# DATA SECURITY OVER RANDOM VIDEO IMAGES USING STEGANOGRAPHY

**Author :D.S.KEERTHANA**
**Email id: : keerthanadharmaraj01@gmail.com**
**Department of computer science and application**
**Sri Krishna College of arts and science**

**Author: A.ABDUL FAIZ**
**Assistant Professor**
**Email id : adbulfaizaa@skasc.ac.in**
**Department of computer science and application**
**Sri Krishna College of arts and science**

**ABSTRACT**

*Video Steganography is the process of hiding some secret information inside a video generally, in data hiding, the actual information is not maintained in its original format. The format is regenerate into another equivalent transmission files like pictures, video or audio. This in turn is being hidden within another object. Multiple random video Steganography is the process of hiding some secret information inside a video. The addition of this information to the images is not recognizable by the human eye as the change of a pixel color is negligible. This project aims to provide an efficient and a secure method for Video Steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the images itself. With the assistance of this index, the frames containing the key info are situated Hence, during the extraction process, instead of analyzing the entire images, the frames containing the secret information ar analyzed with the assistance of index at the receiving funish.*

*When steganographed by this technique, the chance of finding the hidden info by associate wrong doer is lesser when put next to the traditional technique of activity info frame-by-frame in a sequential manner. It conjointly reduces the machine time taken for the extraction method.*

## INTRODUCTION:

The word Steganography was originated from the Greek words "stegos" symbolic worth is "cover" and "grafia" symbolic worth is "writing" meaning is "covered writing". It is a field of concealment secret data during a concealing media. The secret message is being hid during a audio wave enter a precise method so the incidence of the message remains unidentified to the one UN agency makes observations. A systematic arrange behind Audio wave Steganography method is to hide the hidden text message in an associate audio wave known as carrier audio wave. The audio associate in nursing outcome when this method is termed stego audio, that is send to the receiver from a channel that is free from attack. At the cryptography aspect audio wave is changed to extract secret text message from it by the act of applying a secret key.

There area unit an oversized variety of alternative steganography techniques that area unit in repetition of late for improvement, amidst that Text, image and Video Steganography area unit common.

The actual existence of this paper is to send secret message in associate degree audio wave and check the protection and security of the audio wave by doing spy analyses
which embrace Signal to Noise magnitude relation take a look at and exposure analyses.

## EXISTING SYSTEM:

There are various approaches for information and data security to achieve secret communication. There are many existing works related to steganography, which includes audio steganography. The existing methods were used LSB (Least Significant Bit) technique for hiding secret data. But the least bit stganography is always can be detected and not much protected. Due to this problem, image steganogaphy failed in many applications. Another problem of the existing technique is the quality of the image can leak the hidden information in the image.

## DRAWBACKS:

- Data can be easily leaked.
- Data loss
- Quality of the images were affected

**PROPOSED SYSTEM:**

In the proposed system a fresh unique scheme of data hiding images is presented with random bit selection, where the application select image as a carrier medium and select random pixels RBS which is abbreviated as random block steganography to hide the data rather than the sequence least bit. Using the proposed system, the secret data can be embedded in the image without quality degrades. The data owner selects the original text content and embeds the data into the images using standard randomized ciphers with hash keys to produce the stego images.

**ADVANTAGES**:

- High security
- The hacker cannot able to retrieve the data without the key
- Reliable and effective
- Doesn't affect image Quality

**LSB (LEAST SIGNIFICANT BIT)**

Least vital Bit is one amongst technique in steganography.LSB could be a wide used as steganography algorithmic rule.LSB utilizes the proper way little bit of the computer memory unit array that compose pixels in a picture file.

In the order of bits in a very computer memory unit, there square measure bits known as LSB and a few square measure known as savings bank. Steganography technique using Least Significant Bit (LSB) modification method is the simplest technique, simple approach to insert information in a digital image (medium cover). Convert **a picture** from GIF or BMP format, which reconstructs the same message as the original (lossless compression) to JPEG that is lossy compression, and when it is done it will destroy the hidden data within the LSB.

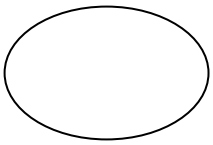
The LSB bit becomes the place wherever the bit price of the binary arrangement of associate degree data is inserted, as a result of the modification within the price solely changes one bit higher or 1 bit lower than the previous value. So, once the computer memory unit values modification, the changes that occur within the component won't be too substantive.

The LSB algorithmic rule utilizes the weakness of the human eye to ascertain terribly tiny color changes.

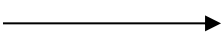
**DATA FLOW DIAGRAM**

DFD depict hoe data interact with the system. DFD are extremely useful in modeling many aspects of a business function because they systematically subdivide a task into basic parts, helping the analyst understand the system that they trying to model data flow diagram models a system by using external entities from which data flow to a process which transmission the data and creates output data which goes to other processes on external entities of files. Data may also flow to process as inputs.

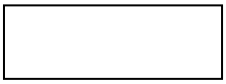
The symbols appearing in the DFD has been explained below:



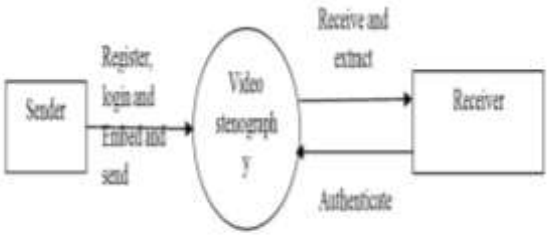
- Represents a process



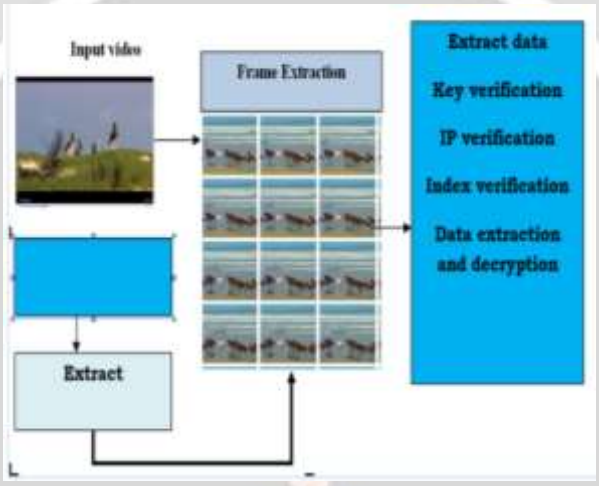
- Which shows data

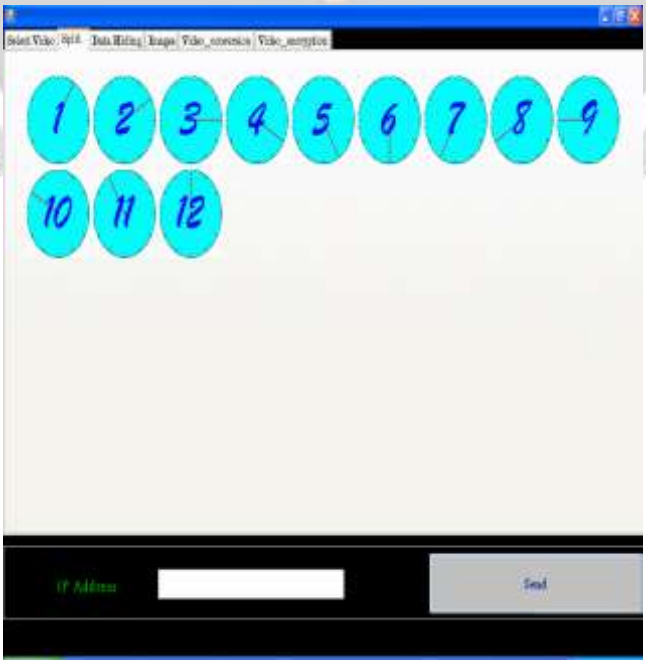


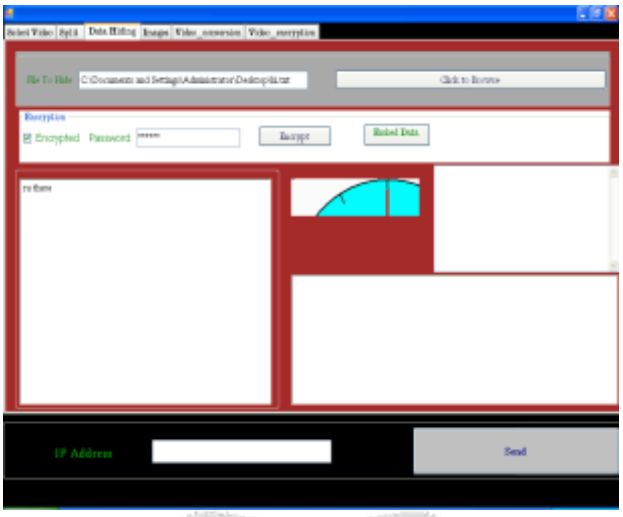
- Designation of the data

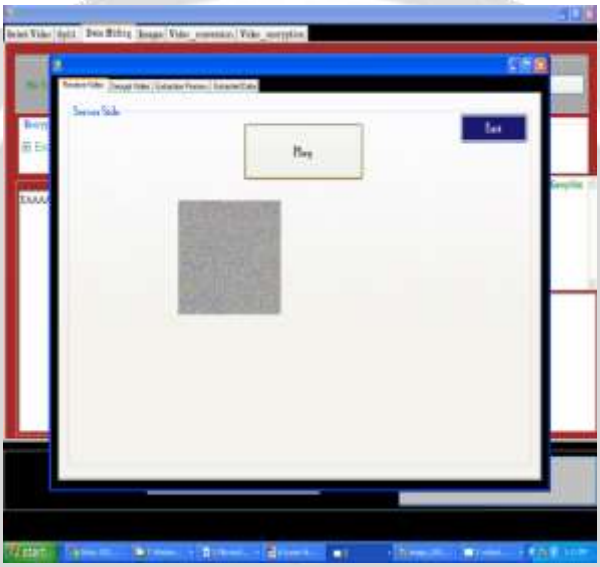



**EXTRACTION PROCESS**







## CONCLUSIONS:

a. LSB is one technique that may be accustomed insert info in a picture.
b. the scale of the message doesn't exceed the scale of the duvet image.
c. The larger image resolution, the larger message or info is inserted.
d. RGB pictures will hold additional info or messages than with Grayscale pictures of an equivalent resolution.
e. the information antecedently encrypted exploitation vigenere when extracted from the stego image can then be processed once more.
f. variations within the use of vigenere cipher coding is once the message before it's inserted (plaintext) and when it's extracted (ciphertext).
In the insertion method is that the same because the usual LSB methodology.

Future analysis is anticipated to use cryptography not solely restricted to at least one methodology solely. Rather it can be applied some cryptographic methods that make messages or information more secure even though messages embedded in a media can be extracted by irresponsible parties, but the information they really get isn't actual, however the encrypted info.

## REFRENCES:

[1]. K. Stefan, P. Fabien A.P., "Information Hiding Techniques for,Steganography and Digital Watermarking" , Artech House , London, 2000.
[2]. Cox, Ingemar J., "Digital Watermarking and Steganography", Burlington, Morgan Kaufmann Publisher, 2008.

[3] TanmyBhaowmik, PramathaNathBasu, "On Embedding of text in Audio – A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and computing, IEEE 2010.
[4] Ashis Kumar Mandal, Mohammed Kaosar, Md. Olioul Islam and Md. DelowarHossain, "An Approach for Enhancing Message Security in Audio Steganography", IEEE 16th International Conference on Computer and Information Technology, 8-10 March, 2014.