# Steganography in Audio/Video files using Modified F5 Algorithm

Amol Khedekar
B.E. Computer Engineering
Viva Institute of Technology
Mumbai

Aakash Ilag
B.E. Computer Engineering
Viva Institute of Technology
Mumbai

Pooja More
B.E. Computer Engineering
Viva Institute of Technology
Mumbai

Tatwadarshi P N
Assistant professor
Viva Institute of Technology
Mumbai

## ABSTRACT
Today's large demand of internet applications requires data to be transmitted in a more secure way. The transmission of data in public communication system is not secure because of been used throughout history. Audio steganography is the scheme of hiding the existence of secret information by suppressing it into another medium such as audio file. The first input is an audio/video files whose audio/video samples, which are used to suppress the hidden data. Whereas, the second input is a grammatically interception and improper manipulation by attacker. So the best solution for this problem is Steganography. Steganography is an effective method of hiding data that has correct text. Then it encodes the location of the random audio samples in the audio file. The proposed technique of modified F5 algorithm provides a secure way for data transmission that it is difficult for unauthorized user to detect the presence of and recover the secret data. It will also help in the transfer of the information from one machine to another machine.

## Keywords
Steganography, Messaging, Secure communication, Audio/video files, Modified F5 algorithm.

## 1. INTRODUCTION
Steganography is an art of sending hidden data or secret messages over a public channel so that an unauthorized user cannot detect the presence of the secret messages[3]. Steganography is method of embedding textual information in an audio file, images or in video files. The term hiding refers to the process of making information imperceptible or keeping existence of information secret.
Embedding information into 'audio/video' seems more secure due to less steganalysis technique for attacking to audio. Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stegokey. Steganography is implemented using some of algorithms such as Least Significant Bit (LSB), Echo-hiding, Direct Sequence Spread Spectrum (DSSS), etc. Audio steganography is the scheme of hiding existence of secret information by concealing into another medium such as audio file[7]. This paper proposes audio steganography using 'Modified F5 algorithm' which provides more secure way for data transmission and reliable as compact to other algorithms. This paper will basically implement the steganographic technique of hiding the data or information behind the audio/video file. It will also help in the transfer of the information from one machine to another machine. The main aim of this paper will be the data security aspect.

## 2. RELATED WORKS
There are many algorithm developed for image steganography. Meanwhile, the interest in using audio data as cover object in steganography is more reliable than image data[9].This paper describes the implementation of steganography in audio data using direct sequence spread spectrum method. Modified F5 can be applied to embed message in audio/video data & to send hidden message through radio waves. Spread Spectrum method is known very robust, but it is expensive, the implementation is comparatively complex and the information capacity is very limited [2].

A perfect audio steganographic techniques aim at embedding data in robust way and then extracting it by authorized people. Hence the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. In this paper, a current state of art literature in digital audio steganography is presented. The potentials and limitations have been identified to ensure secure communication [4].

Till now in steganography the hidden or secret text message is firstly stored in an image and then that image has been send to the user with the help of audio, But this process is too lengthy because there is an involvement of image and audio also. LSB is one of the most widely used algorithms for audio steganography. This method permits high embedding capacity for data and is relatively easy to implement. But this technique is characterized by low robustness to noise addition and hence it is less secure and very vulnerable even to simple attacks [11].

Later on another technique was introduced and implemented named as Echo Hiding in which data is embed into audio signal by introducing short echo to the host signal. This method still has some issues in data transmission, since there may be chances to get add additive noise [5].

Taking all those issues into consideration and to some extent solve such problems this paper presents a more secure, robust and reliable algorithm named as Modified F5. This paper is focused on working of Modified F5 algorithm and applications of this algorithm to achieve secure data transmission in audio files. Modified F5 uses matrix encoding to improve efficiency of embedding. It is a secure steganographic algorithm hides confidential messages within

another carrier file. An unauthorized user should not be able to find out whether there is any secret data is embedded in the steganogram (i. e., a steganographically modified carrier file).

## 3. PROPOSED TECHNIQUE

This system is based on steganography for security purpose. So we are using the Modified F5 algorithm and the necessary step. The technology which will be used in this system is JAVA and HTML. The JAVA technology will be used for providing platform independency to the application and for doing the bit level calculations in the modules. The HTML technology would be used for the development of help modules which will be meant for providing to the application.

### 3.1 Modified F5 algorithm

In 2001, the German researchers Pfitzman and Westfield introduced the F5 algorithm. The goal of their research was to develop concepts and a practical embedding method for JPEG images that would provide high steganographic capacity without sacrificing security. The F5 algorithm embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to embed a message of certain length [13]. In Modified F5 algorithm on the given text encryption is performed on that text and message bits are embeds into audio beats. It is used to reduce the necessary number of changes required for embedding a secret message.

Steps for embedding:

1. Input one audio/video cover file.
2. Calculate DCT value of beat matrix.
3. Apply quantization to DCT coefficients the quality factor 'Q' is used to build quantization table.
4. Take a password from user which is served as random embedding position in a DCT blocks.
5. To hide messages, choose available coefficient.
6. Apply entropy encoding algorithm.
7. Save stego file in Wave/Mp3 format.

Steps for decoding:

1. Take input as stego file for performing steganalysis.
2. Decompress stego file.
3. Perform filtering for noise removal.
4. Recompressed the audio/video.
5. Count different histogram value for the stego audio and cover audio.
6. Calculate different stego audio/video-cover audio.

### 3.2 Discrete cosine transform

Sound file consists of vectors that vectors are divided into smaller frames and arrange in the matrix form. The matrix is manipulated with the DCT operation. By performing DCT operation elements are sorted in their matrix form through which components and their positions can found out[12]. Elements are arranged in descending order and then threshold value is decided which are below the threshold values, so the compression takes place because of the reducing size of the signal[12]. So by using reconstruction process the data is then converted into the original form. For this IDCT operation, perform on the signal then it is converted into vector form. Formula:

$$x_{n=} \sum_{k=1}^{n} y_k \, w(k) \cos\left(\frac{\pi(2n-1)(k-1)}{2N}\right)$$

Where

$$w(k) = \begin{cases} \frac{1}{\sqrt{N}}, & k = 1 \\ \sqrt{\frac{2}{N}}, & otherwise \end{cases}$$

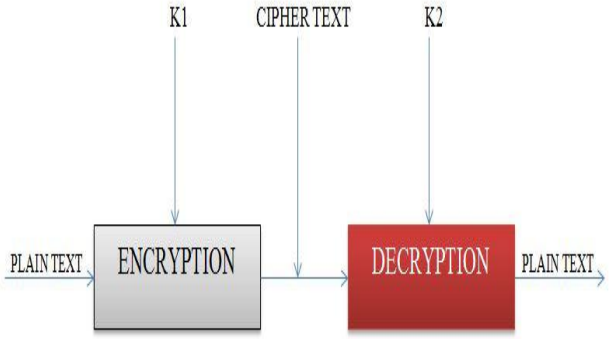


**Figure 1: Basic Working**

In above diagram describes the basic working of how the actual process is been takes place in application. First the plain text will be encrypted with encryption key k1. This plain text will be converted into cipher text which will go for further process that is decryption which will be done at end user side. For decryption a decryption key K2 will be use and with the help of that key the end user can get his desired output that is plain text.

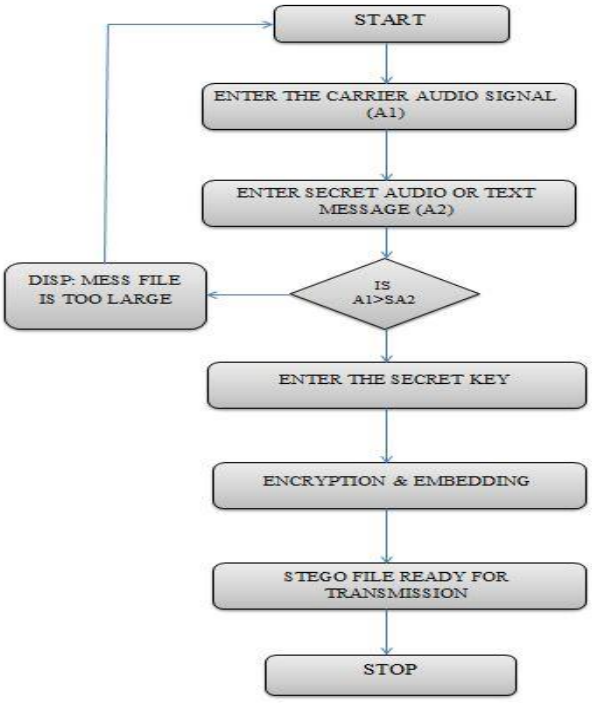


**Figure 2. System flowchart**

To accomplish the steganography process the following steps have to be followed:

**Step 1:** Take the input audio file from user and the message that he/she want to transfer.

In above step an application will receive an input file from the user which is known as cover file. Also it will accept a message or text file which user wants to send the end user.

**Step 2:** convert message into appropriate binary numbers.

This step converts the message or the text file into appropriate binary numbers and then it goes for further processing.

**Step 3:** Insert that binary numbers into audio file.
In this step the converted binary numbers are inserted into the cover file which is selected by the user.

**Step 4:** Performing algorithms for data hiding.
This step is the heart of the algorithm in which an appropriate binary numbers get combined with the cover file. If the data size is too large then data compression will take place using DCT algorithm. In the whole process actual working is run in the backend which will lead to message hiding and finally meet the desired goal.

**Step 5:** Then another user decrypt that files and get desired data. This is the final step which is performed at the receiver side. Here also the algorithm will be running in the backend and the decryption process has been done through which end user can get his/her desired data or message.

# 4. RESULT ANALYSIS

This system has a high steganographic capacity. The Modified F5 algorithm helps to prevents visual attacks. The user will communicate more securely then existing available software. This project provides safe & secure way for data transmission like text transmission which will be helpful to the users. This application will be useful in various fields like e-shopping, e-mail etc. It will be also helpful in military purpose for secret data transmission. Use of this application is one can send message more secretly with the less chances of data loss.

Modified F5 algorithm has a high steganographic capacity. The Modified F5 algorithm helps to prevents visual attacks. Also it provides more secure communication than F5 algorithm.

In following table it can be seen how modified F5 algorithm is different in terms of capacity, efficiency and robustness. This system is to give a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. This system will not change the size of the file even after encoding and also suitable for any type of audio and video file format. Encryption and Decryption techniques have been used to make the security system robust.

**Table 1. Result analysis of all algorithms with modified F5**

| Algorithm | Capacity | Efficiency | Robustness |
|---|---|---|---|
| LSB Algo. | Low | Poor | Low |
| Echo hiding | Medium | Low | Medium |
| Direct Spread Spectrum | Low | Poor | Medium |
| Phase coding | Medium | Medium | Low |
| Modified F5 Algo. | High | High | High |

In this system the user can send his message to end user through networking in a secure manner. In this system login process have been used for encryption and decryption so that an unauthorized party cannot detect the message easily.

# 5. CONCLUSION

This system provides a good, efficient method for hiding the data from hackers and sent to the destination in a secure manner. This system maintain the size of the file even after encoding and also suitable for any type of audio/video file format. Encryption and Decryption techniques have been used to make the security system robust.
Thus this method provides a more reliable way for secure communication and help to achieve high capacity robust steganography system. The main goal of modified F5 algorithm is to provide high security. It decrease the number of changes which are necessary for message hiding.

# 6. REFERENCES

[1] Adriansyah, Y. 2010 “Simple Audio Cryptography”, Bandung, Indonesia: Department of Informatics Engineering, Schools of Electronics and Informatics Engineering, Bandung Institute of Technology

[2] Cvejic, N. Seppiinen, T. 2002, Increasing the capacity of LSB-based audio steganography, IEEE Workshop on Multimedia Signal processing, pp. 336 -338

[3] Cvejic, N. Seppanen, T. 2004, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04), vol. 2, pp. 533

[4] Cvejic, N. and Seppnen, T. 2005 Reduced distortion bit-modification for LSB audio steganography, Journal of Universal Computer Science, vol. 11, no.1, pp. 56-65

[5] Amin, M. M. Salleh, M.Ibrahim, S.et.al, Information Hiding using Steganography, 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, IEEE, Oct 2012.

[6] Sullivan, K. Bi, Z. Madhow, U. et.al., Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168

[7] Jar no Mielikainen, 2006 LSB Matching Revisited, Signal Processing Letters, IEEE, Publication Volume : 13, Issue : 5, pp. 285- 287

[8] Chen and Womell, G. W. 2001, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443

[9] Chen, B. 2010, Design and analysis of digital watermarking, information embedding, and data hiding systems,” Ph.D. dissertation, MIT, Cambridge, MA

[10] Amin, M. M. Salleh, M. Ibrahim, S. et.al., 2012 Information Hiding using Steganography, 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, IEEE

[11] Gunjan.Nehru, Puja.Dhar, A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach, IJCSI International Journal of

Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[12] Patel, H. Dave, P. 2012, Steganography Technique Based on DCT Coefficients

[13] Jessica.Fridrich, Miroslav.Goljan, Dorin.Hogea, Steganalysis of JPEG Images: Breaking the F5 Algorithm, Department of Electrical and Computer Engineering, SUNY Binghamton, NY 13902-6000, USA, 2011.