A Unique Approach for Data Hiding for Secure Information Interchange

Payal Gupta
Shri ram institute of technology
Jabalpur (M.P)

Ravi Mohan
Shri ram institute of technology
Jabalpur (M.P)

Abstract: **Steganography is a form of security technique through obscurity; the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The three most important parameters for audio steganography are imperceptibility, payload, and robustness. Different applications have different requirements of the steganography technique used. This paper intends to give an overview 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

I. INTRODUCTION

Information security is essential for confidential data transfer. Steganography is one of the ways used for secure transmission of confidential information. Hiding information in a photograph is less suspicious than communicating an encrypted file. The main purpose of steganography is to convey the information secretly by concealing the very existence of information in some other medium such as image, audio 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, variable bit key for data hiding, fast and flexible easy to implement. Disadvantage of cryptography is that it is limited for mobile devices only, complex hardware, easy to detect cipher patterns.

Steganography: It is an ancient art of hiding information. It hides information in digital images. Advantage of Steganography methods reduces the chance of a message being detected. Disadvantage of Steganography Transmitting same images again and again may arouse suspicious-ness to the intruder, easy to decipher ones detected.

II. DESIGN TECHNIQUES

A. 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;

Substitution Audio Steganography:It is proposed method for data hiding in audio file let D3 is the data

D3 = [y1 y2 y3 y4 y5 ……y_n]
And audio file samples are
A1 = [W1 W2 W3 W4 W5 ……..W_m]
And key-2 can be any value in between 100 to 255 is key2

Then with the spacing of K2 = Key2*10 the data will get substituted 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 will be the ciphered audio.
ASCII conversion of data:- It is required because in image steganography pixels are there is in binary

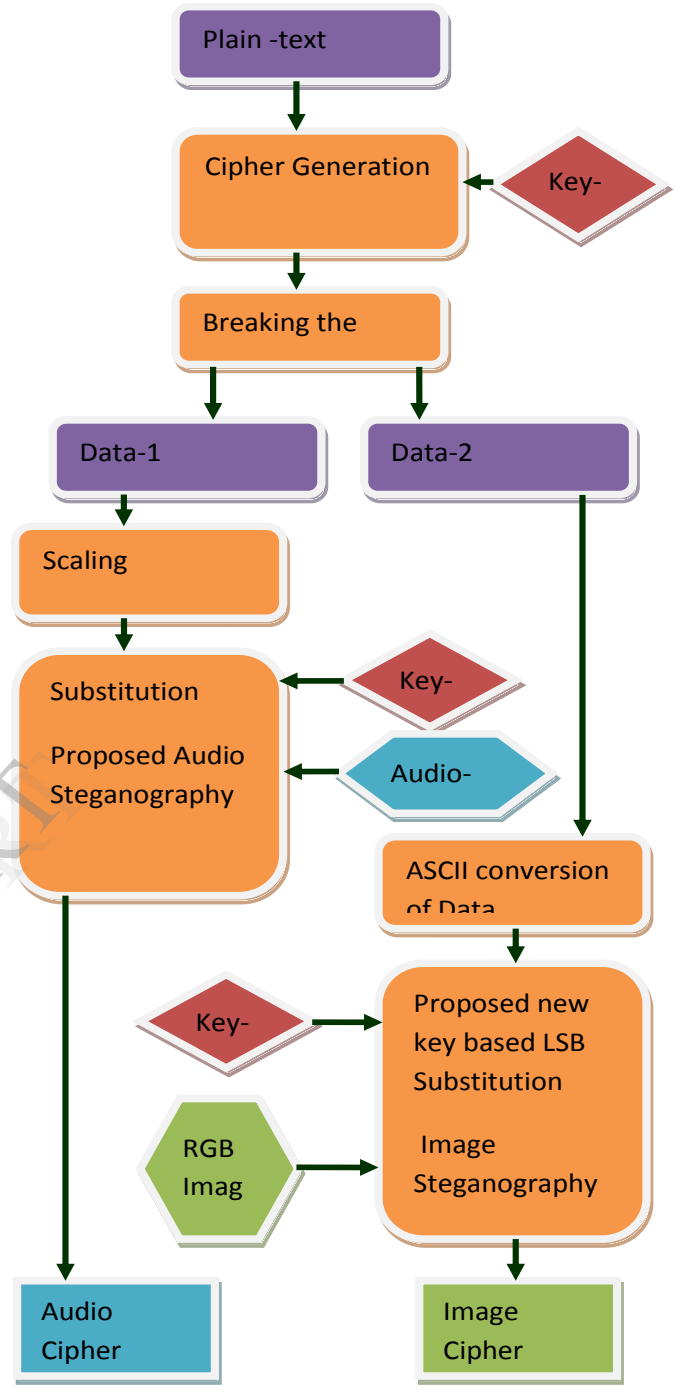

Figure 1: Proposed Encryption technique

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
$D5_{(L3length)}$ = (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=[b1b2b3b4b5b6b7b8……..]

And image I is

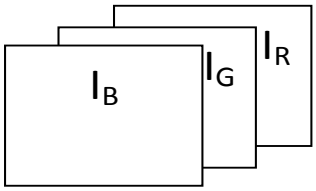

Figure 2: Image segments

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

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

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

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.

B . 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.

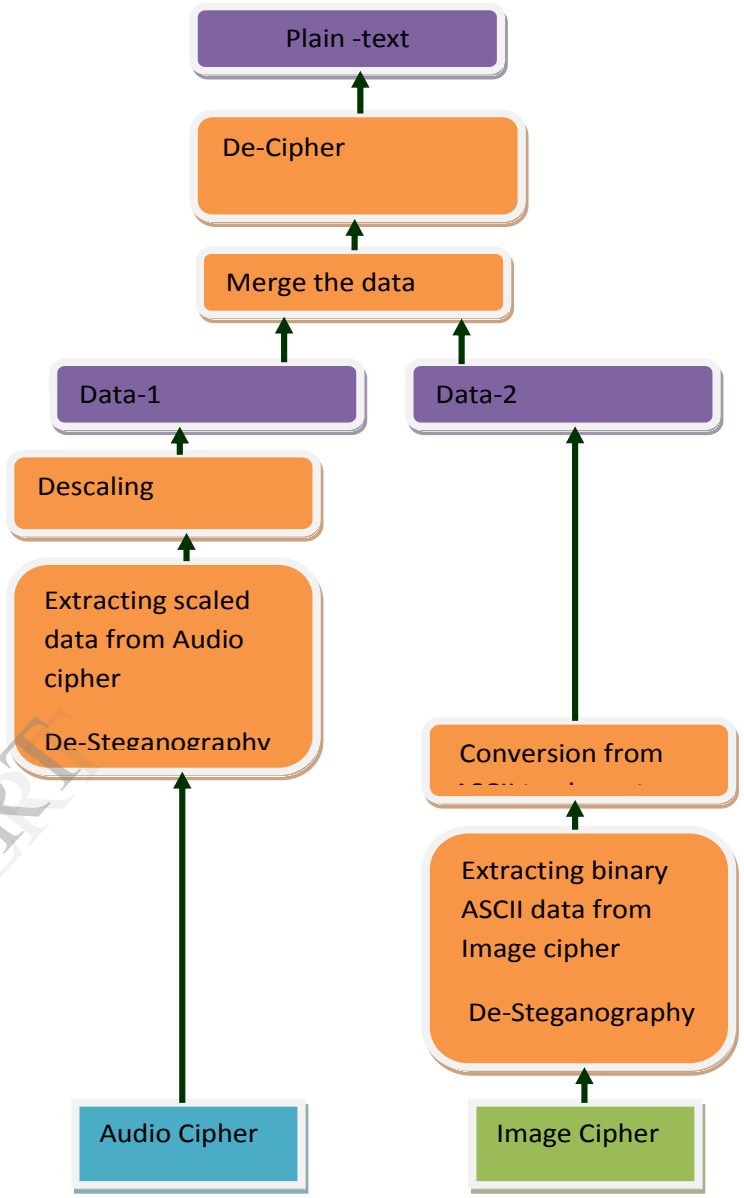

Figure3: The Decryption process

III. RESULTS

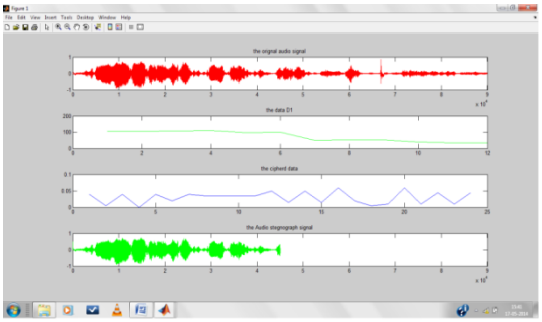

Figure 4: The audio steganography

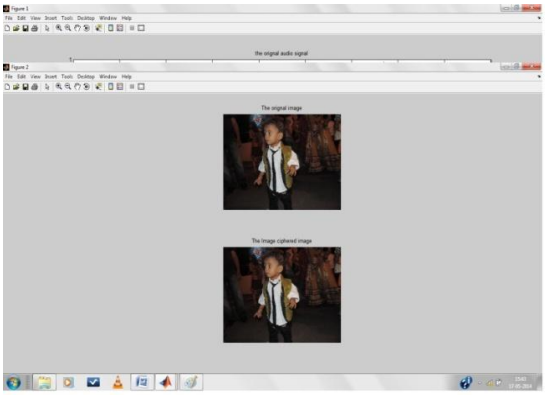

Figure 5: The Image

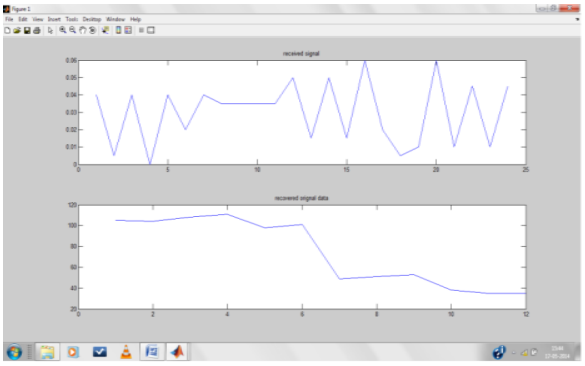

Figure 6: The Received Signal

Table 1: Audio Stenograph results

Audio File	Audio File Size (In KB)	Thesis Results (SNR in db)
Wave_1	390	84.60
Wave_2	490	85.87
Wave_3	590	83.69
Wave_4	680	84.36
Wave_5	830	82.60
Wave_6	940	82.63
Wave_7	1660	84.58
Wave_8	2050	82.86

Table 2: Image Stenograph results

No. of characters inserted	*MSE*	*PSNR*
2	0.5787×10^{-5}	100.5402
5	0.7716×10^{-5}	99.2908
7	0.7716×10^{-5}	99.2908
10	0.8681×10^{-5}	98.7793
12	0.9645×10^{-5}	98.3217

CONCLUSIONS

Both the cryptography and steganography have their own respective pros and cons, but the combination of both the model provides better protection of the data from the intruders. As can observed from the results the proposed method have less MSE and very good SNR value for both Audio and Image steganography.

REFERENCES

[1] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, Text Steganography: A Novel Approach, *Research paper* , International Journal of Advanced Science and Technology, Vol. 3, February, 2009
[2] Arvind Kumar, Km. Pooja, Steganography- A Data Hiding Technique, *Research paper* , International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010
[3] Zaidoon Kh. AL-Ani , A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010
[4] Ross J. Anderson, Fabien A.P. Petitcolas, On The Limits of Steganography, *IEEE Journal*, May 1998
[5] Miroslav Dobs´cek, Modern Steganography, Czech Technical University in Prague