

A New High Capacity and Secure Steganography Approach for Hiding Data

Divya Anand

School of Computer Science and Engineering, Lovely Professional University, Phagwara,
Punjab, India,

divyaanand.y@gmail.com

Aman Singh

School of Computer Science and Engineering, Lovely Professional University, Phagwara ,
Punjab, India

Amansingh.x@gmail.com

Abstract

Due of the expanded interest of trading information over web, one of the most troublesome errands is to control unapproved data. Concerning security, steganography gives a superior method to conceal information from unapproved clients. It is a helpful apparatus that permits the transmission of data over an obvious correspondence channel. This paper gives a general review on steganography and a decent steganographic procedure for concealing mystery information under the spread picture. Another exceptionally precise and solid technique is proposed for covering the data from the unintended individuals. Implanting in dissipated pixels in both 24-piece shading pictures and 8-piece grayscale or shading pictures is done using the new proposed technique.

Keywords: Steganography, color images, grayscale images.

1. INTRODUCTION

The word 'Steganography' is of the Greek starting point and its meaning is "Secured Writing". Steganography is the capacity of whipping the endurance of correspondence information. In this, the data is hidden in a spread media so automatically individuals won't see that such information is here. It is the act of whipping information in such a strategy, that it

shows up nothing out of the typical. It is a soonest artistic work of trouncing information[1]. The point in this is to disguise information well adequate that unexpected beneficiary don't expect the Steganography moderate of containing covered data. Using an express picture as a spread is the chiefly acknowledged method to shroud the information in file[2,3]. There has been a quick improvement of interest in this subject over the little past years. Above all else, the distribution and conveyance enterprises are focusing in strategies for whipping encoded patent imprints and successive data in computerized films, aural accounts, books and interactive media merchandise; an endorsement of new commercial center open doors made by advanced sharing is gotten together with frenzy that advanced works could be anything but difficult to copy [4,5]. Furthermore, moves by an assortment of government to restrain the openness of cryptographic administrations have constrained individuals to learn ways by which mystery information can be embedded in evidently guiltless wrap messages.

It resembles with a term "Cryptography". Cryptography is another methodology used to safeguard data by modifying it into another framework. Steganography is much verifying than cryptography. Cryptography secures the stuffing of a message, Steganography can be said to watch together correspondence and imparting parties [6]. The information can be much safely covered up with the assistance of steganography procedure when contrasted with the cryptography. Different innovations that are legitimately associated with steganography are watermarking and fingerprinting.

The paper is organized as: Section II defines the terms used in the steganography. Section III gives the various techniques of steganography. Section IV provides the basic principle of the new proposed technique. In section V, the algorithm for both embedding and extracting is given.

2. TERMS USED

There are different terms which are utilized in Steganography.

A. Cover media: A cover media is anything under which we can shroud the information. It very well may be any picture, sound document, video record and so forth. It is the medium which holds the shrouded information.

B. Secret information: The mystery data which we need to stow away under the spread media. This is the valuable data which must be stayed quiet.

C. Embedding Function: This capacity shrouds the secretive data under the spread picture. This utility is utilized at the sender side to implant the helpful data under the spread media.

D. Payload: The amount of valuable data which is to be secured. This ought to be as higher as could be allowed yet to remember one thing that the nature of spread media and mystery information ought to be kept same.

E. Stego-yield: The yield after the stage of steganography on the secret information. It must be same as the spread media. It must give the less twisting and it must have high limit and high vigor.

F. Extracting Function: The capacity utilized at the recipient side to separate the mystery information from the spread picture effectively.

H. Correspondence Channel/ Communication Function: The methods by which the message is sent to receiver [7, 8, 9].

3. TECHNIQUES

There are different techniques by which we can perform Steganography on our data.

A. Substitution techniques

The substitution of the repetitive component of information inside a secret message is done by substitution techniques. It contains LSB substitution, supplanting with consistency bits of piece, substitution in double pictures and substitution in reserved or inert space in processor framework [10].

B. Transform domain techniques

Change space strategies conceal correspondence in significant regions of the encompass picture which make them progressively solid to assaults, for example, immovability, trimming and so forth.

C. Spread spectrum techniques

The spread spectrum technique has two variations: direct-arrangement and recurrence jumping plans. In the direct arrangement plan, the secret sign is reached by a consistency rate called chip rate, tweaked with a pseudorandom sign and added to the spread. In recurrence jumping plan, the recurrence of transporter signal is mutilated in a manner such that it jumps rapidly starting with just one normality function then onto the next [11].

D. Statistical techniques

Factual Steganography system uses the endurance of "little piece" Steganography plans, which implant one piece of data in an advanced carter.

E. Distortion techniques

Bending method requires the information on the first spread in distortion process. It stores data by signal twisting and in the extraction step quantifies the deviation from the remarkable spread [12, 13].

F. Cover generation techniques

It encodes data that guarantees development of an envelope for secretive message [14, 15, 16].

4. BASIC PRINCIPLE

The substitution steganography approach for concealing mystery information under the spread picture is proposed. This strategy is utilized for concealing an extremely huge measure of mystery information under the spread picture. The new method decreases the size of the information without utilizing any pressure system. The changing of information into various

structures will diminish the size and increment the security and limit. The picture utilized for this procedure is 24-piece picture.

5. STEPS OF NEW TECHNIQUE

The steps for newly proposed technique are:

PROBLEM DEFINITION

Given a cover image and payload, the payload is to be embedded into the cover image.

A. EMBEDDING (AT SENDER END)

Input: Cover Image, Secret Message and key.

Output: Stegoimage.

Step 1: Enter the text message

Step 2: Convert that message to message of 1000 characters

Step 3: Then convert the message to ASCII code

Step 4: Convert each row to binary representation of ASCII code

Step 5: Select the cover image under which the data is to be hidden

Step 6: Enter the key for encryption

Step 7: Create coordinate pairs for the key

Step 8: House the hiding points in this.

Step 9: Form a zero matrix of same dimension as image

Step 10: Embed data

Step 11: Save the stegoimage

B. EXTRACTION (AT RECEIVER END)

Input: Stegoimage and Key.

Output: Secret Message and Cover Image.

Step 1: Start decoding

Step 2: Input the stegoimage

Step 3: Enter the key for decryption

Step 4: Find the positions where data is hidden

Step 5: Convert the message from binary format to ASCII format

Step 6: Convert the message from ASCII format to message of 1000 characters

Step 7: Convert the message to original message

Step 8: Extract message and cover image

References

- [1] A. A. G.Ghinea, "Image Steganography and Chrominance Components", 10th International Conference on Computer and Information Technology (CIT), 2010.
- [2] B. Krishan, A. P. Singh, "Moderate Bit Insertion for Hiding Crypto-Data in Digital Image for Steganography", IP Multimedia Communication, International Journal of Computer Application (IJCA), 2009.
- [3] D. Artz, "Digital Steganography: Hiding Data within Data", Los Alamos National Laboratory, 1089-7801, IEEE, pp 9-13, 2001.
- [4] F. S. Abed, "A Proposed Encoding and Hiding Text in an Image by using Fractal Image Compression", International Journal on Computer Science and Engineering (IJCSE), 2007.
- [5] F.Alnawok and B. Ahmed, "Multi Segment steganography Technique", International Arab Journal of Information Technology , Vol. 5, No. 3, pp13, 2008.
- [6] G.Canceli, G.Doerr, I. J. Cox and M. Barni, "Detection of ± 1 LSB Steganography Based on The Amplitude of Histogram Local Extrema", 15th IEEE International Conference on Image Processing, (ICIP), 2008.
- [7] J. J. Roque, J. M. Minguet, "SLSB: Improving the Steganography Algorithm LSB", International Journal of Computer Science and Network Security, Vol. 8, No.6, pp12, 2008.
- [8] K. S.Babu, K. B. Raja, U. M. Rao K, Val, K. R. L. M.Patnaik, "Robust Image Steganography Using SVD", IET-UK International Conference on Information and Communication Technology in Electrical Sciences(ICTES), 2007.

- [9] K. F.Rafat and M. Sher, "Survey Report – State of the Art In Digital Steganography Focusing ASCII Text Documents", (IJCSIS) International Journal of Computer Science and Security, Vol. 7, No. 2, 2010.
- [10] M.S.Sutaone and M.V. Khan dare, " Image Based Steganography Using LSB Insertion Technique", International Journal of Computer Science and Information Security, U.S.A, Vol.6, No. 2, pp. 269-274, 2011.
- [11] M.Bano, "Improving Embedding Capacity with Minimum Degradation of Stego-image", International Journal of Basic & Applied Sciences IJBAS – IJENS, Vol. 10, No. 06, 2011.
- [12] M.Juneja, "Application of LSB Based Steganographic Technique for 8-bit Color Images", World Academy of Science, Engineering and Technology, 50, 2019.
- [13] M. A.Zaher, "Modified Least Significant Bit (MLSB)", International Journal of Computer and Information Science Vol. 4, No. 1; pp. 12-17, 2017.
- [14] M. A. B. Younes and A.Jantan," A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion", IJCSNS International Journal of Computer Science and Network Security, Vol.8, No.6, pp11, 2018.