A Framework for Efficient and Secure Information Transform by using LSB and Diffie Hellman Algorithm

Sushant Mangasuli[1]
Assistant Professor, Alva's Institute of Engineering and Technology Moodbidri, India

Arundhati Nelli[2]
Assistant Professor, KLS Gogte Institute of Technology, Belagavi, India

Sneha K N[3]
Alva's Institute of Engineering and Technology Moodbidri, India

Suraksha R B[4]
Alva's Institute of Engineering and Technology Moodbidri, India

Abstract: **Steganography is hiding private or secret data within a carrier in invisible manner. The medium where the secret information is secreted is called as cover medium which can be an image, an audio or video file. Any stegno algorithms removes the redundant bits in the secret media and adds the secret data into that media. As the quality of video or sound is higher, more redundant bits are accessible for hiding. To make available secure communication between the users by using the video Steganography is used. Here to provide a secure transfer of the data in the military information using video Steganography by applying the Diffie- Hellman algorithm used for key generation and LSB matching revised algorithm this method creates a directory for the secret information and the directory is placed in a frame of the video itself. By means of the help of this directory, the frames containing the secret information are found. Henceforth, during the de-embedding process, instead of analysing the whole video, the frames containing the secret information are analysed with the help of index at the receiving side. This both techniques used for encrypt and decrypt the data.**

Keywords: Information security, Steganography, key generation.

I. INTRODUCTION

Steganography is the practice of hiding information "in plain sight". This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the presence of the data is unknown to an observer. Importantly, the transport layer – the carrier file - is not secret and can therefore be viewed by observers from whom the secret message itself should be concealed. The influence of steganography is in hiding the secret data by obscurity, hiding its presence in a non-secret file. In that sense, steganography is unlike from cryptography, which comprises of making the content of the secret data unreadable while not avoiding non-intended observers from learning about its presence. Because the success of the technique depends completely on the ability to hide the data such that an observer would not doubt that secret data is there at all, the highest effort is essential for ensuring that the message is invisible unless one knows what to look for. The way in which this is done will differ for the specific media that are used to hide the information [1,2].

In each case, the value of a steganography approach can be measured by how much data can be hidden in a medium before it becomes detectable, each method can thus be assumed of in terms of its capacity for data hiding. There are numerous methods used to hide data inside of Image, Audio and Video files. The desire to transfer the message as securely as possible has remained the main idea of discussion since many years. Data is the treasure of any organization. This leads to security-issues topmost importance to any organization dealing with private data. Any of the method we choose for the security purpose; the only concern is the rate of security [3].

Steganography is the art of covered or hidden writing. The purpose of this technique is secret communication to hide a message from a non-intended user. Steganography is frequently confused with cryptology as the two techniques are similar in the way that they both are used to secure the secret data. The difference among these are that Steganography includes hiding data, so it looks as if that no data is secreted at all. If a non-intender user tries to view the object that the data is hidden inside of, he or she will have no knowledge that there is any hidden data, hence the person will not attempt to decrypt the data. Steganography in the modern-day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file [4,5].

What Steganography basically does is exploit human perception; human minds are not trained to look for files that have data concealed inside them. Normally, in steganography, the actual data is not maintained in its unique format and in that way it is transformed into an another equivalent multimedia file like image, video or audio which in shot is being concealed within alternative object. This apparent data (known as cover text) is sent through the network to the recipient, where the actual data is separated from it [6].

II. LITERATURE SURVEY

A. A study Of Steganography and Art of information Hiding.
Steganography is technique that hides the secret data within text, image, audio, or video file. It is often confused with the term cryptography. The easiest method to distinguish in the two is to think of Steganography not only hides content of data but also the mere presence of data. Unlike other methods of steganography are discovered. A new term came into knowledge called Steganalysis. Steganalysis is a technique to spot presence of a hidden data and attempt to reveal the true content of the data. This study demonstrates various components of steganography which is said in the report. The research discovers set of rules applied to preserve planned results which is non-visible secret data with a cover information. Paper enlightens application of steganography in defense, government purpose [7].

The main goal of this method is to hide information on the output image of the instrument (such as image displayed by an electronic advertising billboard). This technique can be used for declaring a secret data in a public place. In wide-range, this technique is a kind of steganography, but it is completed in real time on the output of a device such as electronic billboard.

Following are the stages involved in inserting the secret data within a cover media.
a) Send the regular data that must be displayed to the display board.
b) With a suitable Steganography algorithm secure the secret data within the normal data before moving it to the display board. This technique can be used for declaring a secret data in public place. It can be prolonged to other means such as electronic advertising board around sports stadium.

B. Performance improving LSB video steganography.

The proposed technique is enhanced version of the LSB technique used for audio steganography, united with coding technique gives high embedding capacity with reference to literature survey LSB technique provides best outcomes hence considered for execution. The present steganography methods take assistance of renowned cryptography algorithms to rise security level. But our proposed technique uses additional coding technique. The data to be embedded is initially changed to decimal then converted to binary. Later it is converted to matrix where there are rows equal to total no of character to be embedded. Then that matrix is transformed to column matrix. In addition, then each bit is embedded into LSB of each audio example. When inserting the textual data in any audio folder, initial the audio sign is converted into bits. Then the data to be embedded is transformed from above approach. By applying LSB algorithm, the data is embedded into audio sample read at 16-bit format.

The proposed technique is enhanced version of the LSB technique used as audio steganography, combined with coding technique provide high embedding capacity. Listening test is accepted to find Minimum Opinion Score (MOS) which satisfies imperceptibility value. Text Intelligibility Index (TII) demonstrates 100% accurate extraction of the embedded text, for different message length, which varies from 16.5 kbps minimum to 97.6 kbps maximum length of messages. Time domain representation of original and stego signals show dissimilarities, but the effect of these dissimilarities is inaudible when the two audio signals heard separately. Proposed method is applied to various audio, speech and music envelope signals and it gives best outcomes satisfying steganography idea [8].

C. limits of Steganography
This paper discovered the restrictions of steganographic theory and practice. We started outlining several techniques both ancient and modern, collected with attacks on them (some new); we then discussed several probable methods to a theory of the subject. We pointed out the difficulties that stand in the way of a theory of perfect surreptitiousness" with the same power as Shannon's theory of perfect secrecy. But considerations of entropy give us roughly quantitative leverage and the selection channel the bandwidth of the stego key led us to suggest embedding information in parity checks rather than in the data directly. This approach gives improved efficiency, and also allows us to do public key steganography. Finally, we have revealed that public key steganography may be likely in the presence of an active warden.

A new perspective of LSB image steganography technique is presented. The main idea behind this technique is treating the contents of the secret data as a set of words instead of as a set of characters. And using a exact words dictionary, at the sender and the receiver of the secret message, to mean each word in the secret data as a number and concealed the bits of these numbers in the Least Significant Bit (LSB) of the pixels in the stego- image [9].
This will give the subsequent strong facts to Word-Based LSB technique.
a. Improve extra security to the secret message.
b. Rises the capability of hiding very long secret data in a small stego-image.
c. Decrease the noise that is appearing in the stego-image because the change that may happen in the LSB of the pixels in the stego-image.
d. Lessen the time that is required to hide and extract the secret data.

III. SYSTEM ANALYSIS

A. Existing System
The existing system of Video Steganography stances more limits on the selecting of video files. User can select only wav files to encode. It supports water marking method to encode. Its

complexity arises when more message to be encoded. The message length is restricted to 500 characters. It doesn't show the variations occurred after encoding the message. The LSB algorithm in the present system is not effective because it hides the message in consecutive bytes received from video files.

B. Proposed System

The existing systems want moral user interface, non-provision of selecting the key and additional encode-decode time consumption. There are bags of steganographic programs accessible. A few of them are brilliant in every respect; unfortunately, most of them lack usable interfaces, or comprise too many bugs, or unapproachability of a program for other operating systems. The proposed application will yield into account these limitations, operability over numerous operating systems and even over different hardware platforms would not be a problem. This proposed stego machine provides easy method of implementing the methods. The idea behind this design is to provide a good, efficient method for hiding the data from hackers and sent to the destination securely.

IV. SYSTEM ARCHITECTURE

Diffie–Hellman key exchange creates a shared secret amongst two parties that can be used for secret communication for exchanging information over a public network. The conceptual diagram to the right illustrates the general idea of the key exchange.

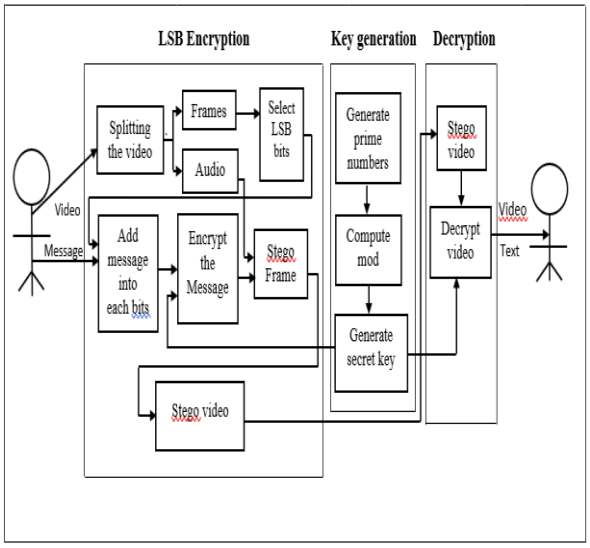

Figure 1: System Architecture

V. MODULES DESCRIPTION

A. Input module

In this module the user takes the video and the text message as two different input.

B. LSB Encryption module

In this module initially, the user video that would be converted to stegno video is split into the multiple frames and audio. Each frame contains bits where message bits are added into it using the LSB. The LSB bits are used because they do not form any modification of color as much like MSB bits. Then the messages are encrypted into frames of the images. Then each of the frames are converted into stegno frames. Then the merging of frames and audio takes place to form a complete stegno video.

Least significant bit (LSB) insertion technique is accurately what it sounds like; the least significant bits of the cover-image are changed so that they form the embedded information. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image. Pixels: (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001) and assume data is A: 01000001 Then the final Result is: (00100110 11101001 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001). The three featured bits are the only three bits that were essentially altered. LSB insertion wants on average that only partial the bits in an image be altered. Since the 8-bit letter A only needs eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden information.

C. Key generation and exchange module

In this module the generating of prime numbers takes place. Then the Diffie-Helman Key exchange algorithm is computed. This algorithm generates secret key that has to added to the stegno video. The stegno video and the secret is added to the stegno video and directed to the legitimate user through the mail.

Fig. 2 explains how key exchange algorithm works. The only problem was "If the attacker knows the common paint and he knows the end mixtures, why can't he figure out the original color?". The answer is of course that it's not the color he needs to know, but the actual original mixture, and as we mentioned, the mixture separation is expensive.

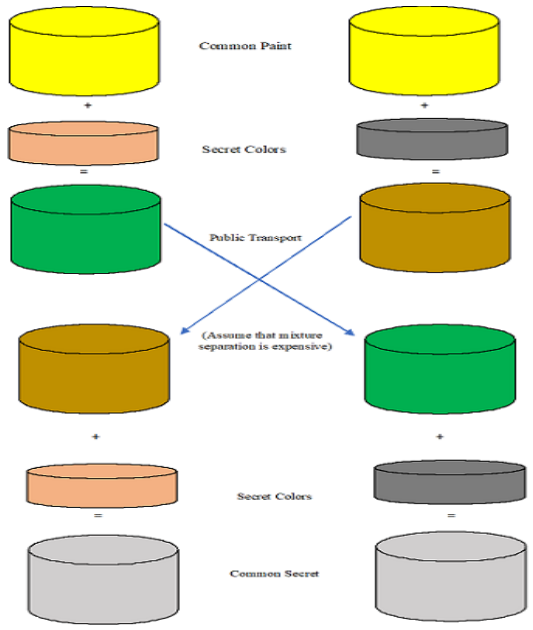

Figure 2: Key exchange mechanism

D. Output module

In this module the decryption of the steno video by using the secret key. Finally, the video and the secret message can receive by the user. Then the message is decrypted from the bit frames of the stegno video.

VI. RESULTS

By analyzing the algorithm and the method used in this paper the user can get the secret message that is encrypted in a video. The video has frames where each bit contains secret message combined to get a stegno video. The stegno video is sent from one end to another end through the communication channel. Here an algorithm is used where a secret key is added to make a secure transfer of the stegno video. The secret messages are hidden in the video that is received in another end by using the secret key. Then the video is separated from secret key and the stegno video is decrypted to obtain the secret message sent by the sender.

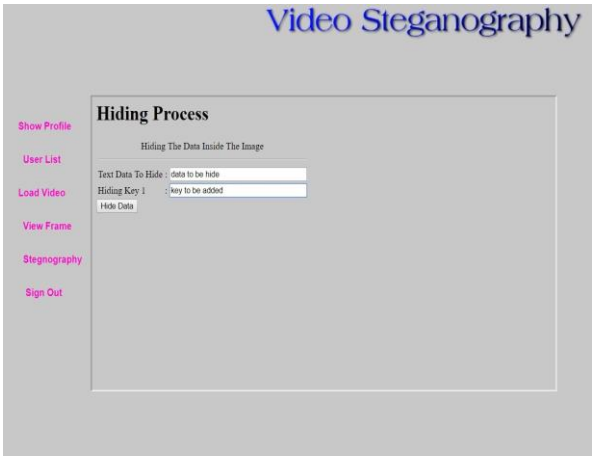

Figure 3(a) Before image encryption

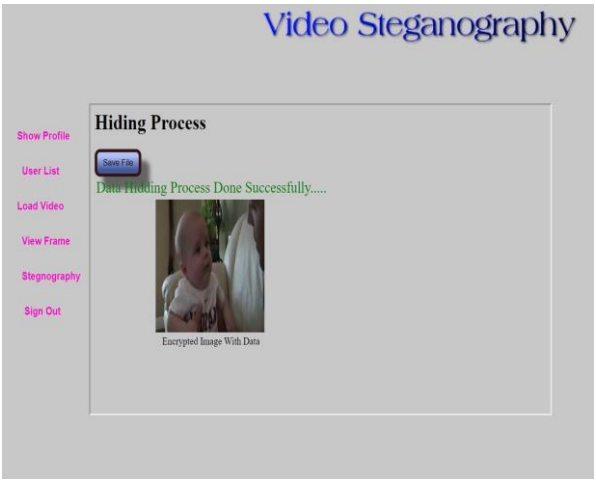

Figure 3(b) after image encryption

VII. CONCLUSION

The proposed technique is useful technique for protected communication over any medium. In the process of Steganography, the message which is hidden is invisible. An effort has been tried to implement encryption and decryption procedures on the information to be hidden into the video, so that this will bring additional safekeeping of the data. The main advantages of LSB are its simplicity to insert the bits of the data straight into the LSB plane of cover-image and many procedures use these approaches. Modulating the LSB does not result in a human-perceptible alteration because the amplitude of the alteration is minor. The sender and receiver only know how to hide and unhide the data into the video. No other intermediate person will even know that there is a second message inside the carrier file. The enhanced LSB technique described in this project helps to fruitfully hide the secret data into the cover object without any misrepresentation. The data hiding capacity of LSB technique is high and more secure. Embedding secret information with Ste-

ganography technique decreases the probability of secret information being detected and also allows high perceptual transparency.

REFERENCES

[1] Sofyane Ladgham Chikouche and Noureddine Chikouche, "An improved approach for lsb-based image steganography using AES algorithm", 5th International Conference on Electrical Engineering - Boomers (ICEE-B), IEEE Xplore, (2017)
[2] Alain C. Brainos II., "A study Of Steganography and Art of information Hiding", IEEE International Conference on Acoustics, East Carolina University (ICASSP '03), vol 2, (2013).
[3] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", International Journal of Advanced Science and Technology, Vol. 54, pp. 113-124, (2013).
[4] Ashish T. Bhole and Rachna Patel, "Steganography over video File using Random Byte Hiding and LSB Technique", IEEE international conference on computational intelligence and computing research. Vol.6, 2012, pp.674-679.
[5] Nivedita, Dr.T. Meyyappan, "Image Security using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, Vol.7, 2012, pp. 366- 371
[6] Anjali A. Shejul, Prof. U. L. Kulkarni, "A DWT based Approach for Steganography using Biometric", International Conference on Data Storage and Data Engineering, IEEE, 2010, pp. 39-43,
[7] Samir K Bandyopadhyay, Debnath Bhattacharyya, "A Review on Steganography" International conference on contemporary computing, volume 101, 2008.
[8] I.J. Cox, M.L. Bloom, Fridrich, "Digital watermarking and Steganography", USA: Morgan Kaufman Publishers,vol.05, 2008, pp. 1-591
[9] C. Science and B. Bridgeport, "A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes," 2015.