# Data Security Using Steganography Through Media Files

Burri Yaswanth Sai[1], Kolli Greeshma[2], Gorijavolu Sai Keerthi[3], Meer Kamal Arif[4], Mr. B. Dasaradha Ram[5]
[1,2,3,4] Student, Department of CSE, NRI Institute of Technology, Vijayawada, A.P., India.
[5]Associate Professor, Department of CSE, NRI Institute of Technology, Vijayawada, A.P., India.

***Abstract***

Although cryptography and steganography can provide data security, each of them has a problem. The problem with cryptography is that the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. In steganography, once the presence of hidden information is revealed or even suspected, the message becomes known. According to this paper, a merged technique for data security is proposed using both cryptography and steganography techniques to improve data security. Therefore, two levels ofsecurity will be provided using the proposed hybrid technique. In addition, the proposed technique provides high embedding capacity and high-quality images and videos.

Cryptography means encrypting the message using a symmetrickey and decrypting the message using the samekey. Steganography is the art of hiding the fact that communication takes place by hiding the information in other media files. So, encrypting themessage and hiding that encrypted message in the media file is called double security providing. This project hides the message in the media file.

## *I. Introduction*

Data Security using Steganography through Media Files is a Standalone application having the functionality of hiding secret information. This application uses both the concepts of Cryptography and Steganography. The Symmetric key concept is used in this application. Before hiding the secret information in the media files, the user needs to register/login to the application. The following are the functionalities of the application-

- Login/Register:

User Registration is the first step in the application. After User Registration, the user needs to login to the application with the username and password. After logging in to the application, the User can hide and retrieve data to/from media files.

- Embed Data in Image File:

The Embed Data in Image File is the functionality to hide the information inside the Image File. Initially, the data is encryptedand then the encrypted data will be hidden.To hide data in an image file, the user needs to select the Master Image File which the data needs to be hidden, and also the user needs to select the output folder in which the image will be saved. And finally, the user needs to give the secret information.

- Embed Data/Image in Video File:

In the video file, the user can hide both the text data and the image file. The image can be directly hidden in the video file but the text data needs to be encrypted before hiding. To hide image/data, initially,the user needs to select the Master Video file and the image/data which needs to be hidden, and the output folder in which the output file is located after hiding the data.

- Retrieve Data from Image File:

The Retrieve Data functionality is the reversible process of embedding data in the Image file. To retrieve data from the Image, the user needs to select the Stego-image and need to enter the symmetric key correctly. The hidden data will come as the output which was hidden by us.

- Retrieve Data from Video File:

In this, the data/image which is hidden in the video file can be the result as output. It also has the same functionality as the Retrieve Data from Image File but only the change is the Master Video File and output of the process. To retrieve data, we need a Stego-video file in which data is hidden.

## *II. Existing System*

Mostly security-based applications are completely based on Cryptography or completely based on Steganography. Cryptographic applications provide single-layer security. It means Encrypted data can be hacked or decrypted with enough time and computing resources, revealing the original information. Hackers prefer to steal encryption keys or intercept data before encryption or after decryption. The most common way to hack

encrypted data is to add an encryption layer using an attacker's key. And the Steganographic application means hiding data in the image. There is a chance of extracting information from these Stego-images as well.

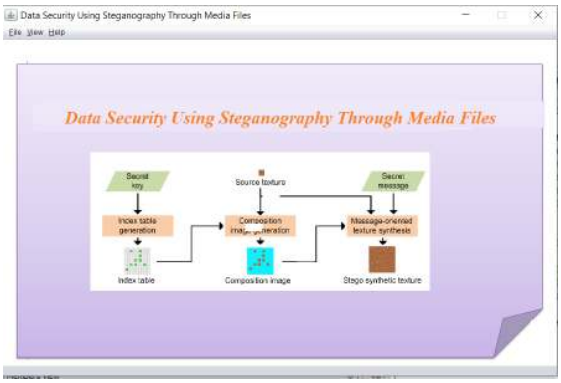
### *III.* Proposed System

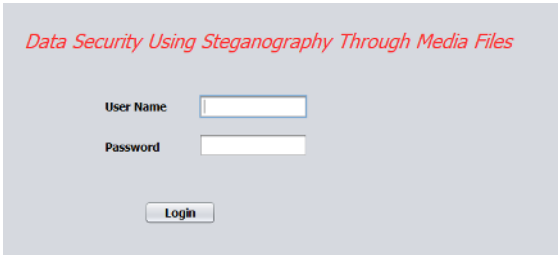
Data Security using Steganography through Media Files is the proposed system which uses both the concepts of Cryptography and Steganography as a combined unit. This proposed system is a standalone application in which every user can access it by logging in.In the proposedsystem,Video Steganography is also introduced in which the image or text file can be hidden in the Video file. In the proposed system, it provides double security for the data. Double security can be achieved by using both Cryptography and Steganography. In this application, initially, the given secret information can be encrypted and then can be hidden in the image. This process is called Double Security. And in the case of Video steganography, the image can be hidden directly and in case of hiding the text, the text will be encrypted and then hidden into the Video file. While encrypting the data it takes a key of length8which consists of letters and digits called Symmetric key. After the completion of hiding the data, the extraction of the same data is the reversible process of hiding. It involves data extraction from Stego-file and decrypting the data it has. In the proposed system, the user can compress the Stego-image if the user wants.

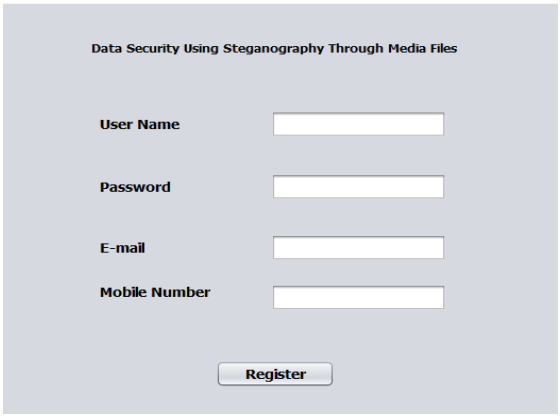
### *IV.* Implementation (Modules)

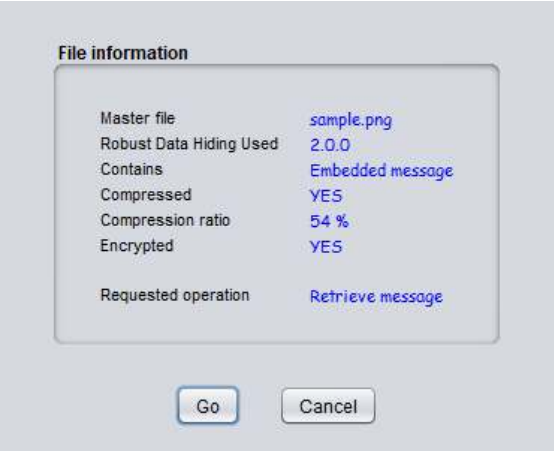
Data Security Using Steganography through Media Files is implemented using a Cryptographic algorithm Data Encryption Standard and also using some Steganographic methodologies. DES is used to transform the original data into encrypted data. Then this encrypted data will be hidden into media files using Steganography methodologies. Thus, data can be encrypted. The Decryption of the data can be done by extracting the encrypted initially and then the encrypted data can be converted to normal data. In the case of Video Steganography, directly the image file can be hidden using the steganographic methodologies and a symmetric key is used for security.

### Sample Screens




## *V. Conclusions*

Today, we are at the age of modernization, and we should prepare for the changes that will occur in the next few years. A change in providing security to secret information will be shocking and can be possible with the right approach.

Security is an important issue while transferring the data using the internet because any unauthorized individual can hack the data and make it useless or obtain information un-intended to him.

To avoid these threats, this application provides double security for data using cryptography and steganography. It provides secrecy by adding a symmetric key concept to the application.

Therefore, by using this Standalone application every user can hide the data in the media files and also hide the existence of the communication.

## *VI.* Future Scope For Further Development

As time passes, new machines will be introduced into different sectors and industries. Providing security to the user's data will play a pivotal role.

Extracting the data from the image which is hidden in the video file is Nested Extracting. This can be done by using consecutive algorithms of Steganography.

More than one system can be accessing the other systems present in the LAN. By accessing which, one user can hide the data and the remaining users can access the hidden data if the key is known.

1. It is evident that by controlling the air flow rate we can govern the heat transfer.
2. Here the performance of the fin is evaluated using lowest temperature recorded and low range of fluxes.

## *VII.* References

[1] Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

[2] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.

[3] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," International Journal, vol. 4, no. 10, 2014.

[4] M. K. I. Rahmani and M. A. K. G. M. Mudgal, "Study of cryptography and steganography system," 2015.

[5] N. Khan and K. S. Gorde, "Data security by video steganography and cryptography techniques," 2015.

[6] https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf

[7] https://arxiv.org/ftp/arxiv/papers/1009/1009.2826.pdf

[8] Provos, N. & Honeyman, P. (2003). Hide and seek: An Introduction to Steganography, IEEE Security and Privacy Magazine.

[9] https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/