mysore.

***Abstract* -** Due to advances in technology and high speed of internet people are becoming more worried about information being hacked by attackers .Most common technique used in video steganography is to store information in the LSB of the cover frames .Along with embedding, many different encryption techniques such as XOR, AES, DES, Hash have been applied to convert original message to secret form. Cover image frames selection is an important task in video steganography process which can act as one of the important security measure. Embedding along with encryption techniques makes video steganography stronger and reliable. This paper proposes a novel video steganography algorithm based on Divide and Conquer rule using midpoint logic. The proposed system considers all the parameters i.e. robustness, undetectability, and capacity required to design a more reliable and efficient system for hiding important information.

***Keywords* -** Steganography, Blowfish algorithm, Toofish algorithm, key frame extraction, video analysis.

I. INTRODUCTION

Information security requirement became more important, especially after the spread of Internet applications. Steganography means invisible communication by hiding important data behind certain cover. There are various ways of hiding important data in digital mediums Information security requirement became more important, especially after the spread of Internet applications. Steganography means invisible communication by hiding important data behind certain cover. There are various ways of hiding important data in digital mediums.

This paper presents the hiding of text in video using haar wavelet transform in particular frame and BCH codes. Haar wavelet transform is applied to get the low frequency sub-band in an image to hide data. The frequency sub-bands are (LL, LH, HL and HH). BCH codes are used to encrypt the data. The work of various researchers is discussed about video steganography and their techniques for embedding and extraction of data. With the advancement of technology and multimedia information, Videos and digital images are increasing very quickly. Steganography is hiding private or secret data within a carrier in invisible manner. A lot of information can be stored in video files. It contains number of frames played over a period of time. .Information can be stored in any or number of frames. Moreover, Attacker or Human eye cannot detect the presence of message in video because video frame is only visible for a fraction of time.

Keywords: Steganography, Cryptography, Encryption Algorithm.

Video Steganography is a very important task in real life where the users want to keep data secret. Data is the heart of computer communication and over the years, different methods have been proposed and created to accomplish the goal of using steganography to hide data. The problem occurs when Traditional Text and Image Based Steganography techniques is not plentiful .They are able to carry only small files. So there is a problem, how to get much enough files to hide our message. This becomes a very tedious task for carry large amount of data. Here, comes the need of Video Steganography. The use of video as a carrier cover for the secure message is overcame the capacity problem. Information can be hidden in any frame of video. Video has a large Capacity to store information. Added small enhancement to the security aspects. The integration of Steganography and cryptography techniques provided powerful systems for sharing secure messages.

II. EXISTING SYSTEM

In the existing system, the video classification on the basis of data recognition is a Manual task where Human can recognize data without any significant delay and effort but recognition of data by machine is a big challenge. Making data redundant may huge loss for organizations and data hiding can be done using images only. There are currently three effective methods in applying Image Steganography: LSB Substitution, Blocking, and Palette Modification. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the carrier image.

Disadvantages of existing system -

- Static Image
- Pixel based data hiding.
- Single algorithm to encrypt
- Less security
- Less integrity

III. PROPOSED SOLUTION

Taking all of this information into consideration, a simple but somewhat novel steganography tool for hiding data in Video frame is proposed. Four Stages on sender end are shown in

i) Encryption Technique i.e. used for converting original secret message to encrypted message.
ii) Selection of frames of the selected frame in a video.
iii) Data embedding into selected frames.
iv) Resequence the frames to form stego frame in a video.

Advantages -

- Dynamic Image
- Pixel based data hiding.
- Multiple algorithm to encrypt
- More security
- More integrity
- Key based data sharing

IV. METHODOLOGY

Here we are using two algorithms for encryption:

The Blowfish Algorithm - Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both Encrypt and decrypt messages. Blowfish is also a block cipher [5], meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.

Blowfish consists of two parts: key-expansion and data encryption. During the key expansion stage, the inputted key is converted into several sub key arrays total 4168 bytes. There is the P array, which is eighteen 32bit boxes, and the S-boxes, which are four 32-bit arrays with 256 entires each. After the string initialization, the first 32 bits of the key are XORed with P1 (the first 32-bit box in the P-array). The second 32 bits of the key are XORed with P2, and so on, until all 448, or fewer, key bits have been XORed Cycle through the key bits by returning to the beginning of the key, until the entire P-array has been XORed with the key. Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to geta 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the Parray with the block. Repeat for all the values in the P-array and all the S boxes in order.

Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to get a 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the P-array with the block. Repeat for all the values in the P-array and all the S boxes in order.

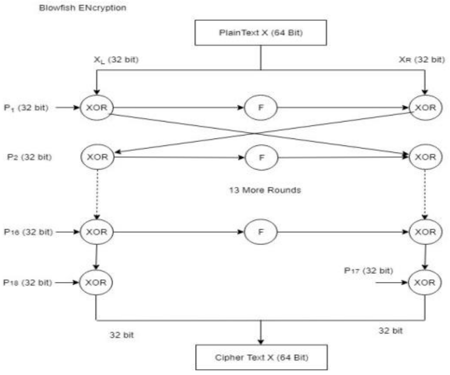

Figure 1: Blow Fish Algorithm

Twofish Algorithm - Twofish algorithm is a strong algorithm that until now declared safe because there is still no crypt analysis attacks which can really break it. This algorithm is also not patented so its use on encryption tools does not need cost. Twofish algorithm is one of the algorithms which is recommended as AES. It is due to the fulfillment of design criteria by NIST as standard of AES namely:

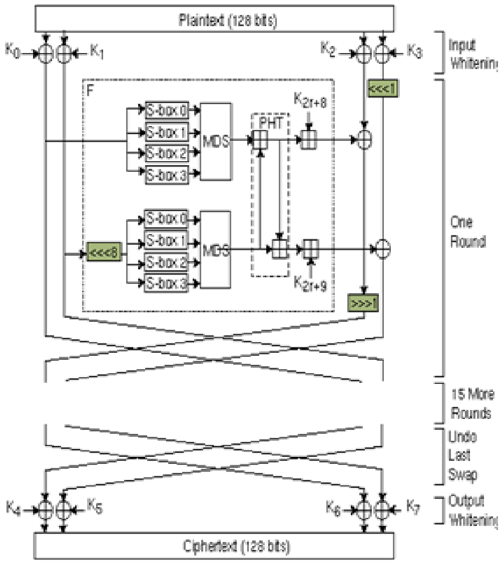

Figure 2: Two Fish algorithm

Two Fish algorithm: 128-bit symmetric cipher blocks .Having key lengths among others: 128 bit, 192 bit, and 256 bit. There are no weak keys. Having the efficiency on the software and hardware from different platforms. Having a flexible design, for example, receive an additional key length, can be applied to software and hardware from different plat form, suitable for stream cipher, hash function and MAC. The design is simple in order to facilitate the process of analysis and implementation of algorithms.

In addition to the criteria mentioned above, it also added the performance criteria on Twofish as follows:

i) Accept any key lengths up to 256 bit.
ii) Encrypt the data in less than 500 clock cycles per block on Intel Pentium, Pentium Pro and Pentium II, for a fully optimized version of the algorithm.
iii) Able to form 128-bit key (for optimal encryption speed) in a time less than the time required to encrypt 32 blocks on Pentium, Pentium Pro and Pentium II.
iv) Does not use operations that make Twofish inefficient on microprocessor except 32-bit, 8 bit microprocessor and 16 bit microprocessor.

Techniques used:

A. Randomness - A random number is a technology designed to generate a sequence that does not have any pattern, therefore appear to be random. This method based on selection of random pixels from a image and again secret data is hidden in random bits of these randomly selected pixels. These pixels are selected by using a random number.

B. LSB Technique - The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. In this work, a new technique of LSB steganography has been proposed which is an improvised version of one bit LSB technique.

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is to use steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

C. Luminance calculation - It is also known as brightness calculation technique. It is based on the visual ability of individual person. It is a measure the amount of light emitted from the surface. Here brightness is measure based on the average brightness of neighbouring frames.

V. CONCLUSION

This paper proposed a high security data hiding technique in videos using multi frame, image cropping and LSB algorithm. Random frame selection technique in video steganography provides more security to the secret data as well as it increases the quality of stego video. Video is used as a carrier to embed a secret message. Selecting low frequency sub band for embedding information increases robustness of secret data. This proves to be a more secure method for data hiding. This technique can implemented in secrecy departments like military, banking even in daily life.

VI. REFERENCES

[1]. Ide, H. Mo, N. Katayama, S.i. Satoh, “Exploiting topic thread structures in a news video archive for the semi-automatic generation of video summaries,” IEEE International Conference on Multimedia and Expo, Proceedings, pp.1473–1476, 2006.

[2]. K. Choros, P. Pawlaczyk, “Content-based scene detection and analysis method for automatic classification of TV sports news, in: M. Szczuka, M. Kryszkiewicz, S. Ramanna, R. Jensen, Q.H. Hu (Eds.),” Rough Sets and Current Trends in Computing, Proceedings, vol. 6086, pp. 120–129, 2010.

[3]. K. Choros, “Categorization of sports video shots and scenes in TV sports news based on ball detection, in: N.T. Nguyen, B. Attachoo,” B. Trawinski, K. Somboonviwat (Eds.), IntelligentInformation and Database Systems, Pt 1, vol. 8397 2014, pp.591–600, 2015

[4]. X. Gao, J. Li, B. Yang, “A graph-theoretical clustering based anchorperson shot detection for news video indexing, FifthInternational Conference on Computational Intelligence andMultimedia Applications,” Proceedings, pp. 108–113, 2003.

[5]. K. Choros, “Temporal aggregation of video shots in TV sports newsfor detection and categorization of player scenes, in: C. Badica, N.T. Nguyen, M. Brezovan (Eds.), Computational Collective Intelligence: Technologies and Applications,” vol. 8083, pp. 487– 497, 2013.

[6]. Z. Rasheed, M. Shah, “Scene detection in Hollywood movies andTV shows, 2003, IEEE Computer Society Conference onComputer Vision and Pattern Recognition, Proceedings,” vol. 2, IEEE, pp. 343–348, 2003.

[7]. L. Ott, P. Lambert, B. Ionescu, Coquin, “Animation movie abstraction: Key frame adaptive selection based on color histogramfiltering, 14th International Conference on Image Analysis and Processing Workshops, Proceedings,” ,pp.206–211, 2007.