ISSN 2320-9984
Volume 2 Issue 2 | June 2014 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

# An Approach for Data Hiding for Secure Information Interchange

**Lokesh Vishwakarma**
*M. Tech. Scholar,*
*Vindhya Institute of Technology and Science*
*Jabalpur, (M.P) [India]*
*Email: lokesh0202@gmail.com*

**Prof. Shivam Khare**
*Assistant Professor*
*Department of Electronic & Communication Engineering*
*Vindhya Institute of Technology and Science*
*Jabalpur, (M.P) [India]*
*Email: shivamkahre2008@gmail.com*

***Abstract—*** *Steganography is a kind of security technique with obscurity; the way and art of hiding the even existence of a message between transmitter and intended recipient. Steganography generally used to cover secret messages in different kind of files, including digital audio, image and video. The most important three parameters for audio steganography are payload, imperceptibility, and robustness. Various applications have various requirements of the steganography methods used. This paper aims to give a highlight of image steganography, its uses and techniques. Paper work is an implementation of Audio and Image Steganography for the same plaintext, paper work uses three defendant key triple layer of data protection, The avalanche in plaintext is very high in present paper work.*

***Keywords:—****digital image; information hiding; multimedia security; watermarking; steganography*

## 1. INTRODUCTION

Information security is important for confidential data transfer. Steganography is one type of the kinds used for secure communication of confidential information. Hiding data in a photograph i.e image is less suspicious than transmitting an encrypted file. The ultimate purpose of steganography is to carry the information secretly by hiding the very even existence of data in some another medium such as audio, image, or video.

Following counted features and restrictions are the criteria which a data embedding algorithm must meet

1. Quality of host signal should not be degraded objectionably and the perceptibility of embedded data must be kept minimal.
2. The data must be embedded into whole body of the target media rather than wrapper or header. Therefore it would be kept intact in different formats.
3. The data must be secure against intentional and intelligent removal attempts such as filtering, encoding, cropping, channel noise, lossy compressing, resampling, scanning and printing, digital to analog (D/A) conversion, analog to digital (A/D) conversion, and etc.
4. Since data hiding goal is to keep the embedded data into host signal, embedded data asymmetrical encoding is desirable feature but not essential.
5. To guaranty data integrity error correction coding is necessary.

Degradation of embedded data at signal modification time is unavoidable.

6. Arbitrary re-entrant and self clocking are mandatory properties of the embedded data. These properties are to guaranty that embedded data will be retrievable even if only some fragments of the host be available.

Today there are various applications of information hiding. Knowledge of data hiding might be used either in ethical or unethical ways. However, data hiding algorithms cannot easily be categorized either in steganography or watermarking categories as there is no transparent boundary between these two terms and mostly the classification relies on application of the algorithm. Therefore regardless classifying data hiding the most common data hiding applications are fingerprinting, secret communication, secure storage, covert communication, and copyright protection.

**Cryptography:**

Cryptography scrambles messages so it can't be understood. Advantage of cryptography is secure data, changeable bit key for information hiding it is fast and flexible very easy to implement. Only Disadvantage of cryptography is that it is for mobile devices only and it has complex hardware and cipher patterns is less complicated.

**Steganography:**

It is an ancient good art of for hiding information. It used to covers information in digital images. Main Advantage of Steganography approach to reduce the chance of a message to get detected. Disadvantage of Steganography Transmitting same images again and again may sound suspicious to the intruder, and it is easy to decipher ones detected.

## 2. DESIGN TECHNIQUE

### *2.1 Encryption*

As figure 1 shows plain-text can be of any size but it must be at-least ten times less than depend on the size of its massager audio or image.

***Cipher Generator:*** It performs initial cipher generation and use division and modulation with specific key let A is plaintext K1 is the key then

B = abs (A / K1)
C = A % K1
D = [B C];

Now D will be the data which will be transmitted

***Breaking the data:-***

Let D = [ x1 x2 x3 x4 x5……xn] it will break in data1 and data2 as

D1=[x1 x2 x5 x6 …… ]

And

D2 =[x3 x4 x7 x8…….. ]

***Scaling:-*** Data amplitude will get scaled by fix parameter 200

D3=D1 / 200;

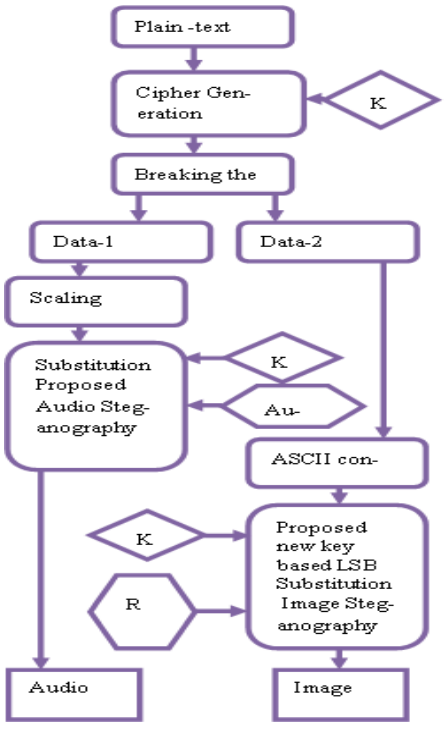


*Figure 1: Proposed Encryption technique*

***Substitution Audio Steganography: -***

Below is the proposed approach for data hiding in audio file consider D3 is the data

D3 = [Y1 Y2 Y3 Y4 …..……$Y_n$]

And samples of audio file are

A1 = [W1 W2 W3 W4……..$W_m$]

And key-2 can be anything in between 100 to 255 is key2

After that the spacing of K2 = Key2*10 the data get interpreted in audio file as

D4= [w1 w2 …….$W_{K2}$ y1 $W_{K2+1}$ $W_{K2+2}$ …… . . $W_{K2+K2}$ y2 .$W_{2*K2+1}$……] D4 is the ciphered audio.

***ASCII Conversion of Data:-***

It is necessary because in image steganography pixels are there is in binary form. And data can be any characters or number first it is required to convert each in ASCII binary form. let data is D2 of length L1 characters then each of character will get converted in ASCII binary form with length of L3=L2x8

$$D5_{(L3length)} = (\text{ASCII of } D2_{(L1\ length)})$$

***Proposed substitution image steganography: -***

If D5 is the binary form of data and as known any color image has three different components RGB. With proposed method of steganography let image is I and $I_R$ $I_G$ & $I_B$ are its three components then

D5 = [b1b2b3b4b5b6b7……..]

And image I is

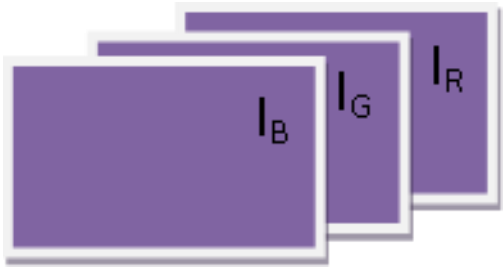


*Figure 2: Image segments*

$$I_R = \begin{matrix} ir11 & ir12 & ir13 & \dots & ir1m \\ ir21 & ir22 & ir23 & \dots & ir2m \\ ir31 & ir32 & ir33 & \dots & ir3m \\ ir41 & ir42 & ir43 & \dots & ir4m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ irn1 & irn2 & irn3 & \dots & irnm \end{matrix}$$

$$I_G = \begin{matrix} ig11 & ig12 & ig13 & \dots & ig1m \\ ig21 & ig22 & ig23 & \dots & ig2m \\ ig31 & ig32 & ig33 & \dots & ig3m \\ ig41 & ig42 & ig43 & \dots & ig4m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ign1 & ign2 & ign3 & \dots & ignm \end{matrix}$$

$$I_B = \begin{matrix} ib11 & ib12 & ib13 & \dots & ib1m \\ ib21 & ib22 & ib23 & \dots & ib2m \\ ib31 & ib32 & ib33 & \dots & ib3m \\ ib41 & ib42 & ib43 & \dots & ib4m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ibn1 & ibn2 & ibn3 & \dots & ibnm \end{matrix}$$

Each pixels is are size of 8 binary bits, and with proposed method the first binary bit of D5 (i.e. b1) with replace the LSB of first pixel of $I_R$ than second binary bit of D5 (i.e. b2) with replace the second LSB of first pixel of $I_G$ than third binary bit of D5 (i.e. b2) with replace the LSB of first pixel of $I_B$ and so on…..next pixel will pick as per the Key-3, K3.

***2.2 Decryption***

The process of decryption requires the approach in reverse manner but it can be easily observe the intended party requires having both files (i. e. cipher image and cipher audio) and it also not enough for to have both files the end used also should have knowledge of all three keys that are Key-1, Key-2 and Key-3. Without lack any single information the intended party cannot decipher the encrypted massage.

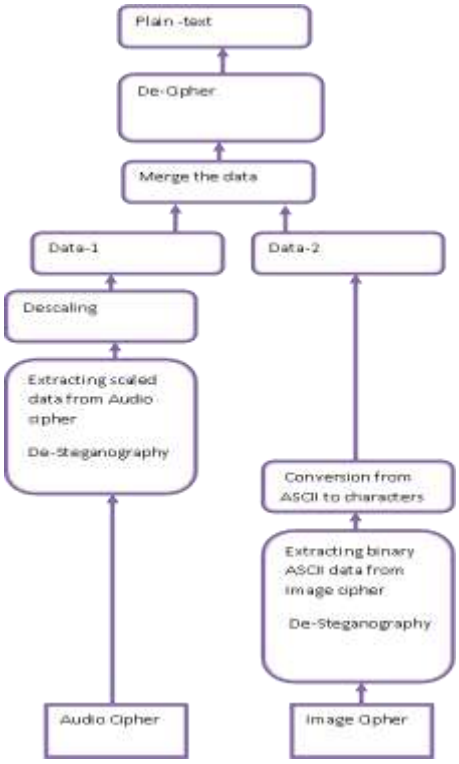


*Figure 3: The Decryption Process*

## 3. RESULTS

**Table 1: Audio Stenograph Results**

| Audio data | Audio File Size (KB) | SNR (db) |
|---|---|---|
| Wav_1 | 392 | 85.05 |
| Wav_2 | 491 | 84.17 |
| Wav_3 | 595 | 82.39 |
| Wav_4 | 689 | 85.36 |
| Wav_5 | 841 | 83.67 |
| Wav_6 | 920 | 83.83 |
| Wav_7 | 1770 | 85.98 |
| Wav_8 | 2140 | 83.83 |

**Table 2: Image Stenograph results**

| No. of Characters in data | MSE | Peak SNR |
|---|---|---|
| 3 | $0.6\times10^{-5}$ | 99.5402 |
| 15 | $0.8\times10^{-5}$ | 98.9908 |
| 17 | $0.83\times10^{-5}$ | 98.508 |
| 19 | $0.89\times10^{-5}$ | 98.4993 |
| 22 | $0.91\times10^{-5}$ | 98.3517 |

## 4. CONCLUSIONS

Both the steganography and cryptography have their self respective advantage and deficiencies, but the mixing of both the model provides best protection of the data from the hikers. As can seen from the results the proposed approach have less Mean Square Error and very good high SNR value for both Image and Audio steganography.

## REFERENCES:

[1] Text Steganography: A Novel Approach, Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, and Tai-hoon Kim, International Journal of Advanced Science and Technology, *2009* February Vol. 3

[2] Steganography- A Data Hiding Technique, Km. Pooja, Arvind Kumar, Research paper, International Journal of Computer Applications (0975 – 8887), November 2010, Volume 9– No.7

[3] Main Fundamentals for Steganography, AL-Ani, A. A. Zaidan, Zaidoon Kh. B.B.Zaidan and Hamdan. O. Alanazi, Journal of Computing, March 2010, Volume 2, Issue 3

[4] On The Limits of Steganography, Fabien A.P. Petitcolas, Ross J. Anderson, *IEEE Journal*, May 1998.

[5] Modern Steganography, Miroslav Dobscek, Czech Technical University in Prague.