

# A Novel Approach of Encrypted Video Steganography

T.Venkat Narayana Rao<sup>1</sup>, M.Likhitha<sup>2</sup>, A.Anukritha Reddy<sup>3</sup>, K.Sravani<sup>4</sup>

<sup>1</sup>Professor, <sup>2,3,4</sup>Student, Dept. of Computer Science and Engineering

Sreenidhi Institute of Science and Technology,  
Hyderabad, Telangana, India.

**Abstract:** *Steganography is immediate need of today's world due to want for of privacy in modern age. It is an essential system to hide a secret information within a digitally covered media which can be either a text, an image, an audio or a video in a way that the data embedded in it is transmitted secretly and securely. The hidden message can be image, text, speech (audio) or a video. The existing scheme of using image as a cover media has a restriction of embedding dimension. This paper implements a video as a cover media to overcome the limitation of embedding dimension. The proposed scheme uses a complete Java language based approach for both encryption and embedding processes. The concealed message is first encrypted by XOR and shifting the bit positions of the data file along with the key followed by split and swap operations to ensure double encryption, later it is embedded on the cover media in a way that the video do not mislay its functionality. By this process, the possibility of finding the hidden information by the attacker is slighter as compared to the standard method of hiding information frame-by-frame in a sequential approach. It also reduces the computational time taken for extraction process.*

**Keywords:** *Steganography, encryption, embedding, de-embedding, decryption, stego video.*

## I. Introduction

Today, majority of the cyber-crimes and frauds are due to lack of proper protection to sensitive data. Preserving the secrecy of confidential information has its own importance in almost all the branches of computing from storing a simple file on an external disk to transferring a complex blob file across various protocols on the network. While cryptographic techniques are used to protect sensitive data, steganography serves a different purpose. It is considered as a dark cousin of cryptography because steganography focuses on ensuring secrecy unlike cryptographic techniques that assure privacy [2][6].

Considering an example such as sending of credit card details over the internet which involves risk of being infected with a malicious content. Using Cryptography such sensitive data is randomized or confused and hence is not revealed. Steganography is an task of hiding the messages in a harmless data medium in a way that an attacker cannot even sense the presence of some secret message. Steganography provides an added gain to the already encrypted data by hiding the confidential data itself. An unhidden coded message, no matter how unbreakable it is, will provoke suspicion and may incriminating, as in some countries encryption is prohibited. Therefore, steganography plays an important role by limiting the attention to sensitive data and thereby keeping it a secret [1][3].

## II. Existing System

The sole purpose of steganography is to make sure that the attacker or the hacker is unaware of the existence of the secret message in a cover media but once the enemy comes to know about the confidential data hidden in it, then the security of the secret message is compromised and thus the purpose of steganography is violated. There are many techniques which serves the purpose of steganography but the existing systems lacks good user interface, non-provision of choosing the key and more encode-decode time consumption. There are plenty of steganographic programs available. A few of them are excellent in every respect; unfortunately, most of them lack in interfaces, or contain too many bugs, or unavailability of a program for other operating systems. The existing system till date is based on video Steganography for hiding data in video image, retrieving the hidden data from the video are LSB (Least Significant Bit) and DCT (Discrete Cosine transform) modification methods. The proposed application will take into account these shortcomings, and since it will be written in Java, operability over multiple operating systems and even over different hardware platforms would not be an issue. This proposed method provides easy way 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. The proposed design is completely based on Java which ensures three prime factors : a) the length of the key is increased significantly for any given user defined key (more the length of the key, more the security) b) Double encryption techniques and c) securely embedding

the encrypted data in the cover media i.e., video [1][4][6].

**Existing Method of Concealing Data:**

**1) Least Significant Bit (LSB):** LSB is the lowest bit in a series of numbers in binary. For example in the binary number: 10110001, the least significant bit is far right. The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in the cover media [5].

**2) Discrete Cosine Transform (DCT):** Initially, the video is streamed and use bitmap format for all the frames are collected from the video. Now, each frame acts as an image and the DCT coefficients are used for embedding of data these images. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components [3][8].

**III . Basic Design**

The detailed description for encryption and embedding process of the proposed system is illustrated in the block diagram shown in figure 1(a), the de-embedding process and the decryption The extracted data is explained as shown in figure 1(b).

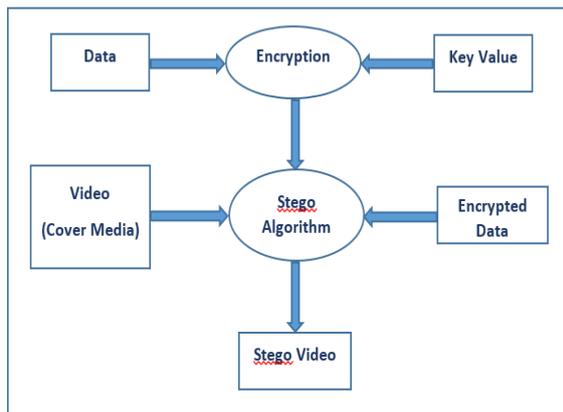


Figure 1(a): Embedding of encrypted data

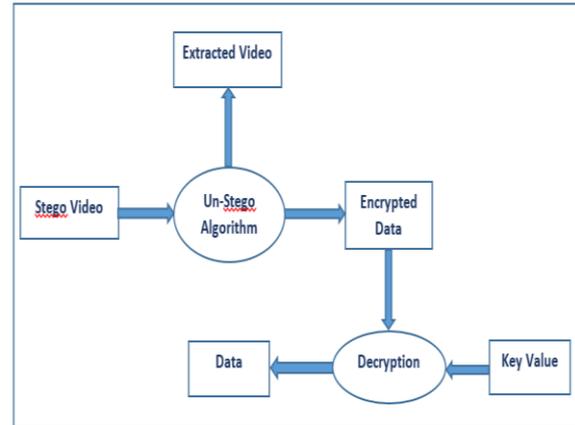


Figure 1(b): De-embedding followed by decryption

**IV. The Proposed System**

Encryption software protects internet connected computers from crackers and other on-line intruders. The technology is widely used to encrypt credit card information, bank account numbers and other type of financial records so they could send safely and securely across the internet. Protect much of the intellectual content that is marketed on the web, such as music, videos, articles, software, billing the customers appropriately. This system helps to conceal the information while sending the vital and secret documents in video files that is invisible for the third person. This system is helpful for the defense and security departments in sending and receiving the confidential matters in emergency situations [7][9].

The proposed system also follows a analogous approach of combining video steganography and encryption techniques together but in a different way, to form a highly secure shell to our confidential data. Even if the attacker senses the presence of data, he/she cannot modify or access the data as the information is first encrypted based on a custom user defined key and then embedded behind a cover video as given in the equation below. The main objective of this system is that to avoid drawing suspicion to the transmission of hidden message. The goal of cryptography is to make data unreadable by a third party, the goal of stenography is to hide the data from a third party through the use of advanced computer software, creators of images and software can place a hidden trademark in their product, allowing them to keep a check on piracy. This is commonly known as watermarking. Hiding serial numbers or a set of

characters that distinguishes an object from a similar object is known as finger printing. Together, these two are intended to fight piracy. The latter is used to detect copyright violators and the former is used to prosecute them. But these are only examples of the much wider field of steganography [8][12].

## V. Implementation of the System

The video steganography software performs the process of conceal and disclose in the following modules. The modules of video steganography are:

- Graphical User Interface (GUI)
- Key Streaming and Scrambling
- Symmetric Encryption
- Steganography – Conceal data
- De-embedding or de-steganography
- Decryption

### A. Graphical User Interface (GUI)

As the design is developed completely using Java, Netbeans IDE is chosen to develop. Java Swings and AWT are used to provide a GUI in a user friendly way. It even does not need any previous training to operate and aid user to do encrypted steganography. This will help user with a wizard to:

- Hide a message in a video file
- Retrieve the hidden message in a stego video
- Encrypt a text file
- Decrypt the encrypted file.

### B. Key Streaming and Scrambling

In Key Streaming and Scrambling, the user is requested to enter a key for encrypting a required secret file. There is no restriction on the length of the key and also different combinations of characters and digits can be chosen. Here the user need not necessarily give the key of more length. The above equation is used to increase the length of the key without any user intervention. Later, the

$$(key.length()*key.length()+* key.length())*128$$

increased key is again scrambled randomly. The main goal of streaming and scrambling the key length is to ensure more security.

### C. Symmetric Encryption

The message to be hidden inside the carrier file is encrypted along with a key to disappoint the prying

eyes of intruders. This is to enhance the security during data transmission. This strong encryption method provides robustness to the stego machine [10]. In this module, the input message is first converted to byte value. The key is obtained from the user which is added to the respective byte and stored in a separate byte array which is then converted into character to get the encrypted form of message as shown in Fig 1 (a). The input to this function can be a plain text message, image file, audio file and also video file along with a key value to encrypt the message. Table 1 illustrates the complete encryption process is based on Split, Swap and XOR process.

TABLE 1: XOR ENCRYPTION BIT LOGIC

Message bit	Key bit	Encrypted Value (XOR)
0	0	0
0	1	1
1	0	1
1	1	0

### Encoding

Message Value: 01011101

Key Value: 00001111

XOR Value: 01010010

### Split and Swap

XOR Value: 01010010

Split Value: 0101-0010

Swap (Encrypted) Value: 10100100

### D. Steganography – Conceal data:

This module performs the task of steganography. In the existing system it was necessary that the video has to be divided into number of frames where each frame acts as an image. The encrypted data is then embedded into the extracted suitable frame. Later all the frames are again recombined to obtain the original video. But in the proposed system the cover media video (AVI, mp4 etc) is not divided into frames rather it is extracted directly in the form of bytes. As shown above the data bytes of the encrypted file are randomly combined with the video bytes and are stored in another byte

array. The original video is deleted and the embedded array is now made as the original video file. The embedded video file now obtained and the original video file chosen resemble the same in all frames. By doing this the attacker perceives the embedded video to be original video file. Hence, the output of this process i.e., stego-video is now safe and secure from any attack and can be transmitted across a secure channel to the receiver. By following this approach there is no need to diving or combines the video frames. Thus, the computational time of embedding and de-embedding also reduced [5][11][14].

**E. De-embedding or De-steganography**

The embedded video i.e., stego-video is de-embedded in this module. De-embedding is complete reverse process of embedding. In embedding process, the encrypted bytes and video bytes are combined together. But in this process, both encrypted data bytes and video bytes are separated. As the video is not divided into frames, only the data bytes are separated from the video byte array. The video bytes remain as same without causing any effect to the cover video. After the bytes separation, only the encrypted data bytes are stored in a separate file to perform decryption.

**F. Decryption**

The hidden encrypted message obtained after de-embedding is decrypted using the same key used in the encryption process. The decryption process is reverse process of encryption. The input to this function is the encrypted message file and a key value to decrypt the message. This module first converts the input encrypted message into byte value. As shown in table 2, Split and swap operations are performed on the data bytes. Later XOR transformation is applied on the swapped bytes to obtain original data. The decrypted value is same as the original value.

**Split and Swap Process**

Encrypted Value:	10100100
Split Value:	1010-0100
Swap Value:	01010010
Decryption	
Swap Value:	01010010
Key Value:	00001111

Re-XOR (Original) Value: 01011101

**Table 2: Re-XOR Encryption Bit Logic**

Encrypted Value (XOR)	Key bit	Decrypted Value (Original)
0	0	0
1	1	0
1	0	1
0	1	1

**VI. Parameters and Performance Metric**

Steganography applications are evaluated on some basic criteria. The criteria upon which the performance of such applications is evaluated are Robustness, Capacity, and Security. These performance evaluation criteria are independent of each other [9].

**Robustness** refers to the ability of the system to withstand various attacks and modifications of the application. It clearly describes the quality of the application. In this regard, the quality of the original video is judged with the quality of the stego video. The parameter used to demonstrate the robustness performance of the application is Peak-Signal- to -Noise -Ratio (PSNR). PSNR is a video quality measure by comparing the original video to the stego-video. The unit of measurement of PSNR is decibels (dB) [12][13]. The higher the PSNR value, the higher the video quality the video. PSNR value computed as :

$$\begin{aligned}
 PSNR &= 10 \cdot \log_{10} \left( \frac{MAX_I^2}{MSE} \right) \\
 &= 20 \cdot \log_{10} \left( \frac{MAX_I}{\sqrt{MSE}} \right) \\
 &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE)
 \end{aligned}$$

MSE is the Mean Square Error which is the measure to resolve the distortion between the original and the stego-video. MSE is calculated using:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

where M and N are the height and the width of the video respectively.

**Capacity** which is mostly referred as embedding capacity or payload capacity is the amount of data that can be embedded or hidden in a cover object without the quality of the video deteriorating statistically or without causing statistically significant modification. Capacity is expressed in terms of bits per pixel whereas the maximum hiding capacity is expressed in term of percentage.

$$\text{Capacity} = \frac{\text{number of bits used to hide data}}{\text{total number of bits in image}} \times 100\%$$

**Security** is the capability of an unauthorized person or a third party to discover or detect hidden information or message in a video. This criterion is purely demonstrated by the embedding algorithm and the encryption algorithm used [10][12].

In this study, five cover videos were analysed with a common text file. The resultant invisibility of the hidden file is shown by comparing the stego-video with the cover video. There was virtually no loss in quality and also the presence of a hidden message in the video has been proven to be undetected.

The MSE is a mean square error between the cover frame of the original video and the cover frame of the stego-video. Different values of PSNR are listed to exhibit the video quality based on the cover image and the hidden file chosen. The process has exhibited high PSNR value that indicates the higher quality of the video and thus the security of the stego-video is also very high as shown in table 3. From table 3 it is observed that, as the MSE value increases, the PSNR value decreases [11][13].

**Table 3: Results and Findings**

Original Video Frame	Embedded Video Frame	MSE Value	PSNR Value
		0.0599	60.356
		0.0298	63.388

		0.0410	62.003
		0.0899	58.593
		0.0698	59.692
Average PSNR Value: 60.8064			

As shown in the table 3, it is observed that the average PSNR value computed for all the video frames is 60.8064. A PSNR value which is greater than 50 indicates a better video quality [8].

## VII. Conclusion

The proposed system eliminates the need for multiple applications to encrypt, embed, de-embed and decrypt the data as the proposed method incorporates all the modules in a single application. It ensures that the user’s data is safely hidden in the video file thereby creating a shell around sensitive information. The process to de-embed and decrypt the secret data is equally consistent and effective. In summary, this system is built to be highly portable and can be used irrespective of platform without compromising with any of the video features.

## References

- [1] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, —Information Hiding—A Survey, Proc. IEEE, 1999.
- [2] Niels Provos and Peter Honeyman, —Hide and Seek: An Introduction to Steganography, University of Michigan, IEEE 2003.
- [3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, Application of LSB Based Steganographic Technique for 8-bit Color Images, WASET 2009.
- [4] Sutaone, M.S.; Khandare, Image based Steganography using LSB insertion technique, IET, 2008.
- [5] Mazdak Zamani, Azizah A. Manaf, and Shahidan Abdullah, —A Genetic- Algorithm-Based Approach for Audio Steganography, WASET 2009.
- [6] Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, —Implementation of LSB Steganography and Its Evaluation for various Bits, Digital Information Management, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349.

- [7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series.
- [8] Neil F. Johnson, Duric, Z., Jajodia, S. Information Hiding Steganography and Watermarking Attacks and Countermeasure. Kluwer Academic Press. Norwrl, MA, New York, The Huague, London vol 32.8(2010) 79-94.
- [9] Neil F. Johnson and S.Jajodia Exploring Steganography. Seeing the Unseen, IEEE Computer, vol. 31.2 (2009) 26 - 34.
- [10] Min. Wu Joint Security and Robustness Enhancement for Quantization Embedding. IEEE Transactions, vol 0-78037750-8/03 (2009) 483-486.
- [11] C. E. Shannon A mathematical theory of communication. Bell System Technical journal, vol. 27 (1948) 379-423.
- [12] G. J. Simmons The prisoners' problem and the subliminal channel, in Advances in Cryptology. Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press vol 12.9(2010)51-67.
- [13] Ashish T. Bhole, Rachna Patel, "Design and Implementation of Steganography Over Video File", The Indian Journal of Technical Education, Special Issue for NCEVT' 12, pp. 69-72, April 2012.
- [14] Ashish T. Bhole and Rachna Patel, "Steganography over Video File using Random Byte Hiding and LSB Technique", International Conference on Computational Intelligence and Computing Research, pp. 189-194, 2012 IEEE.