# Stenography using Image Audio Video

**Sunil Kumar N.[1] K. M. Sowmyashree[2]**
[1,2]Department of Computer Application
[1,2]PES College of Engineering, Mandya, India

*Abstract*— Security often requires that data be kept safe from unauthorized access. And the best line of defence is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option (due to cost and/or efficiency considerations). Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use.
***Key words:*** Least Significant Bit (LSB)

## I. INTRODUCTION

Image is an electronic medium for copying, playback, broadcasting and display of moving visual media. Image security has gained importance over time in numerous applications wherein information in the form of image is to be secured from unauthorized user. Image consisting of several frames which is nothing but images.

The use of internet has increased tremendously over the years and the concept of data security is gaining momentum. The word steganography combines the Greek words steganos meaning "covered" and graphic meaning "writing". The art and science of hiding information by embedding messages within other is steganography. It works by replacing bits of useless or unused data. Steganography is an Encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. It can be applied to images, a image file or an audio file. Steganography is used to supplement encryption. An encrypted file may still hide information, by using steganography even if the encrypted file is deciphered, the hidden message is not seen.

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security.

Hiding information in a carrier file we use least significant bit (LSB) insertion technique. In Least significant bit (LSB) insertion technique, for hiding information we change LSB of image file with the information bits. LSB insertion is the simplest technique for implementing Image Steganography. The LSB method substitutes the LSBs of the hidden message with the LSBs of cover image frames. Substituting data in the LSBs of any cover media is not detectable by human eyes (Human Visual System) i.e. very less change in the color. Here the bits of image from image are directly embedded into the least significant bit plane of cover frame in deterministic sequence.

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low latency or high throughput. We use 128 bit key for an AES algorithm which specifies the number of repetitions should be 10 cycles transformation rounds that convert the input called plain text into final output called cipher text. Each round consists of several processing steps that depends on the encryption key.

## II. LITERATURE SURVEY

Every Software development requires the survey process. The Survey process is needed to get the requirement for the software. The Survey also consists of studying the present system and also studying about the tools needed for the development of the software. A proper understanding of the tools is very much essential. Following an extract of the information of the immaterial collected during literature survey.

In this paper, an introductory look at information hiding techniques and historical details is discussed. Several methods for hiding data in audio, image is described with appropriate to environment of each medium as well as strength and weakness of each medium. The information about secret key, transmission protocol, computer file system, hiding techniques are discussed.

In this paper, the different types of steganographic methods its pros and cons are discussed n detail. It gives information about efficient method for sending safely to this destination. The use of steganography application is to hide different types of data within cover file. This is done according to the embedding algorithm and a secret key that performs the actions of embedding process.

In this paper, the image data embedding scheme is proposed. We can replace one or more LSB of each pixel in image frame. It becomes very difficult for the intruder to guess the data hidden in a frame. An advanced data hiding method by using different bit with help of LSB substitution is proposed and analyzed.

In this paper, it explains the prime need of hiding data from eavesdroppers is accomplished by the use of steganography. It explains about the wide researches that have been carried out on image steganography due to high

 

capacity of information been stored in image file. This paper presented using LSB insertion which is very efficient method to embed data into a cover medium. It has explained the LSB insertion method for image steganography and its application.

In this paper the focus on the data security approach with combined encryption and steganographic techniques for secret communication by hiding it inside a multimedia files is done. The file such as images, audio, image contains collection of bits that can be further translated into same. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This paper explains the proposed algorithm using image steganography for enhancing data security.

In this paper, the explanation on combination of cryptography and steganography is used for data hiding in image clips. A random frame selection, pixel swapping, and encryption of message has been done to enhance security of secret information which goes under the cover of image clips. Image steganography method has been developed to transfer secret data.

In this paper, the modern secure image steganography presents a challenging task of transferring embedded information to destination without being detected. Here, a simple approach for embedding message into image or the image from pixel of carrier image is replaced with message information so that it cannot be observed by human visual system, therefore exploits some limitations of human visual system.

## III. METHODOLOGY

An Image can be viewed as a sequence of still images. Data embedding in image seems very similar to images. However, there are many differences between data hiding in images and images, where the first important difference is the size of the host media, since images contain more sample number of pixels, an image has a higher capacity than a still image and more data can be embedded in the image.

In the process of hiding the secret data in the image which acts as a cover carrier, that secret data will be encrypted using AES Algorithm. The AES algorithm is most secure and robust cryptographic algorithm against attacks. AES has a symmetric block cipher and hence uses same key for encryption and decryption. After the encryption the data is divided into number of chunks, these chunks will be given to the LSB technique, by this technique the chunks will be placed in the marked frame.

The overall process is divided into two parts i.e. sender and receiver. When sender wants to send the secret data, he will register to the access and extract the image file along with the secret data. The secret data will be encrypted using AES Algorithm while sending an image i.e. stego image. The encryption key will be generated at the time of sending. The authorized receiver can only access the image file with the help of encrypted key. If the encryption key is invalid image will be destroyed automatically.

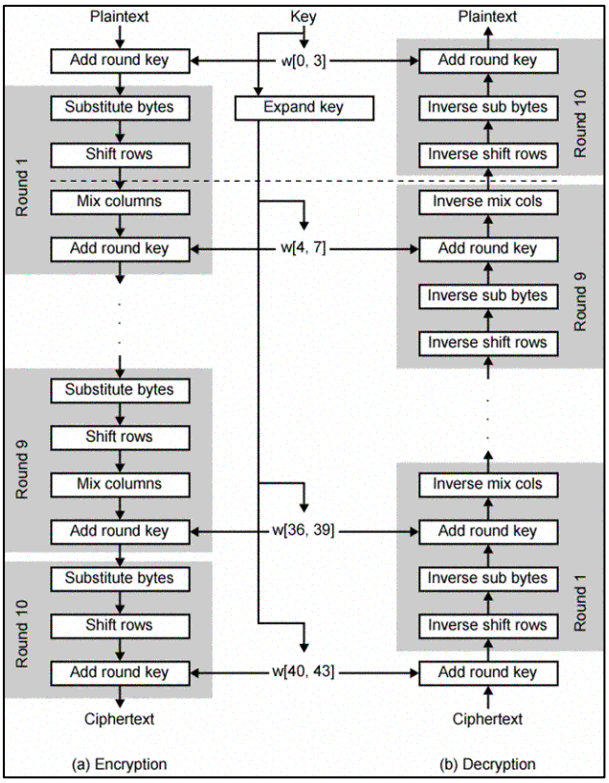


Fig. 1: Proposed System

### A. *System Flow*

In figure 2 Admin, Teacher and Student must register to the application first which creates account for further access. The concept of this project is to intimate the teacher about the progress of every students which helps teacher to give attention equally for distinction student, average student and even for poor student in the class. This concept comes in to picture by generating report which is available after giving test for students. Students must enroll themselves in the tests that is given by teachers which helps them to judge students on their progress Admin role is to make sur e that every process is carried on exactly the way it is designed

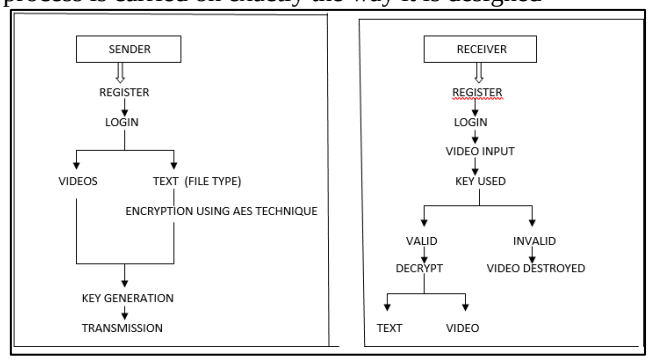


Fig. 2: System Flow

### B. *Advantages are*

- Manual work.
- Manual way of identifying performance.
- Data Analytics was a tedious job.
- Manual work for a data management.

## IV. FUTURE ENHANCEMENT

Future Work may be further enhancement of results by applying some other algorithm than used in this thesis. We can also take two images as input and can embed secret message in both. Other quality metrics can be used to judge the performance of the algorithm.

## V. CONCLUSION

A comprehensive review of image steganographic techniques. Difference between steganography, cryptography, and watermarking were discussed. An overview of steganography using different cover types was presented and special attention was paid to image steganography and its applications. Various categorizations of the existing techniques were illustrated. We adopted a categorization according to the domain of embedding, in which methods are categorized into three categories: Spatial domain techniques, transform domain techniques, and other techniques. Techniques belonging to each domain were discussed and comparisons between those techniques were presented highlighting their advantages and disadvantages. Furthermore, popular image and image quality metrics available in the literature were discussed. Finally, steganography was surveyed from the point of view that improves the design of good steganographic systems. Based on this review, the following recommendations may help interested researchers in image steganography.

## REFERENCES

[1] "Programming C#, Fourth Edition- Building .NET Applications with C#"By Jesse Liberty
[2] "Working With Microsoft Visual Studio 2005 Team System" By Richard Hundhausen
[3] "Begin ASP.NET 2.0 with visual C#.NET", Wrox, By Chris Ullman.
[4] Software Engineering, Ian Summerville, Sixth Edition, Pearson Education Ltd, 2001

### *A. Referential URL's:*

[5] http://msdn.microsoft.com/asp.net
[6] http://www.csharphelp.com
[7] http://www.w3schools.com
[8] http://www.dotnetspider.com
[9] http://www.csharpcorner.com
[10] http://www.codeguru.com

 