

Data Hiding Security Using Steganography

Ashish Kumar Narayan¹, Shilpi Sharma², Shanti Jaiswal³

¹M.Tech Scholar, BIT (Bhopal), ashishkumarnarayan@gmail.com, India;

²Head of Department, BIT (Bhopal), shilpi2000sharma@gmail.com, India;

³ M.Tech Scholar, SIRT (Bhopal), shantijaiswal0810@gmail.com, India;

Abstract – Steganography may be a technique for hiding data in a host signal. The host signal may be a still image, speech or video and therefore the message signal that's hidden within the host signal can be a text, image or an audio signal. For data hiding in host, discrete wavelet transform (DWT) is used. Perfect audio Steganography technique aim at embedding data in an imperceptible, robust and secure way and so extracting it by authorized people. Hence, up to this point the main challenge in digital audio steganography is to get robust high capacity steganography systems. Learning towards designing a system that ensures high capacity or robustness and security of embedded data has LED to great diversity within the existing steganography techniques.

Keywords: Audio steganography, DWT, PSNR, LSB, Data Hiding, Digital data security,

I. Introduction

Over the past decades, research in security has concentrated on the development of algorithms and protocols for encryption, authentication, and integrity of textual data or data with similar characteristics. Despite tremendous advances in security specifically, the development of asymmetric cryptographic protocols and the inception of string symmetric ciphers-plenty of security problems still afflict systems. For example, hackers exploiting weaknesses in other systems and the use of inadequate (too short) cipher keys produce frequent news headlines about broken security systems.

Despite the news headlines, such problems have been well explored and even solved in principle, therefore they aren't the primary focus on this special theme issue. Rather, the articles here cover the unsolved problems in image security, which relate fairly closely to computer graphics. The unsolved challenges arise from the increased availability and distribution of multimedia content over Internet services such as the World Wide Web and their implications for intellectual property protection and copyright issues.

A growing number of scientific groups in computer science and cryptography have confronted these challenges. Researchers are currently working on issues such as visual cryptography, mechanisms for the integrity of image material, digital signatures for multimedia data, and data hiding techniques. Data hiding, which has achieved the highest popularity, contemplates the crucial

needs for protecting intellectual property rights on multimedia content like images, video, audio, and others. These needs demand robust solutions due to the explosion of publicly available multimedia information and the easiness with which this information can be distributed, copied and modified. Watermarking technology meets these demands and provides a feasible approach to protect against-and prove-illegal copying and redistribution in the digital world.

II. Steganography

Steganography is the art of devising astute and undetectable methods of concealing the message themselves. It is therefore broader than cryptography. There is no theory for steganography. The origin of steganography is biological and physiological [8-9]. The earliest allusion to secret writing in the west appears in Homer's Iliad [10]. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. Steganography is a combination of two words "stegano" means covered and "graphy" means writing. Steganography[2] is an art of hiding the existence of the message so it dose attract the attention toward the secret message, hence third party or illegal person cannot be able to detect the message. Steganography is used in ancient times, like messages are written on the bodies using invisible inks, whereas other ways of sending messages is writing messages on envelops in areas which are covered with stamp. Modern

methods of steganography are known as digital steganography.

III. Watermark

The earliest reference to Watermarking in history dates back to the B.C era. The present day Watermarking has developed basically from two different streams, Cryptography meaning, “secret writing” and Steganography, which in the Greek language means, “cover writing”. Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The intended message to be sent is called plain text message and the disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is in the clear.

IV. Proposed Methodology

The creation of digital records in their kind of style has attracted a specific curiosity as of researchers to form positive their safety. System like encoding and watermarking are already utilize throughout this regard. Though, the requirement for new procedure and new algorithms to counter constantly-changing malicious makes an effort to the integrity of digital data has been converted into a necessity in today’s digital time. Steganography, that literary implies that “covered writing” has drawn further thought among the previous few years. Its main goal is to cover the actual fact that a communication is taking place between 2 components. The sender implant secret information of any kind using a key during a digital cover file to produce a stego file, in such the method that an observer cannot observe the existence of the hidden information. At the other finish, the receiver processes the received stego-file to extract the hidden information. An example of audio steganography is depicted in Figure.1 wherever the cover file being used is a digital audio signal. A lucid application would be a cowlt communication exploitation innocuous cover audio signal, like phone or video talk’s conversations. Varied options influence the quality of audio steganographic ways. The importance and so the impact of each feature depend on the applying and so the transmission atmosphere. The most vital properties include robustness to noise and to signal manipulation, safety and hiding ability of embedded data. Robustness requirement is tightly related to the applying and is that the most difficult to satisfy during a steganographic system. In addition, there's a trade-off between robustness and hiding-capacity. Generally, they hardly exist within a similar steganographic system.

The propose approach that uses numerous techniques like thresholding, DCT, LSB, it works with efficiency and supply maximum space at a similar time will increase security level, wherever because the quality of Steganographic image is additionally improved.

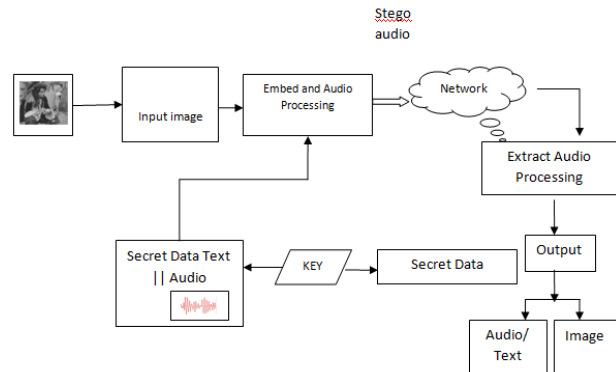


Fig.1 Blocks Diagram For Audio Steganography

Currently encode the audio file using AES (advance coding algorithm), it's the strongest algorithmic rule for coding yet. When encoding audio file is embedded in image using LSB (least significant bit) technique and Stego image is retrieved. Currently decoding part, embedded image is retrieved. Secret information is recovered. Decode the audio file; convert the audio file from hexadecimal to decimal number. Retrieve the first audio file. The propose solution is analyzed on the idea of PSNR (peak signal to noise ratio) and MSE (mean sq. error) frequency. Whereas PSNR is used to measure the image quality of original and Stego image. Generally, high value of PSNR indicates that Stego image is of higher quality. MSE may be a risk performs that represents average sq. error between the first image and Stego image.

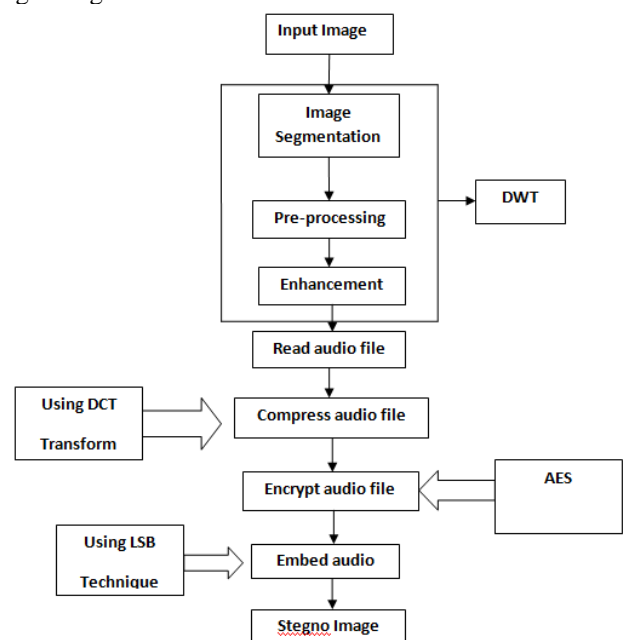


Fig.2 Flow Chart of Encryption Process

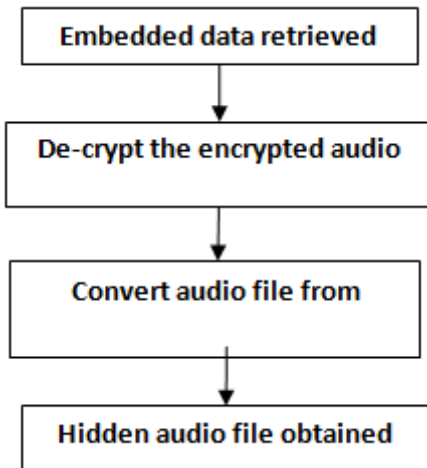


Fig.3 Decryption Process

V. Units

The proposed approaches are used for the proposed research and these results are shown below:

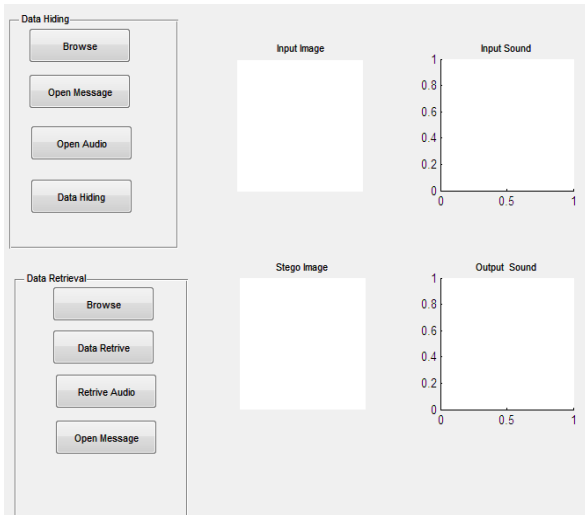


Fig.4 Program Run Then Open Window

This figure shows the data hiding window. When we run the program file then open this window.



Fig.5 Input Image Window

This figure shows when we browse the main input image then this window is open.

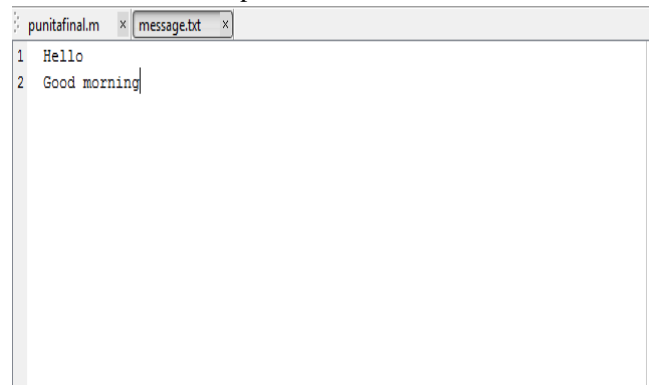


Fig.6 Message Text Editor Window

In this figure we write the text message which text message is hide.

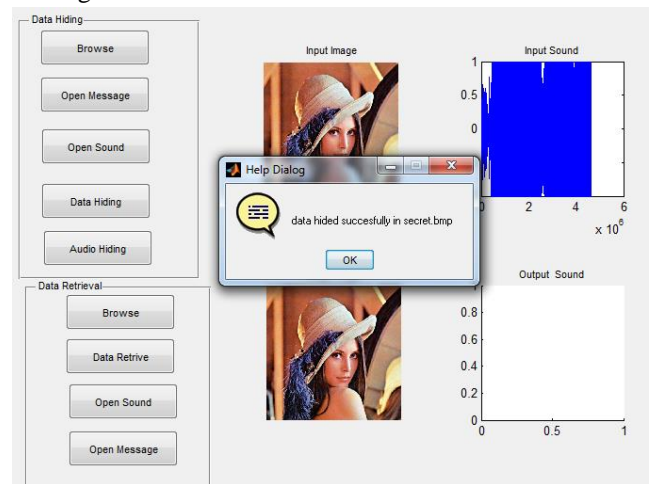


Fig.7 Data Hiding

In this figure we are hide the message then press the data hide button then open the dialog box that is our data is hidid successfully in secret.bmp.

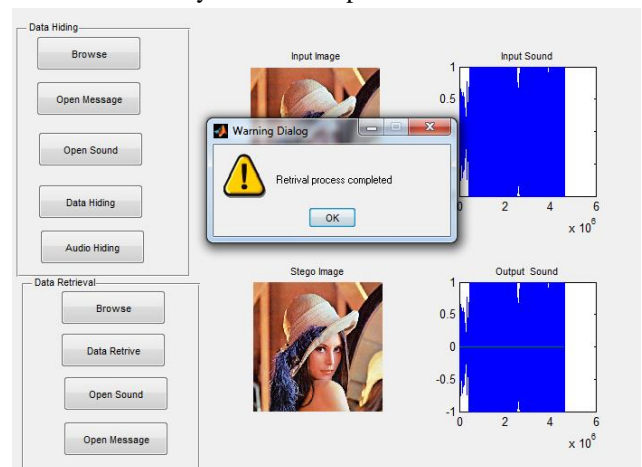
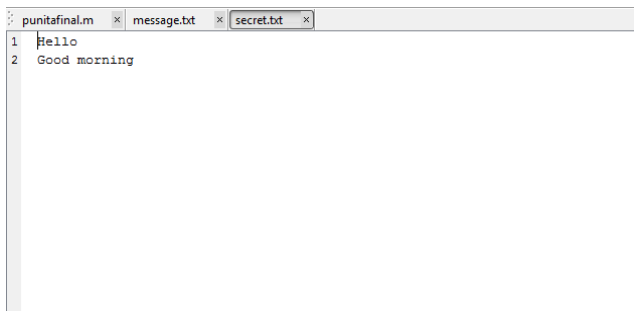


Fig.8 Data Retrieval Window

In this figure we are press the data retrieve button are press then open the dialog box in our window that is we know that our data is successfully retrieved.



```
punitafinal.m x message.txt x secret.txt x
1 Hello
2 Good morning
```

Fig.9 Output Window

VI. Conclusion

The main aim is to come up with a method to hide the information in audio file in such some way there are no perceivable changes within the audio file once the message insertion. Ensure digital information security, numerous techniques are conferred in recent researchers work. Audio steganography, especially, addresses problems related to the necessity to secure and preserve the integrity of information hidden in voice communications, even once the latter passes through insecure channels. This research presents digital audio steganography techniques and approaches. The planned methodology effectively produces Stego image during which secret information is embedded and encrypted similarly using AES algorithmic rule. The efficiency of the technique is measured by using different evaluating parameters.

References

- [1] Razzaq, Mirza Abdur, et al. "Digital image security: Fusion of encryption, steganography and watermarking." *International Journal of Advanced Computer Science and Applications (IJACSA)* 8.5 (2017).
- [2] Azam, Naveed Ahmed. "A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding." *Security and Communication Networks* 2017 (2017).
- [3] Koppu, Srinivas, and V. Madhu Viswanatham. "A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform." *Modelling and Simulation in Engineering* 2017 (2017).
- [4] Pushpad, Akshay, Anjali Ashish Potnis, and Amit Kumar Tripathi. "A Review on Current Reversible Image Security Schemes." *Imperial Journal of Interdisciplinary Research* 2.11 (2016).
- [5] Wang, Wei, et al. "A novel encryption algorithm based on DWT and multichaos mapping." *Journal of Sensors* 2016 (2016).
- [6] Al-Husainy, Mohammed Abbas Fadhil. "A novel encryption method for image security." *International Journal of Security and Its Applications* 6.1 (2012).

- [7] Madhu, B., Ganga Holi, and Murthy K. Srikanta. "An Overview of Image Security Techiques." *International Journal of Computer Applications* 154.6 (2016).
- [8] Baboo, Santhosh, and V. R. Sasikumar. "Fusion of Steganography Digital Watermarking Data Hidden In Patient Medical Image using PPC Approach." *Global Journal of Computer Science and Technology* (2015).
- [9] Muhammad, Khan, et al. "Secure image steganography using cryptography and image transposition." *arXiv preprint arXiv:1510.04413* (2015).
- [10] Muhammad, Khan, et al. "Secure image steganography using cryptography and image transposition." *arXiv preprint arXiv:1510.04413* (2015).