Survey Paper on Image Encryption Steganography With Its Techniques

Sunil Kumar Yadav[1], Manish Dixit[2]
[1, 2] Dept of CSE/IT
[1, 2] MITS, Gwalior, India

Abstract- *Steganography talk about to the data hiding. The core determination of steganography is to conceal the data overdue images. It means that it encrypts the text in the form of image. The steganography is finished when the communiqué proceeds among sender & receiver. Now a day's in data transfer over the network, the security is the core matter concerned with this.*

Keywords- Least significant bit (LSB), Pixel value differencing (PVD), Edges based data embedding method (EBE), Random pixel embedding method (RPE).

I. INTRODUCTION

In this current age, where technology is developing at fast pace and each day new developments are made, security is of utmost priority. The data wishes to be set aside secure & safe so that it could be accessed only by the authorized personnel and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet every day beginning one place to another. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that individual the receiver must be talented to realize the communication. At first technique of cryptography was invented to sent top-secret messages over places. In cryptography the communication were prearranged in alternative communication in a roofed mode such that lone the sender & receiver distinguished the mode to decrypt it [1]. A cryptographic key were cast-off to decode the message that was known only by the certified persons. The drawback of cryptography were that supplementary individual derived to tell that the communication had a unseen text in it and so the possibility of communication being decoded by other person increased. To minimize this drawback the practice of steganography was familiarized. The word steganography belongs to Greek language. In Greek the Steganography standpoints for "covered writing". The first of all steganography were cast-off in Greece. They usage to cross the threshold the communication on a woody tablet and then apply wax on it to hide the written data. The system of steganography were far-off improved than cryptography as in it the data was hidden in image. The picture were then directed done internet. It had advantage over Cryptography as now the middle person does not come to know whether data is hidden in the picture or not. The data might only be decrypted from picture by the accredited person as he distinguishes the marvel to decode it and has the accredited key through him that were obligatory to decipher the data. The safekeeping & dependability of data spread also enhanced with development of steganography as nowadays no additional individual might alter the conducted data. The main application fields of steganography are:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

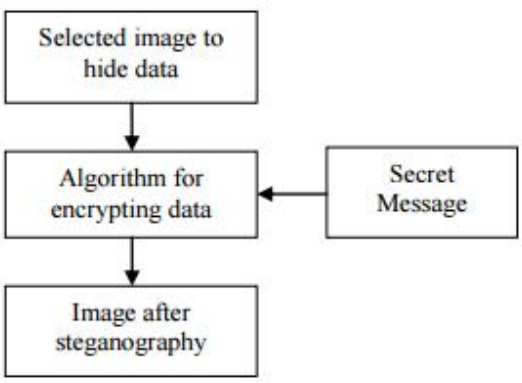
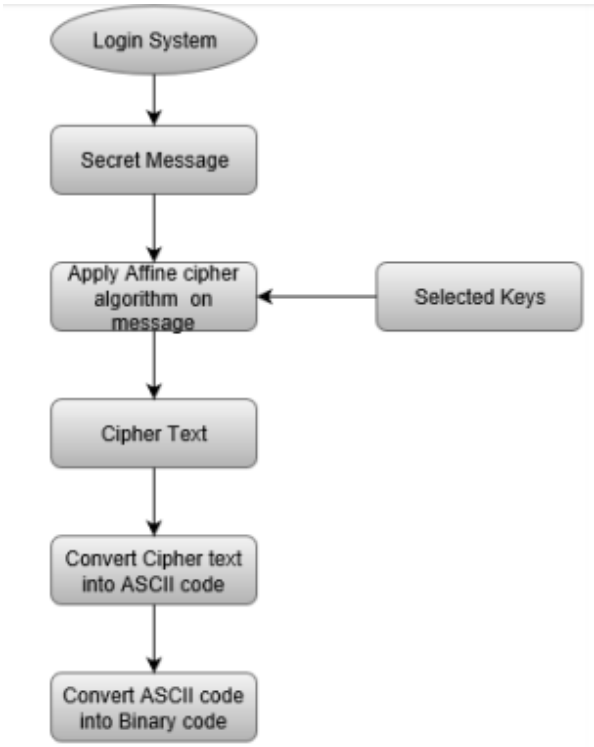


Figure 1 Diagram of Steganography

1. Encryption Phase

At the first phase to entrée into the scheme for thumping the data, the users are needed a user name and password. After login the scheme, user be capable to write the communication to encode the data with the top-secret keys beforehand implanting the data into an image as determine in figure 1. In this scheme the planned scheme uses Affine algorithm to scramble top-secret facts. Affine cipher is single of the algorithms that has cast-off to scramble data. In procedure where every letter in an script is plotted to its numeric correspondent, converted using a mathematical

function, and converted back to a letter. The formulation castoff means that each letter encodes to one other letter, and back again, position the cipher is essentially a standard substitution cipher with a instruction leading which letter goes to which. This technique provides better security. After converting the plain text into cipher text by using Affine algorithm we have taken cipher text and converting each letter into ASCII codes then the ASCII codes have converted into a sequence of binary codes to provide higher security.[2]. This planned practice is used to prevent the intruders to get the real data when they try to retrieve the data. This encrypt data shall be entrenched exclusive the image with almost zero distortion of the original image.



Figur 2: A flow chart demonstrating the encryption phase

2. Encryption Process

Step One: Choose the top-secret message
Step Two: Encrypt the message using Affine Cipher Algorithm
Step Three: Convert the encrypt message into ASCII code
Step Four: Convert ASCII code into binary For Example:
Input Text: Kurdistan
Encrypt Text: Kofmeilgt In this process, the script is going to be the letters A through Z.
In this encoding sample, the plaintext to be encrypted is "Kurdistan". For the numeric values of each letter the following function have been used to encrypt each letter:
$E(x) = (ax + b) \bmod m$

Where:
x: is the numerical value of the communication in the plaintext.
m: is the number of letters in the plaintext alphabet. a and b are the secret numbers amid sender & receiver.
E(x): is the result of transformation.

Table 1 Detect X value

Plaintext	K	u	r	d	i	s	t	a	n
X	10	20	17	3	8	18	19	0	13

Now, take each value of x, and solve the first part of the equation, (3x + 6). After finding the significance of (3x + 6) for each character, take the remainder when dividing the result of (3x + 6) by 26. The resulting table displays the first four steps of the encoding process: Table 2 Convert Plain Text into Cipher Text

Plaintext	K	u	r	d	i	s	t	a	n
X	10	20	17	3	8	18	19	0	13
(3x + 6)	36	66	57	12	30	60	63	6	45
(3x+6)mode 26	10	14	5	12	4	8	11	6	19
Cipher Text	K	o	f	m	e	i	l	g	t

Convert Encrypt Text into ASCII Code: 75 111 119 109 101 105 108 103 116

ASCII Code to Binary Conversion: 01001011 01101111 01110111 01101101 01100101 01101001 01101100 01100111 01110100

II. STEGANOGRAPHY TYPES

1) The various types of steganography include [3]:

   a) Image Steganography The image steganography is the process in which we pelt the data within an picture so that there shall not be any perceivable alteration in the unique image. The conventional image steganography algorithm is an LSB embedding algorithm.
   b) Audio Steganography The way of walloping top-secret evidence in an audio is known as audio steganography. Here are several approaches for wallop top-secret data in an audio such as LSB, Phase Coding etc.
   c) Video Steganography The way of wallop top-secret evidence in a video is known as video steganography.

Video entail of pictures in addition to audio. Hence, both images and audio steganography could be used for video steganography.

d) Text files Steganography The way of walloping top-secret evidence in a text is known as text steganography. Text steganography necessitates fewer recollection as it can only stock text files. It offers rapid communiqué or handover of files from one computer to another. Text steganography is not commonly used as text files containing a large amount of redundant data.

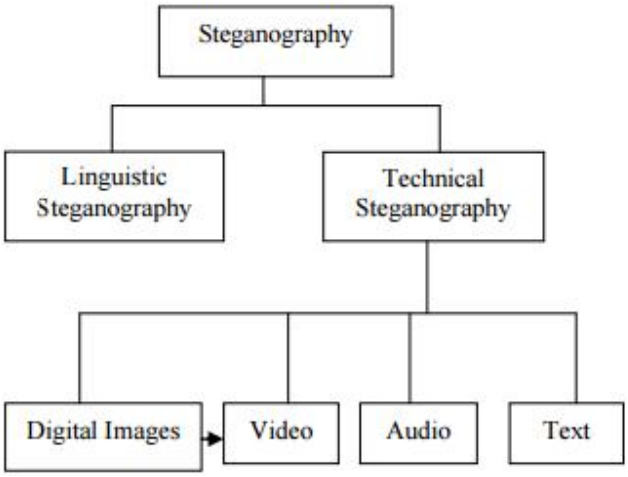


Figure 3 Types of steganography

III. APPLICATION

Few applications of the steganography are [4]:

- Defense Organizations: Security from enemies
- Intelligence Agencies: Security of person's private information
- Government Agencies: Store critical data like criminal record
- Smart Identity Cards: Personal information is embedded into photo
- Medical: Patient's details are embedded within image

IV. LITERATURE SURVEY

Vidhya P.M, et.al (2015) a way of steganography is planned with an Indian native linguistic, Malayalam. The planned process entails of convention Unicode based technique with implanting founded on indexing, i.e. the original message is encoded in Malayalam text with custom UNICODE values generated for the Malayalam text. The proportional education of the planned process against an existing method revealed that, the proposed steganography methods is more precise in the encoding process and in the decoding process. The method achieved a precision rate of .95 and the decoding rate of .81 [5].

Milia Habib et.al (2015) a protected DCT steganography way is projected. It allows walloping a secret image in another image randomly using Chaos. The disordered producer Concord Wise Linear Chaotic Map PWLCM with disquiet was selected, it has good chaotic properties and an easy implementation. It was used to obtain the pseudo-random series of pixels in which the secret image will be embedded in their DCT coefficients. It enhances the LSB-DCT technique with threshold [6].

Yugeshwari Kakde et.al (2015) Working on audio video steganography, which is the mixture of Audio steganography & Image steganography, Here the author is consuming computer forensics practice for authentication purpose. Here our aim is to fleece top-secret evidence overdue audio & image of a video file. As we know that video is the amalgamation of several still frames of images and audio[7]

Kamaldeep Joshi, et.al (2015) a new-fangled process of image steganography in longitudinal domain on gray images merger with cryptography is existing. Steganography and cryptography are used to hide messages and its sense correspondingly. Through this process, the message is first encoded by Vernam cipher algorithms and then the message (encrypted) is embedded inside an image using the new image steganography method i.e. LSB with Shifting (LSB-S) [8].

Sayantari Ghosh, et.al (2015) a Hilbert curve based technique to embed information in an picture by means of the neuro mental performance of the hominid apparition scheme which is robust to different attacks like cropping, scratching, additive noise etc [9].

Avinash Tyagi et.al (2015) a new image steganography technique has been proposed which is based on the pixel value differencing and the pixel value sum of two consecutive pixels of a shelter image. The planned algorithm pelts the top-secret data in the concealment image by operating the difference or sum of the non-overlapping blocks of two consecutive pixels. This technique is an improvement over the Wu and Tsai's PVD technique that is totally based on pixel value differencing [10].

In Ifra Bilal, et.al (2014) a survey on latest audio steganographic methods is carried out along with their strength and weakness. Too, judgment amid numerous steganographic approaches founded on heftiness is carried out. Additional contribution of this paper is evaluation of

performance of various reviewed steganography techniques [11].

Ratnakirti Roy, et.al (2013) here suggests an edge adaptive image steganography instrument which syndicates the benefits of matrix indoctrination and LSBM to embed data and also uses a chaotic mapping scheme to provide enhanced security to the payload. Efforts have been assumed to safeguard that the planned instrument conforms to high Imperceptibility and Fidelity, which are the indispensable excellence necessities for any image steganography system [12].

V. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods: here the top-secret data are rooted straight in the concentration of pixels. It means certain pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories:

I. Least significant bit (LSB)
II. Pixel value differencing (PVD)
III. Edges based data embedding method (EBE)
IV. Random pixel embedding method (RPE)
V. Mapping pixel to have hidden data method
VI. Labelling or connectivity method
VII. Pixel intensity based.

a. LSB: Here greatest normally rummage-sale for walloping data. In this process the implanting is complete by substituting the least significant bits of image pixels with the bits of top-secret data. The image obtained after embedding is almost similar to the original image because the change in the LSB of image pixel does not bring too much differences in the image.

b. PVD: Here, two successive pixels are nominated for implanting the data. The payload is determined by checking the difference between two consecutive pixels and it serves as a basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique: The concept of spread spectrum is cast-off in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it's become difficult to notice the presence of data. Even if shares of the data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus, it is problematic to eliminate the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3. Statistical Technique: In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the scope of message bit is one, otherwise no modification is required.

4. Transform Domain Technique: In this technique; the secret communication is entrenched in the transform or frequency domain of the cover. This is a more multifaceted way of walloping messages in an image. Dissimilar algorithms and alterations are cast-off on the image to hide message in it. Transform domain techniques are broadly classified such as

i. Discrete Fourier transform technique (DFT)
ii. Discrete cosine transformation technique (DCT)
iii. Discrete Wavelet transformation technique (DWT)
iv. Lossless or reversible method (DCT) v) Embedding in coefficient bits

5. Distortion Techniques: In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of the modifications and consequently recover the secret message.

6. Masking and Filtering: These techniques hide information by marking an image. Steganography only hides the information where as watermarks become a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and gray scale images [13].

VI. CONCLUSION

This broadsheet attentions on combining the strong point of steganography, and encryption, and how information could be encrypted and hided. Arrangement of operation matters while combining both the operations, because first presence of information should be hided, and if broken it will be further secured by encrypted message. But it also be subject to on the type of information and security method. Also size of carrier data is important.

REFERENCES

[1] Ashadeep Kaur,Rakesh Kumar, Kamaljeet Kainth, "Review Paper on Image Steganography". 2016, IJARCSSE

[2] Ako Muhammad Abdullah, Roza Hikmat Hama Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm". International Journal of Computer Applications.2016

[3] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "A Crypto-Steganography: A Survey", (IJACSA), 2014.

[4] Hemang A. Prajapati , Dr. Nehal G. Chitaliya, "Secured and Robust Dual Image Steganography: A Survey". IJIRCCE.2015

[5] Vidhya P.M,Varghese Paulb, "A Method for Text Steganography Using Malayalam Text" (ICICT 2014)

[6] Milia Habib, Bassem Bakhache, Dalia Battikh, Safwan El Assad "Enhancement using chaos of a Steganography method in DCT domain"

[7] Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, "Audio-Video steganography" 2015 IEEE

[8] Kamaldeep Joshi, Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication" 2015 IEEE

[9] Sayantari Ghosh, Saumik Bhattacharya Amity University, Kolkata W.B., India "Hilbert Curve Based Steganographic Scheme for Large Data Hiding", 2015 IEEE

[10] Avinash Tyagi, Ratnakirti Roy, Suvamoy Changder, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum" 2015 IEEE

[11] Soon-Nyean Cheong, Huo-Chong Ling, Pei-Lee Teh , "Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system" (2014).

[12] Ratnakirti Roy, Anirban Sarkar, Suvamoy Changder, "Chaos based Edge Adaptive Image Steganography" 2013

[13] Hui Tian, Jie Qin, Yongfeng Huang, Yonghong Chen, Tian Wang, Jin Liu, Yiqiao Cai "Optimal matrix embedding for Voice-over-IP steganography" College of Computer Science and Technology, National Huaqiao University, Xiamen 361021, China

[14] Parmar Ajit Kumar Maganbhai , Prof. Krishna Chouhan, "A Study and literature Review on Image Steganography". (IJCSIT) 2015