Multi-Part Data Hiding in Audio Steganography

Uma Mehta

Student, CSE, JCDMCOE,

Sirsa, India

Abstract— **The security of information is the essential part of organization and security mechanisms need to be implemented. The cryptographic and steganographic methods is one of the techniques of security in which cryptography encrypts the message and steganography hides the information in any digital media file such as sound, image file, etc. In this, the Steganographic method is used based on audio steganography which is concerned with embedding secret data in an audio file. Along with this, the hashing method has been used for information confidentiality and image file concept has also been used for information hiding. The basic idea behind this is that the information should not be centralized but in multiparts storage so that the intruder cannot detect it. Firstly the information is processed under hash algorithm, then cryptographic method has been implemented to be more secure and then, the some part of the information will be hiding in multipart audio and last part in image file. This step provide more security because for data decryption, the all files will be needed else information will not be able to detected. For hiding in media file, the LSB (Least Significant Bit) technique is implemented which replaces the LSB of audio with binary of information. The least significant-bit (LSB) based technique are very popular for steganography in spatial domain .In the networking scenario, the information is shared among the users and this information should be confidential and authenticated to the receiver. The information should be kept in secure medium for protect from the intruders. So the data hiding technique should be used for keep the information available to the users.**

Index Terms— **Cryptography, Steganography, Multi-Part Audio, LSB, Hashing.**

I. INTRODUCTION

Steganography is a technique of hiding the data in Files such as Image, Audio, and Video etc over the Network. In Today's Business Environment, the information is necessary part of an organization that should be secure and private for keep the information confidential. From the security aspects, the information should be available when required. Intruder can alter; remove the information which will be resulted of Information unavailability. From the security perspective, the information should not be readable by intruder and cryptography technique can convert the plain text to encrypted text. The encrypted information can decrypt the intruder by get the key information. The objective of Steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Steganography implies that the hiding of one kind of data into another data means encapsulation of information. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

Steganography basic requires the some elements which will hide the information into a media files such as image (jpg, bmp, png, etc), Sound files (mp3, mp4, etc).

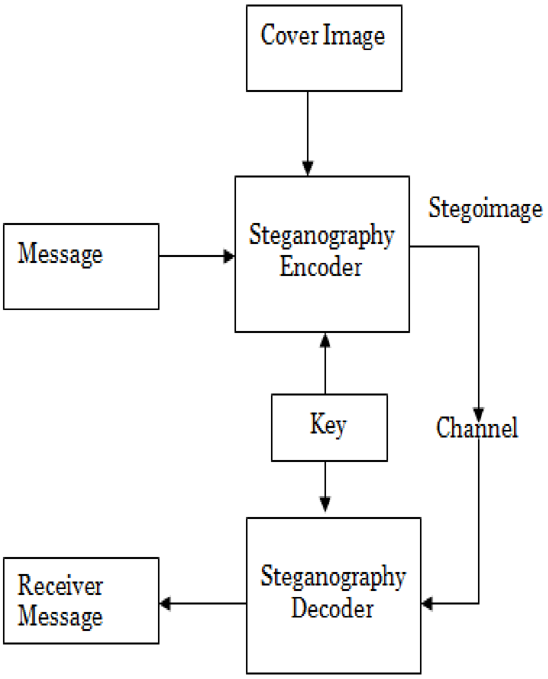


Figure: Steganography Scenario

This above figure explained the concept of steganography. In the security scenario, the sender hides the message in the image and this process is executed by the encoder. The final image will be generated by the encoder having the hidden information. These images further transmitted to the receiver. Then the receiver will follow the same steps to retrieve the confidential information from the covered image. The media can be audio file for secure the information

II. OBJECTIVE

In the research scenario, the different layer data securing technique will be implemented. These layers will secure the content from intruders. This technique will secure the confidential content over the network. These layers are described as:

1. Design/Modify an Algorithm by which Secret Data will be hidden in Audio Format.
2. MD5 Hashing of the information and integrate with Hashed Output.
3. Encrypt data before embed it into audio files to provide two layer security.
4. Design an algorithm to embed data in Multi-Part Audio Files.
5. Output Audio files will be more than one to improve security.
6. Size of output file should be less or equal in size without loss of Data.
7. Embedding data into the file does not alter the integrity of the file.
8. A software need to be designed to perform this task.
9. Perform different data hiding experiments to verify this technique.
10. Experimental results and provides a brief analysis of the application.

III. PROPOSED METHODOLOGY

In our security scenario, the cryptography, Steganography, hashing with media files such as image and sound file has been considered. For effective results of this proposed work, the algorithm has been designed and explains the flow of security mechanism applied on sound file bit stream, hashed-Encrypted information with image Steganography and sound as well for keep the information hidden from the intruder. In the research scenario, the Multi- layer data securing technique will be implemented. These layers will secure the content from intruders. This technique will secure the confidential content over the network. These layers are described as:

- First layer will convert the data using hashing algorithm.
- The output of the first step will be encrypted using cryptography technique
- Split the Audio file in Multi-Part for Decentralized Information and Security Perspective.
- The Some outcome Parts of these two layers will be embedded to Multi-Part Sound files.
- The last Part of Output information will be embedded to Image.
- These Multi-Part layers will work fine from the sender side and sound file will be transmitted over the network.

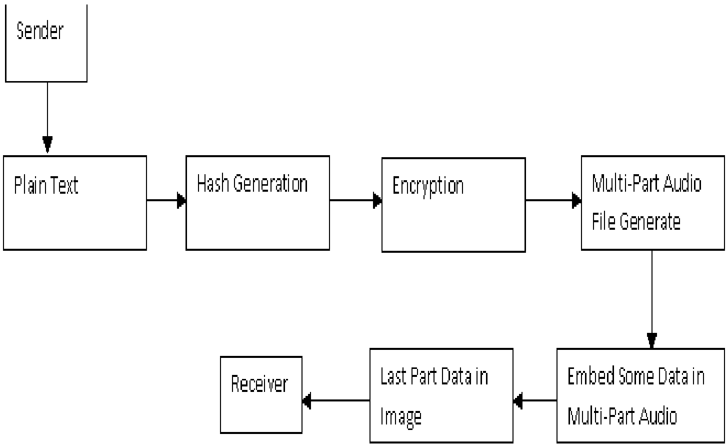


Figure: Flow Chart

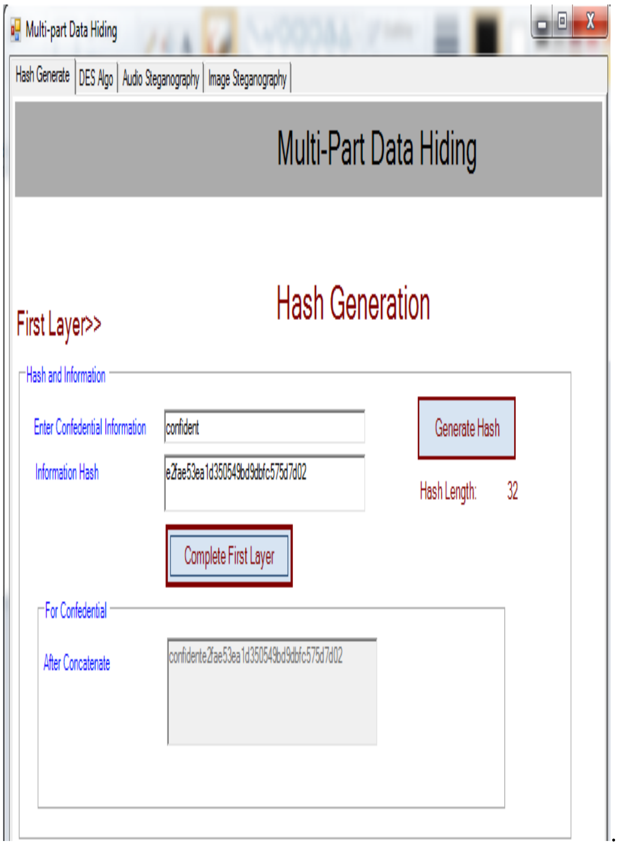
IV. APPLICATION

The majority of today’s Steganography systems use multimedia objects like image, audio, video etc as cover media. In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the similar to watermarks on actual paper and are sometimes used as digital watermarks. We will split out output file in multiparts, So that all information should not be centralized. If the information carrier becomes corrupted or modified, all the secret data becomes irretrievable. Having the secret data residing in one location is prone to the threat of intrusion. If an attacker manages to get hold of the information carrier, revealing its contents becomes easy. This article proposes the use of a secret sharing scheme to address the mentioned weakness. The secret shared data is then hidden in audio files to increase the level of security. In two layer security, the data is not much secure because cipher text can be decrypt from the encrypted text by using the cryptanalysis technique. In network scenario, security of data and transmission is main aspect which cannot be handled by just encryption and stegano techniques and it is dangerous because information can reveal.

.

V. RESULTS

Hash Generation:-



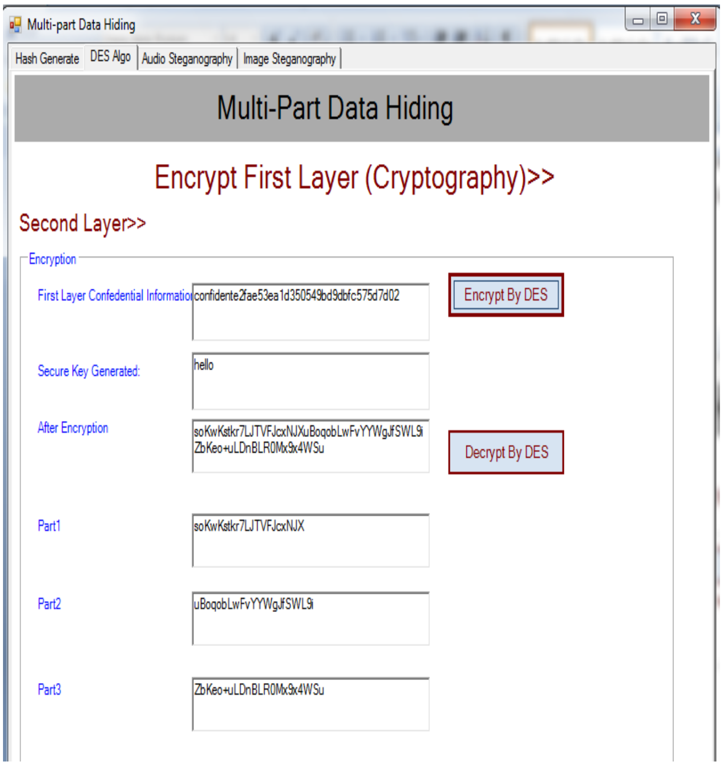
Enter Confedential Information: confident

Information Hash: e2fae53ea1d350549bd9dbfc575d7d02

Hash Length: 32

After Concatenate: confidente2fae53ea1d350549bd9dbfc575d7d02

DES:-



First Layer Confedential Informatio: confidente2fae53ea1d350549bd9dbfc575d7d02

Secure Key Generated: hello

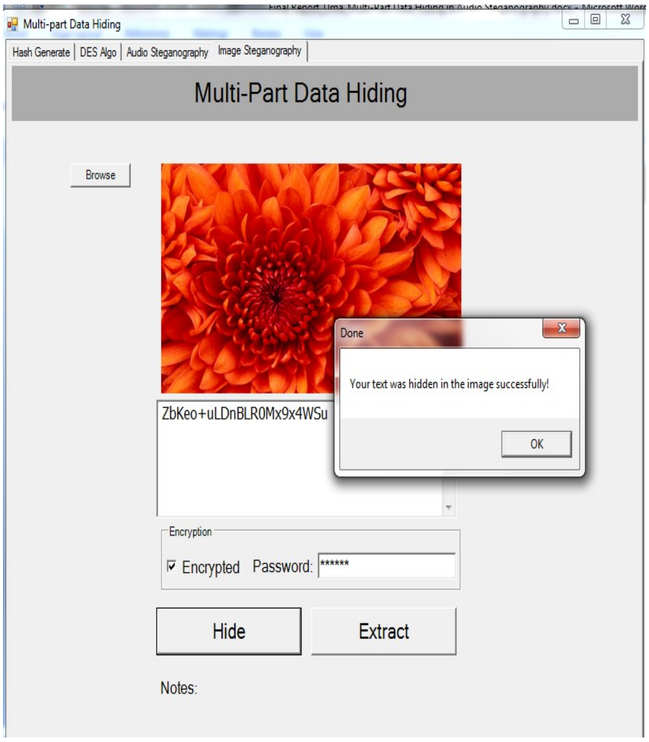
After Encryption: soKwKstkr7LJTVFJcxNJXuBoqobLwFvYYWgJfSWL9i
ZbKeo+uLDnBLR0Mx9x4WSu

Part1: soKwKstkr7LJTVFJcxNJX

Part2: uBoqobLwFvYYWgJfSWL9i

Part3: ZbKeo+uLDnBLR0Mx9x4WSu

IMAGE STEGANOGRAPHY:-



ZbKeo+uLDnBLR0Mx9x4WSu

Your text was hidden in the image successfully!

☑ Encrypted Password: ******

VI. CONCLUSION AND FUTURE WORK

The information security is the main goal of organization and it should be protected. The Storage of secret information is a constant security concern, and the reliability and integrity of this information is important. In the existing work, the problem with steganography and cryptography was the single location storage of all the secret data along with the all key information. This means, if the security breaches at single point, the complete data will loss. We have proposed a method for information security which hides the information in different parts of audio and also, the some part in image. The both media files have been jointly used for improve the security. The complete media files will be required to get the complete secured information and then cryptographic method will be used to decrypt the message and then hashing for identification of confidentiality of information.

REFERENCES

[1] Ajit Singh, Swati Malik(2013), “Securing Data by Using Cryptography with Steganography”

[2] Jagbir Singh, Savina Bansal, R.K. Bansal (2013), “Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique”.

[3] Sonam Pathak, Rachana kamble(2013), “A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique”.

[4] Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S (2014), “A Research Review On Different Data Hiding Techniques”.

[5] Krati vyas1, B.L.Pal2 (2014) , “A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1.

[6] Roy, S. (2014), “Online payment system using steganography and visual cryptography”, Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE.